

**COMMONWEALTH OF MASSACHUSETTS
THE SUPREME JUDICIAL COURT**

NO. SJC-13542

KATHLEEN VITA
Plaintiff - Appellee

v.

NEW ENGLAND BAPTIST HOSPITAL and
BETH ISRAEL DEACONESS MEDICAL CENTER, INC.
Defendants - Appellants

REPORTED TO THE APPEALS COURT FROM THE SUPERIOR COURT
DIRECT APPELLATE REVIEW GRANTED

PLAINTIFF-APPELLEE'S BRIEF

SHAPIRO HABER & URMY LLP
Edward F. Haber (BBO #215620)
Michelle H. Blauner (BBO #549049)
Patrick J. Valley (BBO #663866)
One Boston Place
Suite 2600
Boston, MA 02108
(617) 439-3939
ehaber@shulaw.com
mblauner@shulaw.com
pvalley@shulaw.com

Counsel for Plaintiff

Table of Contents

	<u>Page</u>
Table of Contents	2
Table of Authorities.....	4
Statement of the Issues.....	11
Statement of the Case.....	12
Statement of Facts	14
I. Defendants and Their Implementation of AdTech.....	14
II. How AdTech Worked.....	15
III. Defendants Lied to Consumers, Falsely Telling Them that Defendants Did Not Share Website Communications with Outside Parties.	20
IV. The Nature of the Communications Intercepted.....	22
Summary of Argument.....	25
Argument.....	29
I. The MWA Applies to Communications Between Consumers and Businesses Through Websites.....	29
A. The MWA’s Plain Terms (Including Its Preamble) Support the Decisions.....	29
1. The MWA Is Not Limited to Communications Between Individuals.	31
2. The MWA Applies to Modern Electronic Communications.	33
3. Website Communications Occur by “Wire.”.....	35
B. Legislative History Confirms the MWA Applies to Emerging Technologies.	36

II. Plaintiff Alleges Secret Interceptions.	38
A. Secrecy Cannot Be Decided on a Motion to Dismiss.	39
B. Any Knowledge of Recording By Defendants’ Web Servers Does Not Equate to Knowledge of Third-Party Eavesdropping.	40
C. Defendants Ignore the Difference Between Third-Party Eavesdropping and Subsequent Sharing.	45
III. The Telephone Equipment Defense Does Not Apply.	46
A. AdTech Is Not Telephone Equipment.	46
B. Defendants Did Not Use AdTech in the Ordinary Course of Business.	50
IV. The MWA’s Plain Terms Confer Standing.	52
V. The Court Should Reject Defendants’ Invitations to Disregard the MWA’s Plain Terms.	56
A. The Rule of Lenity Cannot Be Used to Negate the MWA’s Plain Terms.	56
B. Applying the MWA to Defendants’ Conduct Is Consistent with Legislative Intent and Not Absurd.	59
Conclusion	65
Addendum	66
Certificate of Compliance	372
Certificate of Service	373

Table of Authorities

	<u>Page</u>
<u>Cases</u>	
<i>Abraham v. Cnty. of Greenville</i> , 237 F.3d 386 (4th Cir. 2001).....	63
<i>Abramovitz v. Ahern</i> , 96 F.R.D. 208 (D. Conn. 1982).....	63
<i>Adams v. Holder</i> , 692 F.3d 91 (2d Cir. 2012).....	57
<i>Alves v. BJ's Wholesale Club, Inc.</i> , 2023 Mass. Super. LEXIS 59 (June 21, 2023).....	13, 48
<i>Alves's Case</i> , 451 Mass. 171 (2008)	63
<i>Balletto v. Am. Honda Motor Co.</i> , 2024 U.S. Dist. LEXIS 25150 (N.D. Cal. Feb. 13, 2024).....	32
<i>Berry v. Funk</i> , 146 F.3d 1003 (D.C. Cir. 1998)	51
<i>Braun v. Phila. Inquirer, LLC</i> , 2023 U.S. Dist. LEXIS 202528 (E.D. Pa. Nov. 13, 2023)	39
<i>Brown v. Google LLC</i> , 525 F. Supp. 3d 1049 (N.D. Cal. 2021)	51
<i>Calhoun v. Google LLC</i> , 526 F. Supp. 3d 605 (N.D. Cal. Mar. 17, 2021).....	40
<i>Chin v. Merriot</i> , 470 Mass. 527 (2015)	52
<i>Commonwealth v. Brown</i> , 479 Mass. 600 (2018)	59

<i>Commonwealth v. Connolly</i> , 454 Mass. 808 (2009)	35
<i>Commonwealth v. Cruttenden</i> , 58 A.3d 95 (Pa. 2012)	44
<i>Commonwealth v. Diego</i> , 119 A.3d 370 (Pa. Super. Ct. 2015)	48
<i>Commonwealth v. Du</i> , 103 Mass. App. Ct. 469 (2023).....	26, 33, 41
<i>Commonwealth v. Hyde</i> , 434 Mass. 594 (2001)	27, 57
<i>Commonwealth v. Jackson</i> , 370 Mass. 502 (1976)	26, 38
<i>Commonwealth v. Maloney</i> , 447 Mass. 577 (2006)	57
<i>Commonwealth v. Moody</i> , 466 Mass. 196 (2013)	passim
<i>Commonwealth v. Morris</i> , 492 Mass. 498 (2023)	44
<i>Commonwealth v. Peterson</i> , 476 Mass. 163 (2017)	59
<i>Commonwealth v. Proetto</i> , 771 A.2d 823 (Pa. Super. Ct. 2000)	44
<i>Commonwealth v. Rainey</i> , 491 Mass. 623 (2023)	44
<i>Cook v. Patient Edu, LLC</i> , 465 Mass. 548 (2013)	57
<i>Cousin v. Sharp Healthcare</i> , 2023 U.S. Dist. LEXIS 206638 (S.D. Cal. Nov. 17, 2023)	32

<i>Crosland v. Horgan</i> , 401 Mass. 271 (1987)	50
<i>Curtatone v. Barstool Sports, Inc.</i> , 487 Mass. 655 (2021)	43
<i>Dekoladenu v. Gonzales</i> , 459 F.3d 500 (4th Cir. 2006).....	62
<i>Dillon v. Mass. Bay Transp. Auth.</i> , 49 Mass. App. Ct. 309 (App. Ct. 2000)	47, 48
<i>DiMasi v. Galvin</i> , 2020 Mass. Super. LEXIS 102 (July 2, 2020)	63
<i>Doe v. Boston Children’s Hospital</i> , No. 2384CV00411-BLS-1 (Mass. Super. Ct. Sept. 14, 2023),.....	30
<i>Doe v. Emerson Hospital</i> , No.2277CV01000 (Mass. Super. Ct. Nov. 22, 2023)	13
<i>Doe v. Partners Healthcare System, Inc.</i> , No.1984CV01651-BLS1 (Mass. Super. Ct. Dec. 7, 2020).....	13
<i>Doe v. Sutter Health</i> , Case No. 34-2019-00258072 (Cal. Cnty. Ct. June 9, 2022)	32
<i>Fairneny v. Savogran Co.</i> , 422 Mass. 469 (1996)	11
<i>Fournier v. Troianello</i> , 332 Mass. 636 (1955)	53
<i>Garcia v. Steele</i> , 492 Mass. 322 (2023)	31
<i>Garcia v. Yeti Coolers, LLC</i> , 2023 U.S. Dist. LEXIS 158968 (C.D. Cal. Sep. 5, 2023)	32
<i>GlobalTranz Enters. Inc. v. Shipper’s Choice Global LLC</i> , 2017 U.S. Dist. LEXIS 234215 (D. Ariz. 2017).....	59

<i>In re Blixseth</i> , 684 F.3d 865 (9th Cir. 2012).....	62
<i>In re Facebook Inc. Internet Tracking Litig.</i> , 956 F.3d 589 (9th Cir. 2020).....	32
<i>In re Facebook, Inc.</i> , 402 F. Supp. 3d 767 (N.D. Cal. 2019)	42
<i>In re Google Inc. Gmail Litig.</i> , 2013 U.S. Dist. LEXIS 172784 (N.D. Cal. Sept. 26, 2013).....	42, 45, 50
<i>In re Grp. Health Plan Litig.</i> , 2023 U.S. Dist. LEXIS 227218 (D. Minn. Dec. 21, 2023)	32
<i>In re Hokulani Square, Inc.</i> , 776 F.3d 1083 (9th Cir. 2015).....	59
<i>In re Pharmatrak, Inc. Privacy Litig.</i> , 329 F.3d 9 (1st Cir. 2003)	25, 32, 41, 63
<i>James v. Walt Disney Co.</i> , 2023 U.S. Dist. LEXIS 200997 (N.D. Cal. Nov. 8, 2023)	32, 58
<i>Joffe v. Google, Inc.</i> , 746 F.3d 920 (9th Cir. 2013).....	32, 58
<i>Johnson v. Frei</i> , 93 Mass. App. Ct. 1111 (2018)	53
<i>Kelley v. Albuquerque</i> , 375 F. Supp. 2d 1183 (D.N.M. 2004)	59
<i>Kenn v. Eascare, LLC</i> , 103 Mass. App. Ct. 643 (2024).....	53, 54, 55
<i>LaChance v. Comm’r of Corr.</i> , 475 Mass. 757 (2016)	54
<i>Lamie v. United States</i> , 540 U.S. 526 (2004).....	62

<i>Lyon v. Triram Corp.</i> , 2004 Mass. Super. LEXIS 496 (Oct. 29, 2004)	55
<i>Magliacane v. Gardner</i> , 483 Mass. 842 (2020)	64
<i>Marquis v. Google Inc.</i> , SUCV2011-02808-BLS1 (Super. Ct. Jan. 17, 2012).....	33
<i>Marquis v. Google, Inc.</i> , 2014 Mass. Super. LEXIS 104 (June 27, 2014)	64
<i>Metcalf v. BSC Grp., Inc.</i> , 492 Mass. 676 (2023)	28
<i>Morrison v. Lennett</i> , 415 Mass. 857 (1993)	39
<i>Muscarello v. United States</i> , 524 U.S. 125 (1998).....	57
<i>O’Sullivan v. NYNEX Corp.</i> , 426 Mass. 261 (1997)	47
<i>Phone Recovery Servs., LLC v. Verizon of New England, Inc.</i> , 480 Mass. 224 (2018)	53
<i>Pine v. Rust</i> , 401 Mass. 411 (1989).....	27, 52, 58, 60
<i>Popa v. Harriet Carter Gifts, Inc.</i> , 52 F.4th 121 (3d Cir. 2022).....	29, 32, 45, 60
<i>Price v. Carnival Corp.</i> , 2024 U.S. Dist. LEXIS 10175 (S.D. Cal. Jan. 19, 2024)	32, 45
<i>Revitch v. New Moosejaw, LLC</i> , 2019 U.S. Dist. LEXIS 186955 (N.D. Cal. Oct. 23, 2019)	31
<i>Ribs v. Clark</i> , 696 P.2d 637 (Cal. 1985)	46

<i>Rich v. Rich</i> , 2011 Mass. Super. LEXIS 148 (Super. Ct. July 8, 2011)	33
<i>Sanders v. Robert Bosch Corp.</i> , 38 F.3d 736 (4th Cir. 1994)	50, 51
<i>Spokeo Inc. v. Robins</i> , 578 U.S. 330 (2016).....	53
<i>Telebrands Corp. v. Altair Instruments, Inc.</i> , 2019 U.S. Dist. LEXIS 136594 (D.N.J. Aug. 13, 2019)	34
<i>Tze-Kit Mui v Mass. Port Auth.</i> , 478 Mass. 710 (2018)	28
<i>United States v. Lyons</i> , 740 F.3d 702 (1st Cir. 2014)	35
<i>United States v. W. R. Grace</i> , 504 F.3d 745 (9th Cir. 2007).....	58
<i>Vonbergen v. Liberty Mut. Ins. Co.</i> , 2023 U.S. Dist. LEXIS 220178 (E.D. Pa. Dec. 11, 2023).....	32, 45
<i>Watkins v. L.M. Berry & Co.</i> , 704 F.2d 577 (11th Cir. 1983)	41, 50
<i>Weld v. Glaxo Wellcome, Inc.</i> , 434 Mass. 81 (2001)	54
<i>Williams v. Poulos</i> , 11 F.3d 271 (1st Cir. 1993).....	47, 49
<i>Zaratzian v. Abadir</i> , 2014 U.S. Dist. LEXIS 129616 (S.D.N.Y. 2014)	58

Statutes

18 U.S.C. §252064
1920 Mass. Acts c.55837
1968 Mass. Acts c.73836
G.L. c.272 §99..... passim
G.L. c.93A §954
G.L. c.93A, §1155

Rules

Mass. R. Civ. P. 6413

Other Authorities

H. Bill 1435 (Mass. 1967)..... 48, 56, 62
H. Bill 3665 (Mass. 1968)..... 56, 62
S. Bill. 201 (Mass. 1964)37
S. Rep. 1132 (Mass. 1968)..... 38, 41
S. Rep. 1198 (Mass. 1967)..... 37, 49, 62
S. Rep. 1469 (Mass. 1967)..... 38, 62

Statement of the Issues

In reviewing the Superior Court’s denial of Defendants’ motions to dismiss, this Court must, as the court below did, “accept as true the allegations in the complaint, and draw all reasonable inferences in favor of the party whose claims are the subject of the motion,” *Fairney v. Savogran Co.*, 422 Mass. 469, 470 (1996), to determine whether the factual allegations plausibly suggest an entitlement to relief under the Massachusetts Wiretap Act, G.L. c.272 §99 (“MWA”). When viewed through the proper legal lens, the following issues are presented for appeal:

1. Whether Plaintiff plausibly alleged her communications with Beth Israel Deaconess Medical Center, Inc. (“BIDMC”) and New England Baptist Hospital (“NEBH”)(“Defendants” or “the Hospitals”) through their websites fell within the MWA’s broad definition of “wire communications.”
2. Whether Plaintiff plausibly alleged she had no knowledge Defendants enabled third parties to eavesdrop on her communications with the Hospitals, given her allegations that computer code, which enabled those interceptions, was hidden, and Defendants’ privacy policies represented that no information would be shared with outside parties.
3. Whether Defendants’ facilitation of third-party eavesdropping was accomplished through “telephone equipment” and whether this Court can

determine as a matter of law that it was in the “ordinary course” of Defendants’ business to allow social media and technology companies to intercept communications in contravention of Defendants’ website privacy policies.

4. Whether the MWA confers standing upon Plaintiff—as the aggrieved party whose communications were intercepted—to sue Defendants for enabling the secret interception of her website communications.

Statement of the Case

Plaintiff’s complaints against Defendants arise from the Hospitals’ secret deployment of software-based internet tracking technologies on their websites (“AdTech”), which enabled third parties, including Google and Facebook, to eavesdrop on consumers’ communications with the Hospitals for use in targeted advertising.¹ By enabling the interceptions, Defendants breached their express promise not to share any communications they received through the websites with any outside parties.² Each complaint asserts a class claim for violation of the MWA.³

¹ The complaints do not vary significantly because both Hospitals, which are part of Beth Israel Lahey Health, R:A:I:23, R:A:IV:24, implemented AdTech in a similar fashion, used identical website privacy policies, and the websites share a common design.

² R:A:I:14(¶¶23); R:A:IV:15(¶23).

³ R:A:I:55-56(¶¶116-23); R:A:IV:49-51(¶¶106-13).

Justice Kazanjian of the Superior Court denied Defendants’ motions to dismiss (the “Decisions”).⁴ The Superior Court concluded that Defendants’ secret use of AdTech that enabled social media and technology companies to eavesdrop on Plaintiff’s website communications with the Hospitals stated a claim for an MWA violation. Three other Superior Court justices (Davis, Krupp, and Howe) have separately reached the same conclusion in similar cases.⁵

The Superior Court reported the Decisions to the Appeals Court under Mass. R. Civ. P. 64.⁶ This Court accepted Direct Appellate Review.⁷

Through this appeal, Defendants seek to upend an established body of law broadly applying the MWA to the secret use of emerging technologies to eavesdrop on electronic communications. The Superior Court correctly held that Plaintiff stated a claim under the MWA. The Decisions should be affirmed.

⁴ Addendum:69-92; Addendum:202-11 (incorporated by reference).

⁵ *Doe v. Emerson Hospital*, No.2277CV01000 (Mass. Super. Ct. Nov. 22, 2023)(Addendum:212-23); *Doe v. Partners Healthcare System, Inc.*, No.1984CV01651-BLS1 (Mass. Super. Ct. Dec. 7, 2020)(Addendum:224-315); *Alves v. BJ's Wholesale Club, Inc.*, 2023 Mass. Super. LEXIS 59 (June 21, 2023).

⁶ Addendum:78-80, 90-92.

⁷ DAR-29590, Paper 4.

Statement of Facts

I. Defendants and Their Implementation of AdTech.

Defendants are healthcare providers.⁸ They maintain websites enabling consumers to communicate with the Hospitals about doctors, medical conditions and healthcare services, to book appointments, access medical records, and pay bills.⁹ Healthcare consumers, like Plaintiff, used the websites for those purposes and understood their communications with the Hospitals through the websites were private.¹⁰

Defendants implemented AdTech on nearly every page of their websites. The AdTech contemporaneously intercepted and transmitted to third parties the content of healthcare consumers' communications with the Hospitals.¹¹ Those technologies included Meta Pixel, which transmitted communications to Facebook, and Google Analytics, which transmitted communications to Google.¹² AdTech is not necessary for Defendants' websites' functionality.¹³ AdTech is invisible to website users.¹⁴

⁸ R:A:I:11(¶13); R:A:IV:12(¶13).

⁹ R:A:I:11-12(¶¶14-15); R:A:IV:12-13(¶¶14-15).

¹⁰ R:A:I:10-15(¶¶10, 17-20, 25); R:A:IV:12-16(¶¶10, 17-20, 25).

¹¹ R:A:I:22(¶¶55-56); R:A:IV:23(¶¶55-56).

¹² R:A:I:15-17(¶¶26-37); R:A:IV:16-18(¶¶26-37).

¹³ R:A:I:52(¶¶105-06); R:A:IV:47(¶¶95-96).

¹⁴ R:A:I:20-21(¶51); R:A:IV:22(¶51).

Defendants enabled the secret interceptions of website communications by falsely promising that website communications with Defendants would not be shared with “outside organizations.”¹⁵ It is that secrecy that exposed Defendants to MWA liability.

After a media exposé about how Meta Pixel was used to intercept communications between patients and hospitals, Defendants removed Meta Pixel from their websites in September 2022; however, they continued to employ Google Analytics.¹⁶ Six months after the BIDMC action was filed, Defendants removed the remaining AdTech.

II. How AdTech Worked.

Plaintiff alleges in detail how AdTech worked.¹⁷ Defendants injected hidden code into nearly every page of their websites.¹⁸ When a user communicated with Defendants through their websites, hidden code was loaded into and executed within the consumer’s web browser.¹⁹ The code caused contents of consumers’ communications with Defendants to be intercepted and transmitted from the user’s

¹⁵ R:A:I:13-14(¶¶22-23); R:A:IV:14-15(¶¶22-23).

¹⁶ R:A:I:21-22(¶¶53-54); R:A:IV:22-23(¶54).

¹⁷ R:A:I:17-21(¶¶38-52); R:A:IV:18-22(¶¶38-53).

¹⁸ R:A:1:22(¶55); R:A:IV:23(¶55).

¹⁹ R:A:I:19(¶¶47-48); R:A:IV:20(¶¶47-48).

device to third-parties (including Google and Facebook).²⁰ The code executed in the background without any indication it was operating or transmitting communications to Google or Facebook.²¹

Google and Facebook each maintain detailed data troves on individuals, including their real names, locations, email addresses, friends, and other information collected from various sources.²² The hidden AdTech was designed to permit Google and Facebook to identify the individuals whose communications are intercepted. This identification occurred through several pieces of information AdTech collected, including individuals' internet protocol ("IP") addresses, combinations of web browser configurations unique to individuals ("browser fingerprints"), and persistent identifiers Google and Facebook assigned to individuals.²³ The intercepted communications provided a rich source of information that bolstered Google and Facebook's ability to target advertising to individual consumers.²⁴

When consumers communicated with Defendants about topics such as drug addiction, mental health, sexually transmitted diseases, or pregnancy, the Hospitals

²⁰ R:A:I:20(¶49); R:A:IV:21(¶49).

²¹ R:A:I:20-21(¶51); R:A:IV:22(¶51).

²² R:A:I:15-17(¶¶28-29, 35-36); R:A:IV:16-18(¶¶28-29, 35-36).

²³ R:A:I:20, 26-27(¶¶50, 63-64, 68-70); R:A:IV:21-22, 27-29(¶¶50, 63-64, 67-69).

²⁴ R:A:I:16-17(¶¶30, 37); R:A:IV:17-18(¶¶30, 37).

helped Google and Facebook intercept those communications and use them for individually targeted advertising.

To illustrate how the technology works, consider the BIDMC webpage for its Obstetrics and Gynecology department. The landing page gave patients the option to request an appointment:²⁵



²⁵ R:A:I:30(¶73).

New patients were asked to fill out a form to request an appointment, as illustrated below.²⁶

This form is for new patients only. For current patients: Please call your physician's office or use PatientSite to schedule your appointment online.

[PatientSite](#)

If you are experiencing a medical emergency, call 911. Please do not use this form.

First Name

Last Name

Email Address

Phone Number

Date of Birth (MM/DD/YYYY)

Department

OB/GYN - General 

²⁶ R:A:I:34(¶79).

When the new patient selected the department where she wished to make an appointment (e.g., OB/GYN-General), hidden Google Analytics code intercepted and transmitted that information to Google. The graphic below (created with a special tool) reveals the hidden network traffic generated by Google Analytics²⁷:

```
dl: https://www.bidmc.org/request-an-appointment
ul: en-us
de: UTF-8
dt: New Patient Appointment Request Form | BIDMC of Boston
sd: 24-bit
sr: 1920x1080
vp: 1244x979
je: 0
ec: internal link
ea: www.bidmc.org
el: OB/GYN - General
```

Google Analytics caused the user’s computer to intercept and transmit to Google that the user was communicating with BIDMC to request a “New Patient Appointment” with an “OB/GYN-General” doctor.²⁸ Meta Pixel caused similar information to be intercepted by and transmitted to Facebook.²⁹ Google and Facebook recorded this communication (along with information that helped identify

²⁷ R:A:I:34-35(¶¶80).

²⁸ *Id.*

²⁹ R:A:I:36-37(¶¶81-82).

the user), which they then used to target individualized advertising to the Hospitals' website users.³⁰

III. Defendants Lied to Consumers, Falsely Telling Them that Defendants Did Not Share Website Communications with Outside Parties.

The code for AdTech was invisible to consumers.³¹ Defendants could have, as most businesses do, disclosed that they assisted Google, Facebook, and other third parties to intercept the consumers' communications with Defendants. Not only did Defendants not do this, but they expressly and falsely disavowed sharing such communications. BIDMC said in its privacy policy:

Beth Israel Deaconess Medical Center routinely gathers data on website activity, such as how many people visit the site, the pages they visit, where they come from, how long they stay, etc. **The data is collected on an aggregate, anonymous basis, which means no personally identifiable information is associated with the data.** This data helps us improve site content and overall usage. **This information is not shared with other organizations.** Except for authorized law enforcement investigations or other facially valid legal processes, **we will not share any information we receive with any outside parties.**³²

NEBH made an identical statement in its privacy policy.³³

These statements were false: Communications with Defendants were **not** collected on an "aggregate" or "anonymous" basis. Rather, Google and Facebook

³⁰ R:A:I:34-37(¶¶80, 82).

³¹ R:A:I:20(¶51); R:A:IV:22(¶51).

³² R:A:I:14(¶23). All emphasis in this brief is added unless otherwise indicated.

³³ R:A:IV:15(¶23).

intercepted the communications on an individual basis and associated the intercepted communications with individuals known to Google and Facebook. Additionally, contrary to their express representations, Defendants shared the communications with “outside parties,” including Google and Facebook, by deploying hidden AdTech.³⁴

Defendants’ privacy policies also stated they were “committed to protecting your privacy” and that the “website allows you to visit most areas without identifying yourself or providing personal information. For those areas where you elect to provide identifiable information, we assure you that we make every effort to protect your privacy.”³⁵ These statements, too, were false. AdTech was designed to identify consumers, and Defendants were palpably **not** “committed to protecting [consumers’] privacy.”³⁶

It is difficult to conceive of a more grievous disclosure violation than hospitals permitting for-profit companies to intercept sensitive communications and then lying about it.

³⁴ R:A:I:14(¶23); R:A:IV:15(¶23).

³⁵ R:A:I:13-14(¶22); R:A:IV:14-15(¶22).

³⁶ *Id.*

IV. The Nature of the Communications Intercepted.

Healthcare consumers trust healthcare providers to guard their personal medical information.³⁷ Defendants violated that trust by configuring AdTech to share sensitive information with Google and Facebook. The Superior Court described consumer communications with Defendants through their websites as equivalent to “telephone inquiries and conversations with doctors’ offices.”³⁸ Plaintiff’s allegations amply support that description.

In addition to appointment requests (pp.17-19, *supra*), Defendants allowed Google and Facebook to **secretly** intercept other types of medical inquiries:

Communications Regarding Medical Services. Defendants’ websites permit consumers to obtain information about medical services.³⁹ For example, NEBH has “Pain Management” page⁴⁰ for consumers to request information about its Pain Management Program. When a consumer requested information about NEBH’s Pain Management Program, AdTech caused the user’s browser to transmit to Google and Facebook that the user requested information on NEBH’s “Pain Management” program.⁴¹

³⁷ R:A:I:12-13(¶¶17-21); R:A:IV:13(¶¶17-21).

³⁸ Addendum:74, incorporating Addendum:207.

³⁹ R:A:I:30-32 (¶¶73-77); R:A:IV:29-32 (¶¶71-75).

⁴⁰ R:A:IV:29(¶71).

⁴¹ R:A:IV:30-32(¶¶72-74).

Defendants' websites contain hundreds of pages on medical conditions, treatments, and services,⁴² including highly sensitive topics such as drug addiction, sexually transmitted diseases, and mental health issues. AdTech intercepted for Google and Facebook communications about the specific conditions and treatments each consumer inquired about.⁴³

Search Queries. Defendants' websites contain a search function through which consumers may use search terms to request specific information from Defendants. Such searches often reveal highly personal information about the consumer. For example, a consumer could search BIDMC's websites for the term "pregnant" or NEBH for the term "knee pain."⁴⁴ When a user performed those searches, Google and Facebook intercepted the search and learned that the user had asked BIDMC about being "pregnant" and NEBH about "knee pain."⁴⁵ Whatever precise words consumers used to ask Defendants for information (e.g., "HIV," "drug addiction," "suicide," "depression," or "pregnant") would be intercepted and instantaneously transmitted verbatim to Google and Facebook.⁴⁶

⁴² R:A:I:30(¶73); R:A:IV:32(¶75).

⁴³ *Id.*

⁴⁴ R:A:I:38-39(¶84); R:A:IV:32-33(¶76).

⁴⁵ R:A:I:38-40(¶¶84-87); R:A:IV:33-35(¶¶76-78).

⁴⁶ *Id.* Google and Facebook could know a woman searched about being "pregnant" before she told her spouse or partner she was pregnant.

Find-a-Doctor Queries. Defendants’ websites have “Find a Doctor” features, permitting consumers to request information about doctors based on specialties, location, gender, and language.⁴⁷ For example, a consumer might request from BIDMC a female OB/GYN doctor within five miles of zip code 02210. When a consumer made this request, AdTech transmitted to Google and Facebook the precise attributes of a doctor the consumer requested.⁴⁸

Bill Payments. Defendants’ websites contain a webpage where patients can pay their bills. When a patient communicated to Defendants that they wished to make a payment, hidden code transmitted to Google and Facebook that request, confirming to Google and Facebook the individual’s status as a patient, information highly valuable to those companies’ advertising efforts.⁴⁹

Patient Portal Access and Medical Records. Defendants’ websites have “patient portals” through which patients can access their medical records.⁵⁰ Defendants enabled Google and Facebook to eavesdrop on certain communications connected to patient portals, confirming the individual’s patient status to Google and

⁴⁷ R:A:I:41-43(¶¶88-91); R:A:IV:35-37(¶¶79-82).

⁴⁸ *Id.*

⁴⁹ R:A:I:46-49(¶¶96-100); R:A:IV:43-45(¶¶89-91).

⁵⁰ R:A:I:50(¶101); R:A:IV:45(¶92).

Facebook.⁵¹ AdTech on NEBH's patient portal also transmitted the patient's doctor's name to Google and Facebook.⁵²

In summary, Defendants' interactive websites are designed for patient communications, serving the same communicative function a call to the doctor accomplished in the pre-internet age.

Summary of Argument

Four Superior Court justices have separately reached the same conclusion. Applying the MWA's plain terms and an established body of caselaw, each concluded that the **secret** use of AdTech that enabled social media and technology companies to eavesdrop on website communications stated a claim under the MWA.⁵³ No court has ruled to the contrary.

The Superior Court decisions affirming AdTech wiretap claims, including the two on appeal, align with a wealth of case law spanning decades, including a now twenty-year-old landmark First Circuit decision affirming that the secret use of AdTech on websites violates wiretap laws. *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9 (1st Cir. 2003)(reversing dismissal of class wiretap claims relating to AdTech on pharmaceutical websites). *See* pp.31-32, 64-65.

⁵¹ R:A:I:50-51(¶¶101-03).

⁵² R:A:IV:38-43(¶¶83-84).

⁵³ *See* nn.4-5, *supra*.

The Superior Court’s conclusion that the MWA applied to the secret use of AdTech drew upon the MWA’s broad definition of “wire communication”; the MWA’s preamble, which explains that the statute was intended to target the “grave dangers” from the “uncontrolled development and unrestricted use of modern electronic surveillance devices,” G.L. c.272 §99(A); and this Court’s decisions rejecting efforts to limit the MWA to 1960s-era technologies. *Commonwealth v. Moody*, 466 Mass. 196, 209 (2013)(“In light of the broad statutory definitions of the terms ‘wire communication’ and ‘interception,’ the MWA is “broad enough to cover non-oral electronic transmissions”). *See* pp.29-31.

Massachusetts courts have consistently applied the MWA to modern communication technologies, including internet communications. As the Appeals Court reiterated last year, the “Legislature has created [in the MWA] a strong bulwark against secret surveillance,” the MWA “is among the most protective of electronic surveillance statutes in the country,” and it is “adequately designed to deal even with a sophisticated and novel surveillance tool.” *Commonwealth v. Du*, 103 Mass. App. Ct. 469, 481-82 (2023). *See* pp.33-35.

The Superior Court’s conclusion that Plaintiff sufficiently alleges the eavesdropping was secret was correct given Defendants’ above-quoted false statements in their privacy policies and this Court’s decision in *Commonwealth v. Jackson*, 370 Mass. 502, 507 (1976), holding that for an interception to be non-

secret, there must be a “clear and unequivocal objective manifestation[] of knowledge.” *See* pp.38-46.

The Superior Court properly rejected the Defendants’ argument that the use of AdTech is protected under the “telephone equipment” defense because the defense is limited to the use of “telephone equipment” as an incepting device, and Defendants did not use AdTech the ordinary course of business. *See* pp.46-52.

Finally, the Superior Court’s conclusion that Plaintiff has standing under the MWA correctly applied the MWA’s plain terms, which define precisely who has standing, and this Court’s holding in *Pine v. Rust*, 404 Mass. 411, 418 (1989), that no harm in addition to the privacy invasion caused by the interception itself is necessary to confer standing. *See* pp.52-56.

Defendants barely address the MWA’s terms. When they do, Defendants speculate about what the Legislature must have “intended” rather than addressing what the MWA says. Defendants sidestep the MWA’s strong preamble and this Court’s repeated affirmations that the MWA should be construed broadly. *Moody*, 466 Mass. at 208-09. *See* pp. 30, 33, 57. Defendants also disregard the actual legislative history, which makes clear the Legislature, troubled by the grave dangers posed by electronic surveillance, intended to enact a statute strictly protecting our citizens’ privacy from secret eavesdropping using new technologies. *See* pp.36-38.

Defendants additionally misapply the rules of “lenity” and “absurdity,” which Defendants insist should be used to ignore the MWA’s plain terms. Defendants have it backward. When this Court is “called to construe the terms of a statute and its applicability, [it] begin[s] with the statute’s plain language.” *Metcalf v. BSC Grp., Inc.*, 492 Mass. 676, 681 (2023). The Court considers interpretive tools only if the MWA’s terms provide no answer. Here, the statute’s terms answer all questions on appeal. The breadth of the statute and the strict deterrence mechanisms adopted were intentional legislative choices this Court must respect. The Court should not employ “last resort” tools of construction to undermine the intent of the Legislature. *See* pp.56-60, 62-63.

Finally, Defendants grossly exaggerate the consequences of enforcing the MWA’s plain terms to create the hysterical misimpression that these lawsuits threaten all Massachusetts businesses. **The vast majority of Massachusetts businesses that use AdTech do not violate the MWA because they do not use AdTech secretly.** Defendants, by contrast, did not disclose their use of AdTech and falsely represented that they would not share any information with any outside parties.⁵⁴ **Defendants violated the MWA because the interceptions were secret.**

The Third Circuit, responding to similar doomsday scenarios, aptly explained:

So does this mean websites can never use cookies or third-party marketing companies to analyze customer data? Though the

⁵⁴ R:A:VII:66.

Defendants try to convince us about the certainty of any number of “parade of horrors,” the [Pennsylvania wiretap act] is not so unreasonable. It...includes many exceptions from liability. One is the all-party consent exception, under which [there is no liability] when the person being recorded knew...that the conversation was being recorded [due to a] privacy policy [that] sufficiently alert[s] [website users] that [website] communications [are] being sent to a third-party company.

Popa v. Harriet Carter Gifts, Inc., 52 F.4th 121, 132 (3d Cir. 2022). See pp.60-62.

The court below properly applied the MWA’s plain terms, legislative intent, and authority construing the MWA and similar laws. There was no error.

Argument

I. The MWA Applies to Communications Between Consumers and Businesses Through Websites.

Defendants argue that when consumers communicated with healthcare providers through their websites, no “wire communications” occurred. Defs-Br-34-38. The Superior Court properly concluded, applying the MWA’s plain terms and established case law, that Plaintiff alleged a “wire communication.”

A. *The MWA’s Plain Terms (Including Its Preamble) Support the Decisions.*

A “**wire** communication” is “**any** communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception.” G.L. c.272 §99(B)(1).

Incorporating its earlier decision in *Doe v. Boston Children's Hospital*, No. 2384CV00411-BLS-1 (Mass. Super. Ct. Sept. 14, 2023), the Superior Court held that “the plain language of the statute encompasses the electronic activity alleged here.”⁵⁵ The Superior Court held in *Boston Children's Hospital*: “An analysis of legislative intent likewise points to the inclusion of the website interactions here as communications under the statute.”⁵⁶ The Superior Court correctly emphasized that according to the MWA’s preamble (which doubles as a legislative command and proof of legislative intent), the MWA “was enacted ‘to curtail [the] **grave danger[]**,’” posed by “‘the **uncontrolled development** and unrestricted use of **modern surveillance devices**,’ which the Legislature termed a danger ‘to the privacy of all citizens.’”⁵⁷

As the Superior Court observed, this Court “has established that the statute is to be interpreted broadly, and consistent with that principle, has applied it to electronic text messages, a technology that did not exist in 1968.”⁵⁸ The Superior Court concluded: “Online searches for doctors and requests for appointment also did not exist in 1968, but, similar to texting, are the modern equivalent of telephone

⁵⁵ Addendum:74, incorporating Addendum:207.

⁵⁶ Addendum:206.

⁵⁷ *Id.* (quoting G.L. c.272 §99(A)).

⁵⁸ Addendum:206-07 (citing *Moody*, 466 Mass. at 209).

inquiries and conversations with doctors' offices that would have occurred then. As such, they are protected under the statute."⁵⁹

1. The MWA Is Not Limited to Communications Between Individuals.

Defendants argue the word “communication” is limited to communications “between individuals.” Defs-Br-35, n.54. Nothing in the statutory language supports this construction. After considering the common definition of communication—“the imparting or interchange of thoughts, opinions, or information by speech, writing, or signs”—the Superior Court correctly held: “Nothing in this stated intent or in the remaining statutory language limits its reach to human-to-human” communication.⁶⁰ *See Garcia v. Steele*, 492 Mass. 322, 326 (2023)(“words will be interpreted as taking their ordinary, contemporary, common meaning”).

Defendants cite no authority construing the MWA or any wiretap law as limited to communications between individuals. In construing other wiretap acts, courts have held that communications can be between a natural person and an entity or its website. *Revitch v. New Moosejaw, LLC*, 2019 U.S. Dist. LEXIS 186955, *2-3 (N.D. Cal. Oct. 23, 2019)(requests and responses between customer and retailer—whether online or over the phone—are communications); *Doe I v. Sutter Health*,

⁵⁹ Addendum:207.

⁶⁰ Addendum:206.

Case No. 34-2019-00258072 (Cal. Cnty. Ct. June 9, 2022)(communication may be “between a natural person and an entity or technology created by other natural persons”).⁶¹

Thus, myriad courts have sustained wiretap claims for intercepting communications between website users and corporate websites. *Popa*, 52 F.4th 121; *In re Facebook Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020); *Joffe v. Google, Inc.*, 746 F.3d 920 (9th Cir. 2013); *Pharmatrak*, 329 F.3d 9; *Price v. Carnival Corp.*, 2024 U.S. Dist. LEXIS 10175 (S.D. Cal. Jan. 19, 2024); *Balletto v. Am. Honda Motor Co.*, 2024 U.S. Dist. LEXIS 25150 (N.D. Cal. Feb. 13, 2024); *In re Grp. Health Plan Litig.*, 2023 U.S. Dist. LEXIS 227218 (D. Minn. Dec. 21, 2023); *Vonbergen v. Liberty Mut. Ins. Co.*, 2023 U.S. Dist. LEXIS 220178 (E.D. Pa. Dec. 11, 2023); *Cousin v. Sharp Healthcare*, 2023 U.S. Dist. LEXIS 206638 (S.D. Cal. Nov. 17, 2023); *James v. Walt Disney Co.*, 2023 U.S. Dist. LEXIS 200997 (N.D. Cal. Nov. 8, 2023); *Garcia v. Yeti Coolers, LLC*, 2023 U.S. Dist. LEXIS 158968 (C.D. Cal. Sep. 5, 2023).⁶²

The MWA is not limited to communications between individuals. The Court did not err.

⁶¹ Addendum:334.

⁶² See also Addendum:325-30, 346-66 (collecting additional authorities).

2. The MWA Applies to Modern Electronic Communications.

The MWA was intended to apply to technologies that did not exist when the statute was enacted. The Superior Court correctly held that “the plain language of the statute encompasses the electronic activity” that Plaintiff alleges.⁶³

In *Moody*, this Court reasoned, “[i]n light of the broad statutory definitions of the terms ‘wire communication’ and ‘interception,’” the MWA is “broad enough to cover non-oral electronic transmissions.” 466 Mass. at 208-09. Consistent with *Moody*, the Appeals Court reiterated last year that the MWA is “adequately designed to deal even with a sophisticated and novel surveillance tool.” *Du*, 103 Mass. App. Ct. at 481-82.

Massachusetts courts have long applied the MWA to communication technologies and platforms unimaginable in 1968. In *Rich v. Rich*, 2011 Mass. Super. LEXIS 148, *12-14 (July 8, 2011), the court held the MWA applied to hidden key-logging software that records activities on a computer—similar to the technologies here—reasoning the MWA “is sufficiently broad to include those new technologies.” In *Marquis v. Google Inc.*, SUCV2011-02808-BLS1 (Mass. Super. Ct. Jan. 17, 2012), the court upheld an MWA claim arising from the interception of emails, given

⁶³ Addendum:74, 86.

the MWA’s “definition of ‘wire communications’ is sufficiently broad to include electronic communications.”⁶⁴

Defendants attempt to avoid the MWA’s plain terms by characterizing website communications as “browsing” and “button/link clicks” and insisting website communications are “not...equivalent” to “sending or receipt of any email/text/chat/instant message.” Defs-Br-14, 22-23. Defendants’ characterization of websites as involving only “clicks” and “browsing” ignores the allegations in the complaints about how Defendants’ websites were used to ask for and receive information about doctors and medical conditions, and to schedule appointments, pay bills, and check the patient portal. Statement of Facts, §IV.

Websites have transformed how consumers communicate with businesses. “Today it is common, if not expected, that businesses maintain websites, often with interactive capabilities through which customers can communicate with the businesses.” *Telebrands Corp. v. Altair Instruments, Inc.*, 2019 U.S. Dist. LEXIS 136594, *11 (D.N.J. Aug. 13, 2019). Where, previously, a consumer would obtain information from a business by calling, consumers now obtain the same information via the Internet. When a user visits a webpage, the user requests information from a business (through clicks, searches, or forms), and the business responds (through the

⁶⁴ Addendum:320.

website) with the information requested—no different than a question-and-answer communication via phone, email, or text.

The Superior Court, crediting Plaintiffs’ well-pled fact allegations, aptly described website communications as the “modern equivalent of telephone inquiries and conversations with doctors’ offices that would have occurred” at the time of the MWA’s enactment.⁶⁵

3. Website Communications Occur by “Wire.”

Website communications occur “by the aid of wire, cable, or other like connection,” as the “Internet is an instrumentality” that transmits information “by aid of wire, cable, or other like connection between the points of origin and reception of such transmission.” *United States v. Lyons*, 740 F.3d 702, 716 (1st Cir. 2014)(construing federal law applicable to similarly defined “wire communications” as encompassing website communications).

Defendants argue for the first time on appeal that the word “wire” must be limited to telephone and telegraph wires. Defs-Br-35. Defendants’ argument is

⁶⁵ Addendum:207. The Superior Court properly rejected Defendants’ argument that AdTech is comparable to GPS devices that only “record physical movements.” Defs-Br-36, n.56 (citing *Commonwealth v. Connolly*, 454 Mass. 808 (2009)); Addendum:207 n.2 (rejecting *Connolly*’s relevance). *Connolly* noted that “[d]ata from GPS devices...does not fall within the language of the wiretap statute,” 454 Mass. at 825, as there were no facts in *Connolly* suggesting a GPS device intercepted or even could intercept any oral or wire communication to which the criminal defendant there was a party (that is not what GPS devices do).

foreclosed by this Court’s holding in *Moody* that the MWA is “broad enough to cover non-oral electronic transmissions.” 466 Mass. at 208 (applying MWA to text messages). Defendants offer no reason for this Court to discard this precedent.

The Superior Court correctly held that consumers’ communications with Defendants through their websites are “wire communications.”

B. *Legislative History Confirms the MWA Applies to Emerging Technologies.*

With no sound argument on the MWA’s plain terms, Defendants resort to amorphous assertions about legislative intent. Defendants argue the MWA was designed with a “clear intent to restrict people from secretly listening to or recording other peoples’ interpersonal messages and conversations.” Defs-Br-19. Defendants cite **nothing** to support this assertion.

The MWA’s preamble—the most direct evidence of legislative intent—supports the Superior Court’s conclusion that the MWA was intended to protect Massachusetts citizens from the “grave dangers” of “modern electronic surveillance devices.” G.L. c.272 §99(A). Significantly, the Legislature’s thoughtful and instructive preamble was not borrowed from a uniform or other wiretap law.

Legislative history further bolsters the Decisions. The Legislature rewrote the MWA in 1968.⁶⁶ The MWA’s predecessor statute was limited to devices used to

⁶⁶ 1968 Mass. Acts. c.738 (Addendum:119).

“overhear...spoken words.”⁶⁷ The focus of the predecessor act was “eavesdropping,”⁶⁸ a focus that would continue to animate the Legislature when it expanded the MWA beyond “spoken words” to “wire communications.”

The process leading to the 1968 amendment began when the Legislature formed a Special Commission on Electronic Eavesdropping (the “Commission”) to investigate “laws relative to eavesdropping and the use of electronic recording devices, wireless taps or electronic taps...or similar devices or arrangements...with a view to strengthening the laws relative to eavesdropping.”⁶⁹

The Commission’s Interim Report in April 1967 articulated a concern about emerging “future” technologies that facilitate “electronic eavesdropping” and the need to deter that conduct:

Clearly, the future is frightening, and beyond the layman’s comprehension. Science has a double-edged sword, which can work for the betterment of mankind or for its destruction, depending on how the scientific tools developed are used.... **Even the strictest enforcement of the most all-encompassing statute will not put a stop to electronic eavesdropping. We can only hope to lessen the incidence of eavesdropping....**⁷⁰

The Commission’s October 1967 Interim Report further illuminated the Legislature’s motivations, concluding that a “minimum remedy...should be

⁶⁷ 1920 Mass. Acts c.558 (Addendum:117).

⁶⁸ *Id.*

⁶⁹ S. Bill. 201 (Mass. 1964)(Addendum:132).

⁷⁰ S. Rep. 1198 (Mass. 1967)(Addendum:143)

available to all citizens due to the tremendous expansion of the problem created by...**new technology**.”⁷¹

The Commission’s Final Report articulated unambiguously that the new MWA was designed to be a stringent, pro-privacy statute that would “**strictly forbid** electronic eavesdropping or wiretapping by members of the public.”⁷²

The legislative history confirms the Legislature fully intended to enact a statute strictly limiting the secret use of new and future technologies that secretly intercept wire communications.

II. Plaintiff Alleges Secret Interceptions.

The MWA prohibits secret interceptions of wire communications. G.L. c.272 §99(B)(4). Recognizing the Legislature’s intent to address the “serious threat [to] the privacy of all citizens” posed by “electronic surveillance devices,” Defendants must prove Plaintiff’s “actual knowledge” of an interception to establish an interception was not secret. *Jackson*, 370 Mass. at 507. The “actual knowledge” requirement “impose[s] [a] more stringent restriction[] on the use of electronic surveillance devices” than in other states, requiring a “clear and unequivocal objective manifestation[] of knowledge.” *Id.* at 506-07.

⁷¹ S. Rep. 1469 (Mass. 1967)(Addendum:157)

⁷² S. Rep. 1132 (Mass. 1968)(Addendum:173).

A. Secrecy Cannot Be Decided on a Motion to Dismiss.

The Superior Court properly concluded that the MWA's secrecy element presents a fact question turning on the content and presentation of website disclosures.⁷³ *Morrison v. Lennett*, 415 Mass. 857, 859 (1993); *Braun v. Phila. Inquirer, LLC*, 2023 U.S. Dist. LEXIS 202528, *15 (E.D. Pa. Nov. 13, 2023).

Defendants' insistence that "secrecy" could be resolved in their favor on the pleadings is truly remarkable, considering their brazenly false disclosures. Defendants promised their website users their communications were "**not shared with any other organizations**" and that Defendants "**will not share any information we receive [from consumers] with any outside parties.**" They then secretly did precisely what they promised not to do.⁷⁴

Defendants point to their disclosure: "We and our Third-Party Service Provider collect and save the default information customarily logged by world wide web server software." Defs-Br-15. They argue this disclosure put users on notice of third-party eavesdropping. Defs-Br-44-45. Bluntly, this argument is preposterous considering Defendants' blatantly false disclosures, which told website users information was not "shared with any other organizations" or "any outside parties."

⁷³ Addendum:70-71, 74-75.

⁷⁴ R:A:I:14(¶23); R:A:IV:15(¶23).

Defendants' disclosures did not simply "lack specificity," Defs-Br-44; rather, they were lies.

Undeterred by their overt deception, Defendants argue, despite Plaintiffs' contrary allegations (Statement of Facts §III), that Plaintiff had actual knowledge that Google and Facebook eavesdropped on her communications. Defs-Br-39-40. The Superior Court correctly refused to adopt Defendants' factual contentions. This Court must refuse to do so as well. *See Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 620-21 (N.D. Cal. Mar. 17, 2021) ("disclosures must have only one plausible interpretation" for pleadings-stage dismissal).

B. *Any Knowledge of Recording By Defendants' Web Servers Does Not Equate to Knowledge of Third-Party Eavesdropping.*

Defendants say, "it is common knowledge" that communications through websites are "recorded" by servers, and anyone who communicates over the internet "is on notice of inherent recording." Defs-Br-43. Defendants conflate recording by a party to a communication with the interception of the communication by a third party. Defendants' premise is that knowledge is all-or-nothing—knowledge of any "recording" by a party to a communication should be deemed knowledge of all interceptions by eavesdropping third parties. That is not the law.

The Appeals Court in *Du* addressed this issue head-on, construing the MWA's plain terms to find that a "remote...hearing...of the transmission" is an interception distinct from a "recording" made by a participant to the communication, given that

a “[a] single communication can be intercepted at more than one point in time or place.” 103 Mass. App. Ct. at 478-79. *Du* confirmed that secrecy must be evaluated separately as to each interception. *Id.*⁷⁵

Du is no outlier; it aligns with consistent authority construing wiretap statutes. Given the “strong [legislative] purpose to protect individual privacy [and] strictly limit[] the occasions on which interception may lawfully take place,” consent “is not necessarily an all-or-nothing proposition; it can be limited.” *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 581-82 (11th Cir. 1983). “A party may consent to the interception of only part of a communication.... Thus, a reviewing court must inquire into the dimensions of the consent and then ascertain whether the interception exceeded those boundaries.” *Pharmatrak.*, 329 F.3d at 19.⁷⁶

⁷⁵ Defendants attempt to downplay *Du* by claiming “[t]he *Du* court considered not a single prior Wiretap Act precedent,” pointing to this Court’s decisions in *Rainey*, *Morris*, and *Jackson*. Defs-Br-42, n.78. **This assertion is spectacularly wrong.** The Appeals Court discussed in-depth each of those decisions and others construing the MWA. 103 Mass. App. Ct. at 473-77. Defendants fault *Du* for not discussing *Curtatone*, but as explained below, *Curtatone* and *Du* do not conflict because *Curtatone* did not involve third-party eavesdropping.

⁷⁶ These rulings align with the Commission’s concerns: “[F]reedom includes the right to decide for himself whether his words shall be accessible solely to his conversation partner, to a particular group, or to the public....” S. Rep. 1132 (Mass. 1968)(Addendum:179)(quotations omitted).

In *In re Facebook, Inc.*, the court rejected a similar argument by Facebook, holding that knowledge that recipients may record a communication does not amount to consent to third parties intercepting the same communication:

[A]ccording to Facebook,...if people use social media to communicate sensitive information with a limited number of friends, they have no right to complain of a privacy violation if the social media company turns around and shares that information with a virtually unlimited audience. **Facebook’s argument could not be more wrong.** When you share sensitive information with a **limited audience...**, **you retain privacy rights and can sue someone for violating them...**

402 F. Supp. 3d 767, 776 (N.D. Cal. 2019); *In re Google Inc. Gmail Litig.*, 2013 U.S. Dist. LEXIS 172784, *55–56 (N.D. Cal. Sept. 26, 2013)(“no case that stands for the proposition that users who send emails impliedly consent to interception and use of their communications by **third parties other than the intended recipient of the email**”).

Accepting Defendants’ arguments would gut the MWA and render it inapplicable to any modern electronic communication since the recipient’s device or server almost always records such communications. Defendants’ argument is irreconcilable with this Court’s decision in *Moody*, which applied MWA to text messages, another form of communication “inherently recorded” on the recipient’s device. Defendants concede the MWA applies to “email/text/chat/instant message or equivalent” communications, Defs-Br-9, but ignore that the MWA would not apply

to any of these forms of communications if this Court held the secret interception by third parties of “inherently recorded” communications does not violate the MWA.

Defendants rely heavily on *Curtatone v. Barstool Sports, Inc.*, 487 Mass. 655 (2021) to argue Plaintiff’s supposed knowledge that Defendants’ web servers keep logs counts as knowledge of third-party eavesdropping. Defs-Br-39-41. *Curtatone* contains no such holding. It stands for a narrow proposition: one party’s consent to the other party’s recording is valid, although the consenting party was deceived about the other party’s identity. *Id.* at 659.

This Court’s statement in *Curtatone* that the “act of hearing or recording is that which must be done secretly” must be considered in context. This Court contrasted the facts before it with “electronic eavesdropping,” noting the “legislative intent, apparent both in the legislative history of the act and the act itself, concerns limiting **‘electronic eavesdropping,’ circumstances unlike those at issue here....**” *Id.* at 659. In contrast, Plaintiff here claims that Defendants facilitated “electronic eavesdropping,” the precise conduct absent in and unaddressed by *Curtatone*. The Superior Court properly recognized Plaintiff’s claims involved “third-party eavesdropping...by undisclosed, contemporaneous third parties,” which “differs from *Curtatone*..., which involved a consented-to recorded conversation between two people only.”⁷⁷

⁷⁷ Addendum:75 n.7, 87 n.7.

Defendants cite *Commonwealth v. Morris*, 492 Mass. 498 (2023), and *Commonwealth v. Rainey*, 491 Mass. 632 (2023) for this same argument, Defs-Br-41-42, but both cases are distinguishable for the same reason: both involved recording by a party to the communication; neither involved undisclosed third-party eavesdropping. *Morris*, 492 Mass. at 501-02; *Rainey*, 491 Mass. at 633-34.⁷⁸

Courts in other jurisdictions that have held, like *Curtatone*, that deception about identity does not violate the wiretap act have confirmed that third-party eavesdropping is different and actionable. For example, Pennsylvania’s wiretap law has been construed, like *Curtatone*, to exclude situations where one party to a communication deceived another about his identity. *Commonwealth v. Cruttenden*, 58 A.3d 95, 96 (Pa. 2012); *Commonwealth v. Proetto*, 771 A.2d 823, 826-27, 831-32 (Pa. Super. Ct. 2000).

Businesses accused of wiretap violations by using AdTech have tried to invoke those decisions to argue no violation occurred because website users knew of recording **in general**. Courts consistently reject these arguments, holding that even if a consumer “may have consented to [the website server] recording her personal information,” plaintiff “has plausibly alleged she was not aware [the website owner] had procured an **undisclosed third party** to intercept that

⁷⁸ Defendants’ other authorities (cited at Defs-Br-39 n.63, Defs-Br-43 n.79) likewise involved no third-party eavesdropping.

information too.” *Vonberger*, 2023 U.S. Dist. LEXIS 220178, *40-41. *Proetto* does not stand “for the proposition that users who send emails impliedly consent to interceptions and use of their communications by third-parties other than the intended recipient of the email.” *Google-Gmail*, 2013 U.S. Dist. LEXIS 172784, *56; *Price*, 2024 U.S. Dist. LEXIS 10175, *8-9 (same); *Popa*, 54 F.4th at 126-27.

Curtatone provides no license for third-party eavesdropping.

C. *Defendants Ignore the Difference Between Third-Party Eavesdropping and Subsequent Sharing.*

Contrary to Defendants’ argument, Defs-Br-43-44, the Decisions would not require the police officers in *Morris* and *Rainey* or the reporter in *Curtatone* to disclose that recordings may later “be shared” with other parties, given the MWA’s distinction between third-party eavesdropping as communications happen (which the MWA prohibits) and later sharing of a completed communication (which the MWA does not).

Defendants’ insistence (Defs-Br-30 n.41) that there is no difference between eavesdropping and later “sharing” of completed communications ignores that the MWA draws precisely such a distinction. The California Supreme Court underscored the significance of this distinction, common among wiretap laws:

While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical

device.... [S]ecret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements.

Ribs v. Clark, 696 P.2d 637, 640-41 (Cal. 1985).

The Superior Court’s pleadings-stage decision that the complaints adequately allege secrecy was correct.

III. The Telephone Equipment Defense Does Not Apply.

The MWA exempts from the definition of an “intercepting device,” “any telephone or telegraph instrument, equipment, facility, or a component thereof...being used by the subscriber or user in the ordinary course of its business.” G.L. c.272 §99(B)(7). The defense requires two factual conclusions—that the interception was accomplished through “telephone or telegraph” equipment and that it was in the “ordinary course of [Defendants’] business.” Defendants establish neither element. The Superior Court correctly held the defense did not apply: “Setting aside whether internet tracking occurs in the ordinary course of BIDMC’s business, the electronic software-based internet tracking technology at issue here plainly is not...telephone or telegraph equipment.”⁷⁹

A. AdTech Is Not Telephone Equipment.

AdTech is not “telephone equipment”; Defendants do not claim otherwise. Instead, Defendants argue that if the Court construes “intercepting device” to include

⁷⁹ Addendum:76, 88.

“21st-century website technology,” AdTech should be construed to be “telephone equipment.” Defs-Br-47-48. Defendants cite no case accepting this argument.

Defendants’ simplistic argument ignores the MWA’s plain terms. The MWA regulates “intercepting devices,” defined broadly to include “**any device** or apparatus which is **capable of transmitting**, receiving, amplifying, or recording a **wire...communication.**” G.L. c.272 §99(B)(3). In contrast, the telephone equipment defense is narrow and exempts only “telephone or telegraph instrument, equipment, facility, or a component thereof...” *Id.*

This Court has held “telephone equipment does **not** include eavesdropping devices external and extraneous to regular telephone devices.” *O’Sullivan v. NYNEX Corp.*, 426 Mass. 261, 265 (1997). In reaching that conclusion, this Court relied upon the First Circuit’s decision in *Williams v. Poulos*, 11 F.3d 271, 280 (1st Cir. 1993), which construed the same language in federal wiretap law and confirmed the defense is inapplicable to a system that monitors telephone equipment but is not itself telephone equipment.

Defendants protest that the Appeals Court once construed the telephone equipment defense flexibly, and therefore, a departure from the MWA’s requirements is warranted, pointing to *Dillon v. Mass. Bay Transp. Auth.*, 49 Mass. App. Ct. 309, 314 (2000). Defs-Br-27-28, 46-47. In *Dillon*, the court allowed the defense even where telephone equipment was obtained from a source other than a telephone

company. The *Dillon* court reasoned that “a great variety of equipment and services earlier generally provided by a telephone company” had come to be provided “from numerous non-telephone company sources.” *Id.* But nothing in *Dillon* expanded the exemption beyond telephone equipment.

In *Alves*, the Superior Court rejected the same argument that would “depart even more dramatically from the language of [the MWA than *Dillon*] to include [AdTech with] characteristics quite different from telephone equipment.” 2023 Mass. Super. LEXIS 59, *10–13; *see also Commonwealth v. Diego*, 119 A.3d 370, 375-76 (Pa. Super. Ct. 2015)(declining to “radically expand the definition of ‘telephone’ because the “argument [taken] to its logical conclusions [would mean] any modern computer, in tablet form or otherwise, would have to be considered a telephone under the Wiretap Act when it is used to transmit or receive an electronic communication.”).

Without a sound textual argument, Defendants resort again to a citation-free “legislative intent” argument. Defs-Br-45. The legislative history affirms the limitation of the defense to “telephone equipment” was no accident. An early draft of the MWA would have afforded the defense to “the use by...businesses of **any device** used for security or business purposes.”⁸⁰ The Legislature rejected the

⁸⁰ H. Bill 1435 (Mass. 1967)(Addendum:134).

broader “any device” defense, limiting it instead to “telephone or telegraph instrument, equipment, facility, or a component thereof.” G.L. c.272 § 99(B)(3).

Defendants say “[t]here is no common-sense...explanation” for why the Legislature limited the defense to “telephone equipment.” Defs-Br-49-50. There is. The Commission, as part of its consideration of new wiretap laws, heard testimony from New England Telephone and Telegraph Company about the necessity of “service observation practices” for “quality control,” concluding “it believes the company is sincere in its statement that service observation is essential to the proper functioning of the telephone system.”⁸¹ The Commission was aware of the risk that telephone companies or their customers might be found liable for using standard telephone equipment, so the Legislature created an exception. Defendants’ effort to rewrite this limited defense must be rejected.

Finally, Defendants do not explain why AdTech is the modern analog of telephone equipment. Even if the defense were construed to include modern communications equipment, AdTech that monitors website communications would not be excluded because it is extraneous to website functionality, R:A:I:52(¶¶105-06); R:A:IV:47(¶¶95-96)), just like the extraneous monitoring system in *Williams*. 11 F.3d at 280; *Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 740 (4th Cir.

⁸¹ S. Rep. 1198 (Mass. 1968)(Addendum:144-53).

1994)(telephone voice logger is not telephone equipment). At a minimum, this argument implicates factual issues that cannot be decided without a factual record.

B. *Defendants Did Not Use AdTech in the Ordinary Course of Business.*

The defense is also unavailable unless Defendants' secret use of AdTech was in the ordinary course of their business. This fact question provides an alternative basis for affirming the denial of motions to dismiss.

“[I]n light of the statutory purpose of protection from invasions of privacy, neither the concept of legitimate business purpose nor ‘ordinary course of business’ can ‘be expanded to mean anything that interests a company.’” *Crosland v. Horgan*, 401 Mass. 271, 275 (1987)(quoting *Watkins*, 704 F.2d at 582); *Google-Gmail*, 2013 U.S. Dist. LEXIS 172784, *36 (legislature “did not intend to allow [companies] unlimited leeway to engage in any interception that would benefit their business models” as wiretap law would become “superfluous if the ordinary course of business exception were [so] broad.”).

Plaintiff alleges that Defendants' aiding of technology and media companies' secret interception of website communications was not instrumental to Defendants' business because even if operating websites was within the ordinary course of their business, the secret use of AdTech is not essential to the functioning of Defendants' websites.⁸² This alone requires this Court to reject, at the pleadings stage,

⁸² R:A:I:52(¶¶105-06); R:A:IV:47(¶¶95-96).

Defendants’ argument that the secret deployment of AdTech was in the ordinary course of their business. *Sanders*, 38 F.3d at 741-42 (“no business reason asserted for the decision not to notify [the parties to the communication] of the use of the voice logger.”); *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1071 (N.D. Cal. 2021)(ordinary course of business defense inapplicable because “Google has not shown that its [AdTech] facilitates or is incidental to the transmission of the communication at issue”). Notably, both Google and Facebook directed Defendants to make such disclosures.⁸³

Moreover, when a company violates its own policies, its conduct is not in the “ordinary course of [its] business.” *Brown*, 525 F. Supp. at 1701; *Berry v. Funk*, 146 F.3d 1003, 1009-10 (D.C. Cir. 1998)(defendant’s position was “fatally undermined by the [its] guidelines...which must be regarded as the ordinary course of business for the [defendant]”). Defendants’ policies promised they would not share website communications with “any outside parties.”⁸⁴ Defendants’ policies “fatally

⁸³ <https://www.facebook.com/legal/terms/businessstools> (websites must “represent and warrant that [they] have provided **robust and sufficiently prominent notice to users** regarding [Meta Pixel],” including, a **clear and prominent notice on each web page where our pixels are used** that links to a clear explanation...**that third parties, including Meta, may...collect or receive information from your websites...and use that information to...target and deliver ads**”); <https://marketingplatform.google.com/about/analytics/terms/us/> (“**You must disclose [to users] the use of Google Analytics, and how it collects and processes data.**”).

⁸⁴ R:A:I:14(¶23); R:A:IV:15(¶23).

undermine” their position that secretly enabling third-party eavesdropping of consumers’ communications is part of their ordinary course of business.

IV. The MWA’s Plain Terms Confer Standing.

The MWA’s civil remedy provision provides:

Any aggrieved person whose oral or wire communications were intercepted, disclosed, or used except as permitted or authorized by this section or whose personal or property interests or privacy were violated by means of an interception except as permitted or authorized by this section shall have a civil cause of action against any person who so intercepts, discloses or uses such communications....

G.L. c.272 §99(Q). The same section mandates that an “aggrieved person” “**shall** be entitled to recover” liquidated damages plus other remedies. *Id.* An “aggrieved person” is “any individual who was a party to an intercepted wire or oral communication.” G.L. c.272 §99(B)(6). Consistent with the MWA’s plain terms, this Court has affirmed that statutory damages may be awarded to any individual who was a party to an intercepted wire communication (i.e., an aggrieved person) “even though...no actual harm has been incurred.” *Pine*, 404 Mass. at 414-16.

Defendants essentially ask the Court to overrule *Pine*, ignore the MWA’s express terms, and by **judicial fiat**, repeal so much of the MWA as provides relief unless Plaintiff proves some harm in addition to the injury the Legislature defined in the MWA. But this Court “will not read into the statute a provision which the Legislature did not see fit to put there.” *Chin v. Merriot*, 470 Mass. 527, 537 (2015).

Article III of the U.S. Constitution limits Congress’s ability to confer standing in federal courts. *Spokeo Inc. v. Robins*, 578 U.S. 330, 339 (2016). In contrast, this Court has long held that the Massachusetts Legislature has the power and discretion to define injuries and confer standing as it sees fit:

The State has power to confer jurisdiction upon its courts to consider suits at the instance of those who have very remote and even no personal interest in the subject matter. . . . A stated number of citizens or a single individual may be clothed by the Legislature with authority to invoke the aid of courts in the suppression of violations of law.

Fournier v. Troianello, 332 Mass. 636, 639 (1955). “To determine whether [a plaintiff] has standing, [Massachusetts courts] look to the statute itself.” *Phone Recovery Servs., LLC v. Verizon of New England, Inc.*, 480 Mass. 224, 227 (2018). When a plaintiff “meets the plain reading of an ‘aggrieved person under the statute[,] **we need not look further.**” *Johnson v. Frei*, 93 Mass. App. Ct. 1111, 1115 (2018).⁸⁵

The Appeals Court recently rejected the same argument Defendants make—that principles of “standing” constrain the power of the Massachusetts Legislature to define injuries. In *Kenn v. Eascare, LLC*, 103 Mass. App. Ct. 643 (2024), a federal court remanded to state court a claim under the federal Fair Credit Reporting Act (“FCRA”) after finding the federal court lacked Article III jurisdiction because the plaintiff alleged an FCRA disclosure violation but no separate injury. *Id.* at 649. The

⁸⁵ Although Defendants cite cases (Defs-Br-52) where Massachusetts courts borrowed language from federal case law to define an “injury,” those cases did not involve state statutes, like the MWA, that clearly define who has a right to sue.

defendant sought dismissal in state court, arguing the federal court's finding of no injury mandated dismissal by the Massachusetts state court as well. The Appeals Court disagreed, explaining, "[t]he plaintiff's lack of standing in Federal court is not dispositive of the question of her standing in State court. Because they are not bound by art. III, State courts remain free to define their own jurisdictional limits." *Id.* at 649. The court held: "The plaintiff alleged the violation of her legal rights under FCRA, which if proved, entitles her to damages under FCRA," and those allegations were sufficient to confer standing. *Id.* at 652.

Kenn follows established precedent from this Court, confirming Article III does not constrain Massachusetts courts. *Weld v. Glaxo Wellcome, Inc.*, 434 Mass. 81, 88 (2001)("State courts...are not burdened by these same [Article III] jurisdictional concerns...."); *LaChance v. Comm'r of Corr.*, 475 Mass. 757, 771 n.14 (2016)("[B]ecause art. III does not apply to State courts, State courts remain free to define their own jurisdictional limits....").

Defendants attempt to equate the MWA to Chapter 93A to argue this Court should graft a separate-injury requirement onto the MWA. As Defendants admit (Defs-Br-55), Chapter 93A expressly requires a plaintiff to allege she "has been injured" by a violation to invoke the statute's remedies. G.L. c.93A §9. The MWA does not. This Court must respect the Legislature's choice to impose different requirements for different claims. *Lyon v. Triram Corp.*, 2004 Mass. Super. LEXIS

496, *10-11 (Oct. 29, 2004)(“**unlike the wiretap statute**, G.L. c.93A, §11 requires that the plaintiff demonstrate that he suffered loss of money or property, real or personal, in order to recover monetary damages.”).

Kenn also rejected the argument made here—that because Massachusetts courts apply a separate-injury requirement for c.93A claims, that requirement must apply to all statutory claims:

The interpretation of the “injury” requirement of c. 93A is based on the language and history of the statute. [N]othing in the line of cases construing c. 93A’s injury requirement suggests that our Legislature would not be permitted to create a statutory scheme providing compensation for plaintiffs whose legal rights are infringed, but who are not identifiably injured thereby.

103 Mass. App. Ct. 653. The same rationale applies to the MWA; there is no basis to impose a separate-injury requirement the Legislature chose not to require.

Defendants insist it made no sense for the Legislature to impose more stringent standing requirements on a c.93A claimant than for an MWA claimant, Defs-Br-55, but it is not the role of this Court to second-guess such legislative decisions. In any event, the Legislature’s decision is explained by the MWA’s preamble, reflecting its concern about the “**grave dangers**” posed by ““the **uncontrolled development** and unrestricted use of **modern electronic surveillance devices**,” G.L. c.272 §99(A), stark language with no analog in c.93A.

Despite Defendants’ citation-free insistence that the Legislature “clearly intended” to require an additional “injury,” Defs-Br-55, the MWA’s drafting history

confirms the Legislature made no mistake requiring judicial correction. An early draft of the MWA provided: “Any party to conversation which is eavesdropped upon in violation of Part A, and **who has been damaged due to such violation**, may sue the violator....”⁸⁶ Another bill similarly required that the “person [was] damaged by a violation” of the MWA before being eligible for statutory damages.⁸⁷ However, in the enacted MWA, the Legislature dropped the requirement from the earlier drafts that a plaintiff be “damaged” and instead allowed any “aggrieved person whose oral or wire communications were intercepted,” G.L. c.272 §99(Q), to recover statutory damages. This Court should respect and enforce that choice. Plaintiff, an aggrieved person, has standing under the MWA.

V. The Court Should Reject Defendants’ Invitations to Disregard the MWA’s Plain Terms.

With no real argument that the Superior Court misapplied the MWA’s plain terms or that its rulings contradicted actual legislative intent, Defendants rely on the doctrines of lenity and absurdity to ask this Court to overturn clear legislative commands. Neither doctrine applies.

A. The Rule of Lenity Cannot Be Used to Negate the MWA’s Plain Terms.

Defendants argue the rule of lenity operates as a trump card, enabling the Court to disregard the MWA’s plain terms and legislative intent. Defs-Br-20-26.

⁸⁶ H. Bill 1435 (Mass. 1967)(Addendum:134).

⁸⁷ H. Bill 3665 (Mass. 1968)(Addendum:167).

Defendants cite no case applying the rule of lenity to construe the MWA narrowly. The doctrine is inapplicable for several reasons.

First, the rule has no application where “legislative intent...is clear.” *Cook v. Patient Edu, LLC*, 465 Mass. 548, 555-56 (2013). Its application here would be inconsistent with this Court’s directive that the Legislature intended the MWA to be construed broadly. *Moody*, 466 Mass. at 209; *Commonwealth v. Hyde*, 434 Mass. 594, 603 (2001).

Second, the rule only applies if “there is a grievous ambiguity or uncertainty in the statute.” *Muscarello v. United States*, 524 U.S. 125, 138-39 (1998). The rule of lenity is “a rule of last resort, [applied] only when none of the other canons of statutory interpretation is capable of resolving the statute’s meaning.” *Adams v. Holder*, 692 F.3d 91, 107 (2d Cir. 2012); *Commonwealth v. Maloney*, 447 Mass. 577, 584-85 (2006)(“[T]he rule of lenity ‘is a guide for resolving ambiguity, rather than a rigid requirement that we interpret each statute in the manner most favorable to defendants.’”). There is no ambiguity in the MWA.

Third, courts consistently refuse to apply lenity to wiretap laws, given such laws’ plain terms and clear legislative intent. The Ninth Circuit rejected Google’s reliance on the rule in a wiretap case, explaining: “We do not resort to the rule of lenity every time a difficult question of statutory interpretation arises. Rather, the rule of lenity only applies if, after considering text, structure, history, and purpose,

there remains a ‘grievous ambiguity or uncertainty in the statute.’” *Joffe*, 746 F.3d at 935-36. This Court should decline to apply the rule of lenity to adopt an interpretation which is inconsistent with “the purpose of the statute, i.e., to ‘prohibit unauthorized artificial interception of communication in an era of changing technologies.’” *James*, 2023 U.S. Dist. LEXIS 200997, *40.

Defendants do not use the rule of lenity as a “last resort” but instead as a first principle, which they contend should control the Court’s interpretations on each element of Plaintiff’s claims. That is not a proper application of lenity when there is no ambiguity, much less a “grievous ambiguity” that cannot be resolved by other interpretive tools. *Zaratzian v. Abadir*, 2014 U.S. Dist. LEXIS 129616, *19-20 (S.D.N.Y. 2014)(rejecting “last resort” rule of lenity “[b]ecause the meaning of the applicable provisions of the Wiretap Act are capable of being resolved” without it).

Finally, the elements required to prove criminal and civil liability under the MWA differ. The MWA’s criminal provisions each require proof of either a “willful” violation or specific intent to commit a violation. G.L. c.272 §99(C). The civil cause of action, G.L. c.272 §99(Q), omits any such requirement. *Pine*, 404 Mass. at 413-14. The differences between the MWA’s civil and criminal provisions provide an additional reason not to distort the MWA’s plain terms by the rule of lenity. *United States v. W. R. Grace*, 504 F.3d 745, 755-56 (9th Cir. 2007)(“rule of lenity” inapplicable since the civil and criminal regimes employed “different definitions”);

GlobalTranz Enters. Inc. v. Shipper's Choice Global LLC, 2017 U.S. Dist. LEXIS 234215, *22-24 (D. Ariz. 2017)(same).

B. *Applying the MWA to Defendants' Conduct Is Consistent with Legislative Intent and Not Absurd.*

Defendants argue that applying the MWA to their secret use of AdTech leads to absurd results. Defs-Br-26-33. “The absurdity canon isn’t a license for [a court] to disregard statutory text where it conflicts with [its] policy preferences.” *In re Hokulani Square, Inc.*, 776 F.3d 1083, 1088 (9th Cir. 2015). Its application “is confined to situations “where it is quite impossible that [the legislature] could have intended the result.” *Id.*; *Kelley v. Albuquerque*, 375 F. Supp. 2d 1183, 1223 (D.N.M. 2004)(“‘absurdity’ exception to the plain language rule is a tool to be used to carry out [legislative] intent—not to override it.”). As this Court has held, for an interpretation to be “absurd,” it must result in an application that “the drafters could not have intended.” *Commonwealth v. Brown*, 479 Mass. 600, 606 (2018); *Commonwealth v. Peterson*, 476 Mass. 163, 168-70 (2017).

With no evidence that the application of the MWA to Defendants’ conduct conflicts with the Legislature’s intent, Defendants’ argument veers towards hyperbole. Defendants hyperventilate that application of the MWA here “would make presumptive criminals of thousands of Massachusetts residents.” Defs-Br-25. Not so. To be actionable under the MWA’s civil provisions, “an interception need not rise to the level of criminal conduct covered by the penal provisions of the law.”

Pine, 404 Mass. at 413-14. Moreover, Plaintiffs' claims do not imply that installing or logging communications with AdTech is "*prima facie* evidence of guilt of [a] **felony** offense." Defs-Br-23(emphasis in original). The MWA limits liability to those who "**secretly** record." G.L. c.272 §99(B)(4). Stated simply: the use of AdTech does not give rise to civil or criminal liability; only the **secret** use of AdTech to enable third-party eavesdropping violates the MWA.

Defendants catastrophize that the application of the MWA here would threaten all Massachusetts businesses that use AdTech with "crippling civil liability," Defs-Br-17, and imagine "calamitous consequences" will ensue "across all for-profit and non-profit sectors of the Massachusetts economy." Defs-Br-28. Defendants' shrill warnings ring hollow because most websites do not secretly allow third-party interceptions, as Defendants did, and hence do not violate the MWA. *Popa*, 52 F.4th at 132 (rejecting similar arguments about "parade of horrors"). Plaintiff alleges:

[I]f BIDMC wanted to use tracking technologies to optimize its website or its marketing for a website, there is no legitimate or lawful reason for BIDMC (i) to keep secret from its website users the use of these tracking technologies; (ii) to falsely and deceptively claim that BIDMC does not share the communications with others when it does; or (iii) to claim that BIDMC maintains the privacy of those communications when it does not.⁸⁸

Tellingly, Defendants' hand-selected examples of businesses that use AdTech, Defs-Br-29, undermine their calamity argument. Those businesses expressly

⁸⁸ R:A:I:53(¶107); R:A:IV:47(¶97).

disclosed that they allow third parties such as Google and Facebook to collect information about website users to create targeted advertising, and hence did not violate the MWA. For example, the Red Sox website (operated by MLB) discloses:

“We disclose certain data to Social Networks (as defined below) such as Twitter, Facebook, LinkedIn and Snapchat to allow us to target existing users and customers with highly relevant advertising campaigns.”⁸⁹

Other websites Defendants cite have similar disclosures⁹⁰; their operators, therefore, are not exposed to liability under the MWA.

Most healthcare providers disclosed their use of AdTech and have not been sued. For example, South Shore Hospital discloses: “[w]e currently use Google Analytics” and “pixel tags...or other similar technologies” to facilitate “online behavioral advertising” based on “information about your visits to the Site...”⁹¹ Defendants, like most Massachusetts businesses, would not face liability had they disclosed their use of AdTech, as Google and Facebook directed them to do.⁹²

⁸⁹ <https://www.mlb.com/official-information/privacy-policy>.

⁹⁰ Dunkin Donuts: <https://www.dunkindonuts.com/en/privacy-policy> (“Social Media and Technology Integrations”); Museum of Science: <https://mos.org/privacy-policy>; Commonwealth of Massachusetts: <https://www.mass.gov/info-details/massgov-privacy-policy>. A link in the privacy policy (<https://www.mass.gov/info-details/third-party-data-analytic-tools>) provides detailed descriptions about the data analytics tools used on mass.gov.

⁹¹ <https://www.southshorehealth.org/website-privacy-policy>.

⁹² See n.84, *supra*. Defendants observe that businesses facing lawsuits “employed varying degrees of disclosure on their websites.” Defs-Br-33. Defendants’ argument

Defendants protest that although disclosure provides a solution going forward, they face substantial retrospective liability. Defs-Br-34. The MWA's legislative history confirms the imposition of substantial statutory damages was no fluke; it was intended as a deterrence against "a problem of immense dimensions."⁹³ Earlier drafts of the MWA provided for \$500 statutory damages.⁹⁴ As enacted, the MWA set statutory damages yet higher at \$1,000. G.L. c.272 §99(Q)(1). **That was 55 years ago when \$1,000 was worth much more than today.**

Defendants cannot show that "the drafters could not have intended" stiff penalties. Even if the results were harsh, that does not mean they are absurd results that can be set aside. *Lamie v. United States*, 540 U.S. 526, 538 (2004)("Our unwillingness to soften the import of Congress' chosen words even if we believe the words lead to a harsh outcome is longstanding."); *In re Blixseth*, 684 F.3d 865, 872 (9th Cir. 2012)("The result may be harsh but is not absurd."); *Dekoladenu v. Gonzales*, 459 F.3d 500, 506 (4th Cir. 2006)(" Although this result may be harsh, it is hardly 'nonsensical' or 'absurd.'").

underscores how terrible Defendants' disclosures were: lying to consumers by telling them their communications were not shared with "outside organizations." Wherever the line should be drawn, Defendants crossed it.

⁹³ S. Rep. 1469 (Addendum:156); S. Rep. 1198 (Addendum:143)("We can only hope to lessen the incidence of eavesdropping").

⁹⁴ H. Bill 1435 (Addendum:134); H. Bill 3665 (Addendum:167).

Given that the MWA's imposition of significant statutory damages was not a legislative oversight, this Court's direction that "[t]he Legislature is presumed to intend and understand all the consequences of its actions" is particularly appropriate here. *Alves's Case*, 451 Mass. 171, 179-80 (2008). Here, the Legislature clearly intended significant penalties to redress the "grave dangers" posed by the secret use of modern surveillance technologies. *See* pp.36-38. Its application here is not absurd. *DiMasi v. Galvin*, 2020 Mass. Super. LEXIS 102, *22 (July 2, 2020)("To give effect to the legislative bargain...is to respect the law as passed, and is not a surrender to absurdity.").

Finally, applying the MWA to the secret deployment of AdTech should come as no surprise. The use of wiretap law to place limits on privacy encroachments by new technologies is nothing new. The First Circuit, more than twenty years ago, affirmed class federal wiretap liability relating to software "designed to record the webpages a user viewed at clients' websites." *Pharmatrak*, 329 F.3d at 13. *Pharmatrak* was no outlier; wiretap law has been commonly used in class actions to redress eavesdropping through modern technologies.⁹⁵ *See* p.32, *supra*. Federal

⁹⁵ Defendants' premature argument that the Legislature could not have contemplated class liability because the MWA has no class action provision, Defs-Br-32, n. 51, is incorrect. Nothing in the MWA prohibits class actions. In *Magliacane v. Gardner*, this Court affirmed the availability of class actions under the Massachusetts Tort

courts routinely sustain class wiretap claims notwithstanding the fact that the **federal statute imposes statutory damages of \$10,000—ten times greater than the MWA.** 18 U.S.C. §2520(C)(2)(B).

Partners—the first MWA class case against hospitals relating to AdTech—further undermines any claim of unfair surprise. The Superior Court in *Partners* denied a motion to dismiss in December 2020.⁹⁶ The case settled in September 2021, resulting in mailed class notice to 2.8 million area residents.⁹⁷ Then, in June 2022, AdTech became big news following a report about hospital use of AdTech, which triggered a congressional investigation. In response, Defendants removed Meta Pixel from their websites, but not Google Analytics and other AdTech.⁹⁸ Defendants continued to misrepresent that they did not share any information with third parties

Claims Act, given the absence of express prohibition of class actions. 483 Mass. 842, 855, n.9 (2020).

Defendants cite no case suggesting class actions are unavailable under the MWA. In *Marquis v. Google, Inc.*, 2014 Mass. Super. LEXIS 104 (June 27, 2014), the only case Defendants cite that addressed class certification, the court did not suggest class actions were unavailable; rather, the decision turned on Plaintiff's failure to meet Rule 23's requirements because the evidence showed Google disclosed its automated review of emails to Gmail users (contrary to the facts alleged here). *Id.* at *29-43. The court even suggested a "possible class" of non-Gmail users. *Id.* at *46.

⁹⁶ Addendum:224-227.

⁹⁷ Addendum:367-71(¶¶20-22)

⁹⁸ R:A:I:21-22(¶¶53-54); R:A:I:22-23(¶54).

while still helping Google and others secretly intercept website communications until August 2023, six months after the BIDMC complaint was filed.

Given the long-established law sustaining class wiretap claims, to the degree Defendants now face substantial liability for ignoring these developments and continuing to violate the MWA, they have nobody to blame but themselves.

Conclusion

For the foregoing reasons, the Court should affirm the Decisions.

Respectfully submitted,

/s/ Patrick J. Vallely

SHAPIRO HABER & URMY LLP
Edward F. Haber (BBO #215620)
Michelle H. Blauner (BBO #549049)
Patrick J. Vallely (BBO #663866)
One Boston Place, Suite 2600
Boston, MA 02108
(617) 439-3939
ehaber@shulaw.com
mblauner@shulaw.com
pvallely@shulaw.com

Counsel for Plaintiff

Dated: March 8, 2024

ADDENDUM

Table of Contents

<u>Document</u>	<u>Page</u>
<u>Appealed Orders</u>	
Memorandum of Decision and Order and Report to the Appeals Court in <i>Vita v. Beth Israel Deaconess Medical Center, Inc., 2384cv00480-BLS1</i>	69
Memorandum of Decision and Order and Report to the Appeals Court in <i>Vita v. New England Baptist Hospital, 2384cv00857-BLS1</i>	81
<u>Statutes/Legislative History</u>	
G.L. c. 272, § 99.....	93
An Act to Define and Punish the Crime of Eavesdropping, 1920 Mass. Acts. c. 558 (May 28, 1920)	117
An Act Further Regulating Wiretapping and Eavesdropping, 1968 Mass. Acts c. 738 (July 20, 1968).....	119
<i>Resolve Providing for an Investigation and Study by a Special Commission Relative to Illegal Use of Electronic Recording Devices, Wireless Taps or Electronic Taps or Similar Devices and Arrangements,</i> S. Bill 201 (Mass. 1964)	132
An Act Repeating the Present Wiretapping Statute and Providing for a New Statute in Relation Thereto, H. Bill 1435 (Mass. 1967).....	133
<i>Interim Report of the Special Commission on Electronic Eavesdropping,</i> S. Rep. 1198 (Mass. 1967).....	140
<i>Interim Report of the Special Commission on Electronic Eavesdropping,</i> S. Rep. 1469 (Mass. 1967).....	155
An Act Relating to Eavesdropping and Creating a Commission on Electronic Surveillance and Eavesdropping, H. Bill 3665 (Mass. 1968).....	163
<i>Report of the Special Commission on Electronic Eavesdropping,</i> S. Rep. 1132 (Mass. 1968).....	168

Unpublished Cases

Doe v. The Children’s Hospital Corporation, No. 2384CV00411-BLS-1 (Mass. Super. Ct.), Memorandum of Decision and Order on Defendant’s Motion to Dismiss (Sept. 14, 2023).....202

Doe v. Emerson Hospital, No. 2277CV01000 (Mass. Super. Ct.), Memorandum of Decision and Order on Defendant’s Motion to Dismiss (Nov. 22, 2023)212

Doe v. Partners Healthcare System, Inc., No. 1984CV01651-BLS1 (Mass. Super. Ct.), Order on Motion to Dismiss (Dec. 7, 2020)224

Doe v. Partners Healthcare System, Inc., No. 1984CV01651-BLS1 (Mass. Super. Ct.), Transcript from Rule 12 Hearing Before the Honorable Brian A. Davis, Including Oral Ruling (Nov. 20, 2020).....228

Marquis v. Google, Inc., No. 11-2808-BLS1 (Mass. Super. Ct.), Memorandum Of Decision and Order on Defenant Google Inc.’s Motion to Dismiss (Jan. 17, 2012).....316

Doe v. Medstar Health, Inc., No. 24-c-20-000591 (Md. Cir. Ct.), Memorandum Opinion (Aug. 5, 2020)325

Doe v. Sutter Health, No. 34-2019-00258072 (Cal. Super. Ct.), Minute Order (June 9, 2022)331

Doe v. Bon Secours Mercy Health, No. A2002633 (Ohio Ct. Common Pleas), Decision and Entry Granting in Part and Denying in Part Defendant’s Motion to Dismiss (Nov. 23, 2021)346

Doe v. University Hospitals Health System, Inc., No. CV-20-933357 (Ohio Ct. Common Pleas), Opinion and Order (Nov. 16, 2020).....358

Doe v. Partners Healthcare System, Inc., No. 1984CV01651-BLS1 (Mass. Super. Ct.), Affidavit of Jane Murray (Jan 4., 2022)367

NOTIFY

17

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION
No. 2384CV00480-BLS1

KATHLEEN VITA¹

11/1/23
Notice sent
BA (2)

vs.

BETH ISRAEL DEACONESS MEDICAL CENTER, INC.

MEMORANDUM OF DECISION AND ORDER ON
DEFENDANT'S MOTION TO DISMISS
AND REPORT TO THE APPEALS COURT

Plaintiff Kathleen Vita ("Plaintiff") commenced this putative class action against defendant Beth Israel Deaconess Medical Center ("BIDMC"), alleging that it used internet tracking tools on its website that illegally redirected website users' personal information, and the contents of users' communications with BIDMC's website, to third parties Google and Meta. On the basis of these allegations, the Complaint asserts a single claim for violation of the Massachusetts Wiretap Statute, G.L. c. 272, § 99. Presently before the court is BIDMC's motion to dismiss. After a hearing on September 19, 2023, and consideration of the parties' submissions, the motion is **DENIED**, and, consistent with the parties' request, the matter is **REPORTED** to the Appeals Court.

BACKGROUND

The Complaint and relevant documents attached to the motion to dismiss set forth the following facts.² BIDMC operates a hospital in Boston that offers inpatient and outpatient care

¹ For herself and the class.

² BIDMC's complete website Privacy Policy, which Plaintiff relies on in framing her Complaint, was attached to the motion to dismiss. *Marram v. Kobrick Offshore Fund, Ltd.*, 442 Mass. 43, 45 n.4 (2004).

to residents in the greater Boston area. Plaintiff is an individual residing in Revere, Massachusetts.

BIDMC maintains and controls a website for its hospital. The website allows users to obtain information about the services BIDMC provides, including information about doctors, services, and treatments provided for particular medical conditions. Website users also can book appointments, access and pay bills, and access private medical information through the website's patient portal. The website contains search bars that aid users in finding specific information on the site, and forms that users may submit to BIDMC, such as the "Request an Appointment" form.

As relevant here, BIDMC's website privacy policy ("Privacy Policy") states:

Beth Israel Deaconess Medical Center (BIDMC) is committed to protecting your privacy. The BIDMC website allows you to visit most areas without identifying yourself or providing personal information. For those areas where you elect to provide identifiable information, we assure you that we make every effort to protect your privacy. . . .

Beth Israel Deaconess Medical Center routinely gathers data on website activity, such as how many people visit the site, the pages they visit, where they come from, how long they stay, etc. The data is collected on an aggregate, anonymous basis, which means no personally identifiable information is associated with the data. This data helps us improve site content and overall usage. This information is not shared with other organizations. Except for authorized law enforcement investigations or other facially valid legal processes, we will not share any information we receive with outside parties. . . .

We and our Third Party Service Provider collect and save the default information customarily logged by worldwide web server software. Our logs contain the following information for each request: date and time, originating IP address and domain name (the unique address assigned to your Internet service provider's computer that connects to the Internet), object requested, and completion status of the request. These logs may be kept for an indefinite amount of time, used at any time and in any way necessary to prevent security breaches and to ensure the integrity of the data on our servers.

(Formatting altered). Since 2021, BIDMC's website also has included a pop-up notice that references the use of "cookies and other tools to enhance your experience on the website," with a link to the Privacy Policy "for more information about these cookies and the data collected."

Notwithstanding this Privacy Policy, BIDMC has implemented multiple software-based internet tracking technologies on its website that contemporaneously record and transmit data about users' interactions with BIDMC's website to multiple unidentified third parties. The software is unrelated to the website's functionality and is invisible to users. Two such tracking technologies are Meta Pixel, which transmits data to Meta (the parent company of Facebook), and Google Analytics, which transmits data to Google.

Meta Pixel and Google Analytics operate through the automatic execution of pieces of JavaScript code, embedded in the BIDMC website, which cause a website user's internet browser to record and send information to those third parties when a user visits and interacts with the site. The transmitted information can include: the website address (URL); the title of webpages visited; information about the content of the website; search terms or any other information inputted into a form; selections on drop-down menus and the contents thereof; scrolls down a webpage; and button clicks. A website user's internet protocol ("IP") address and web browser configurations are also revealed, which permits Google and Meta to associate the data it receives from the website visit to the identity of a particular individual known to them. The content of the user's communications with BIDMC's website is added to Google's and Meta's collection of information already known about the individual, which can be used to target advertising to that individual. Google, Meta, and BIDMC may also use the information collected for other commercial purposes. After a media exposé about the use of Meta Pixel on hospital

websites, BIDMC removed it from its website in September 2022. As of the date the Complaint was filed, Google Analytics software remained on the BIDMC website.

In addition to Meta Pixel and Google Analytics, BIDMC also employs other software-based internet tracking technologies that work in a similar fashion. Those include Doubleclick, Siteimprove Analytics, and Marchex.io.

Plaintiff's husband is a BIDMC patient. Plaintiff regularly uses the BIDMC website to obtain information about BIDMC doctors (including their credentials and backgrounds); search for information on particular symptoms, conditions, and medical procedures, both for herself and her husband; and obtain and review her husband's medical records through the BIDMC website patient portal.

STANDARD OF REVIEW

Rule 12(b)(6) allows for dismissal of a complaint when the factual allegations contained within it do not suggest a plausible entitlement to relief. *Iannacchino v. Ford Motor Co.*, 451 Mass. 623, 635-636 (2008); *Fraelick v. PerkettPR, Inc.*, 83 Mass. App. Ct. 698, 699-700 (2013). In ruling on the motions, the court accepts the factual allegations as true and draws all reasonable inferences in the non-moving party's favor. *Fraelick*, 83 Mass. App. Ct. at 699-700.

DISCUSSION

BIDMC argues that Plaintiff's claims must be dismissed due to lack of standing and failure to meet the requirements of the Massachusetts Wiretap Statute. As discussed below, however, under this court's reading of the relevant caselaw and the plain language of the statute, the Complaint states a claim sufficient to survive dismissal under Rule 12(b)(6). Nevertheless, because of the novelty of the issue raised, which also has arisen in several analogous cases

before this court, and for the further reasons discussed below, a report to the Appeals Court is appropriate.³

1. Standing⁴

This court recently addressed standing in an analogous wiretap cases — *Doe v. Boston Medical Center*, 2384CV00326-BLS1, slip op. at 4-5 (Mass. Super. Ct. Sept. 15, 2023) (“*Boston Medical Center*”). There, the court denied the defendant’s motion to dismiss on standing grounds, concluding that “a properly alleged violation of the [Massachusetts Wiretap Statute], alone, constitute[s] injury sufficient to confer standing.” *Id.* (citing *Pine v. Rust*, 404 Mass. 411, 418 (1989); *In re Lubanski*, 186 B.R. 160, 166-67 (Bankr. D. Mass. 1995)). For the same reasons enunciated in that decision, Plaintiff has standing to sue here, as well.

2. Massachusetts Wiretap Statute

General Laws c. 272, § 99(Q) provides a cause of action for “any aggrieved person whose oral or wire communications were intercepted, disclosed or used . . . or whose personal or property interests or privacy were violated by means of an interception,” except as permitted or authorized by the Wiretap Statute. “Interception” is defined to mean “to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication.” G.L. c. 272, § 99(B)(4).

BIDMC argues that the action should be dismissed because, according to it: 1) the statute applies only to “conversations,” not internet tracking; 2) BIDMC’s recording of website user

³ On this same date the court also decides a similar motion to dismiss and reports the correctness of its ruling to the Appeals Court in *Kathleen Vita v. New England Baptist Hospital*, 2384CV00857-BLS1.

⁴ The standard of review for challenging standing in a motion to dismiss under Rule 12(b)(1) is functionally the same as under Rule 12(b)(6). *Abate v. Fremont Inv. & Loan*, 470 Mass. 821, 828 (2015).

activity was not secret; 3) the statutory “ordinary course of business” exception applies; and 4) application of the statute to the facts here would lead to absurd results the Legislature could not have intended. The court addresses each, in turn.

A. Limitation of the statute to human-to-human conversation. In prior analogous cases, this court concluded that the plain language of the statute encompasses the electronic activity alleged here. See *Boston Medical Center*, 2384CV00326-BLS1, slip op. at 6-7; *Doe v. Boston Children’s Hospital*, 2384CV00411-BLS1, slip op. at 4-6 (Mass. Super. Ct. Sept. 15, 2023) (“*Boston Children’s*”). Accordingly, for the same reasons already articulated in those cases, the argument fails here, as well.

B. Secrecy requirement. As noted, an interception under the Massachusetts Wiretap Statute must be “secret.” G.L. c. 272, § 99(B)(4). A “secret” recording is one that is “concealed,” and “kept hidden or unexplained.” *Curtatone v. Barstool Sports, Inc.*, 487 Mass. 655, 658 (2021) (dictionary citations omitted). An interception is not secret for purposes of the Massachusetts Wiretap Statute if the individual communicating has “actual [or constructive] knowledge of the recording,” which is proved through “‘clear and unequivocal objective manifestations of knowledge’ in the [users’] statements or conduct.” *Commonwealth v. Morris*, 492 Mass. 498, 515 (2023) (Budd., J., concurring) (quoting *Commonwealth v. Jackson*, 370 Mass. 502, 507 (1976)). See *Commonwealth v. Du*, No. 22-P-870, 2023 WL 652243, at *6 (Mass. App. Ct. Oct. 6, 2023).

BIDMC argues that its Privacy Policy and related website pop-up disclose BIDMC’s collection of data, and its sharing of that data with a third party, such that the internet tracking activity alleged here is not secret. There are two problems with that argument. First, the Privacy Policy is unclear about the exact nature of the website data BIDMC shares. The Privacy Policy

informs users that BIDMC collects certain user data that is kept anonymous and which “is not shared with other organizations,” but then notes the existence of an external “Third Party Service Provider” that also collects data, but defines that collected data in a different way. The Privacy Policy language is technical and obscures whether the BIDMC data and the Third Party Service Provider data are related or overlap in some ways, and thus whether some of the purportedly private, unshared, “anonymous” data BIDMC collects is nevertheless shared with the Third Party Service Provider.⁵ Second, the Privacy Policy discloses the existence of only a *single* “Third Party Service Provider,” while the Complaint alleges that the data BIDMC collects is contemporaneously shared with *multiple* external organizations (Google, Meta, and others). The existence of these additional third-party “eavesdroppers” are thus kept hidden from BIDMC’s website users.

In sum, the Privacy Policy and website pop-up, while disclosing some amount of data sharing, do not establish users’ actual or constructive knowledge of the totality of the internet tracking alleged here.⁶ Accordingly, on the facts as pleaded and taken as true, the Complaint sufficiently alleges a secret interception, i.e. that BIDMC “aid[ed] another to secretly hear or secretly record the contents of any wire or oral communication.” G.L. c. 272, § 99(B)(4).⁷

C. “Ordinary course of business” exception. The Massachusetts Wiretap Statute excepts from the definition of “intercepting device”:

⁵ Indeed, as a lay reader of the Privacy Policy, the court is unable to determine whether BIDMC’s collected data about “how many people visit the site, the pages they visit, where they come from, how long they stay, etc.” includes some of the same information as it and the Third Party Service Provider’s collection of “default information customarily logged by worldwide web server software.”

⁶ That a website user can reveal the internet tracking software code by employing “Developer Mode” also does not establish actual or constructive knowledge of the software code at issue.

⁷ Because this case alleges third-party eavesdropping on website communications by undisclosed, contemporaneous third-parties, this case differs from *Curtatone v. Barstool Sports, Inc.*, 487 Mass. 655 (2023), which involved a consented-to recorded conversation between two people only. *See id.* at 657, 660.

any telephone or telegraph instrument, equipment, facility, or a component thereof, (a) furnished to a subscriber or user by a communications common carrier in the ordinary course of its business under its tariff and being used by the subscriber or user in the ordinary course of its business . . .

G.L. c. 272, § 99(B)(3). Thus, for the exception to apply, the intercepting device at issue must consist of or include “telephone or telegraph” equipment, instruments, etc. *Id.*

Setting aside whether internet tracking occurs in the ordinary course of BIDMC’s business, the electronic software-based internet tracking technology at issue here plainly is not telephone or telegraph equipment. For that reason, in the absence of an appellate decision extending the exception beyond the realm of telephones and telegraphs, under the plain language of the statute, the court declines to apply the exception here. *See Alves v. BJ’s Wholesale Club, Inc.*, 2284CV02509-BLS1, slip op. at 10 (Super. Ct. June 21, 2023) (“*Alves*”) (declining to extend exception to software-based session replay code technology).

D. Legislative Intent. Finally, BIDMC argues that interpreting the Massachusetts Wiretap Statute to encompass the ubiquitous internet tracking that practically all businesses presently employ would lead to absurd results the Legislature could not have intended when it enacted the statute in 1968. Reading the criminal caselaw that BIDMC cites for this proposition does not compel the denial it seeks, however.

Commonwealth v. Morris, 492 Mass. 498 (2023), and *Commonwealth v. Rainey*, 491 Mass. 632 (2023), upon which BIDMC relies, each involve statements made to police wherein the speakers necessarily understood that their statements were being memorialized for future use or presentation in court, despite the lack of explicit disclosure about electronic recording. *Morris*, 492 Mass. at 503-04; *Rainey*, 491 Mass. at 635, 640-41. In that narrow context, the

court determined that literal application of the Massachusetts Wiretap Statute would result in absurd and unintended consequences, at odds with the Legislature's intent in enacting the statute. *See Morris*, 492 Mass. at 506 ("nothing in the statute as a whole, including its codified preamble, supports the conclusion that the Legislature intended to criminalize the police officers' recording of the defendant's voluntary statement, which the defendant understood was being preserved for future use in connection with the investigation of the crime about which the defendant was speaking voluntarily"); *Rainey*, 491 Mass. at 643 (same as to victim's voluntarily-provided statement to police).

Here, unlike the criminal defendant and victim in *Morris* and *Rainey*, Plaintiff and BIDMC's other website users are not alleged to be proceeding with the implicit understanding that their communications are to be preserved and memorialized, electronically or by handwritten notes, by a government body, for important public safety reasons. Rather, the entire gist of the Complaint is that Plaintiff interacted with the BIDMC website with no concept that the data she inputted would be simultaneously and automatically intercepted and externally shared with multiple external parties. These facts alone distinguish this case from *Morris* and *Rainey*.

In further contrast to those cases, the statute's preamble arguably supports the right to freedom from private electronic surveillance at issue here. Its broad language provides:

The general court . . . finds that the uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the commonwealth. Therefore, the secret use of such devices by private individuals must be prohibited.

G.L. c. 272, § 99. In fact, a broad interpretation of the statute's language is endorsed in *Commonwealth v. Moody*, 466 Mass. 196 (2013), a Supreme Judicial Court decision that

extended the Massachusetts Wiretap Statute's application to electronic text messages. *See id.* at 209 (“[i]n light of the broad statutory definitions of the terms ‘wire communication’ and ‘interception,’ we conclude that the Massachusetts wiretap statute provides protection for the electronic transmission of text messages”).⁸

For the reasons explained above, and absent an appellate decision interpreting the Massachusetts Wiretap Statute in the narrow way that BIDMC suggests, this court concludes that the facts as alleged in the Complaint state a claim for a violation of the statute.

3. Report to Appeals Court

Under Mass. R. Civ. P. 64, a Superior Court judge may report an interlocutory decision “where he or she concludes that the finding or order ‘so affects the merits of the controversy that the matter ought to be determined by the [A]ppeals [C]ourt before any further proceedings in the trial court.’” *Patel v. Martin*, 481 Mass. 29, 32 (2018) (quoting Mass. R. Civ. P. 64(a)). The Supreme Judicial Court has cautioned that “[i]nterlocutory matters should be reported only where it appears that they present serious questions likely to be material in the ultimate decision, and that subsequent proceedings in the trial court will be substantially facilitated by so doing.” *Globe Newspaper Co. v. Massachusetts Bay Transp. Auth. Ret. Bd.*, 412 Mass. 770, 772 (1992) (quoting *John Gilbert Jr. Co. v. C.M. Fauci Co.*, 309 Mass. 271, 273 (1941)). Such is the case here. The parties here also have requested that the court report the matter to the Appeals Court.

Whether the Massachusetts Wiretap Statute applies to the internet tracking alleged here is a novel question unresolved at the appellate level in Massachusetts, and is the central and

⁸ The most recent published case interpreting the Massachusetts Wiretap Statute is consistent with this view. *See Commonwealth v. Du*, No. 22-P-870, 2023 WL 6522435, at *6-*7 (Mass. App. Ct. Oct. 6, 2023) (court interpreted statute to prohibit surreptitious audio-visual video recording of drug transaction made by police using cell phone application).

dispositive issue in this case. Although the Massachusetts Wiretap Statute is broadly drafted, and states the Legislature's explicit intention to protect citizens from the grave danger of electronic surveillance by private individuals poses, it was enacted in 1968 — long before the internet, let alone internet tracking, became available. The Legislature did not, therefore, contemplate internet tracking as a form of secretly intercepting communications. BIDMC argues that internet tracking is practically ubiquitous across all businesses and organizations with websites, and that BIDMC's use of such tracking is a legitimate, ordinary part of its business. Had the Legislature been aware of internet tracking and its possible business uses in 1968, it might have written the statute to allow the type of tracking alleged in this case.

The novel question here has arisen in several other cases. As noted, this court already has denied motions to dismiss in two other internet-tracking wiretap cases. *See Boston Medical Center*, 2384CV00326-BLS1; *Boston Children's*, 2384CV00411-BLS1. Other Superior Court judges have issued similar decisions. *See Alves*, 2284CV02509-BLS1; *Doe v. Partners Healthcare System, Inc.*, 1984CV01651-BLS1, endorsement denying motion to dismiss (Super. Ct. Dec. 7, 2020). There are many other analogous cases presently pending in the Superior Court, including in this session.⁹ If, as BIDMC argues, the Massachusetts Wiretap Statute does not apply to business-related internet tracking, significant judicial and party resources will be saved by the quick resolution of these cases before discovery and other stages of litigation.

⁹ Other analogous cases pending in BLS1 include: *Progin, Janice v. UMass Memorial Health Care, Inc.*, 2284CV2889; *John Doe v. Boston Medical Center Corp.*, 2384CV326; *Jane Doe v. The Children's Hospital Corp.*, 2384CV411; *Kathleen Vita v. New England Baptist Hospital*, 2384CV00857; *Karen McManus v. Tufts Medical Center, Inc.*, 2384CV930; *Elizabeth Nova v. Boston Medical Center Corporation*, 2384CV1086; *Jane Doe v. Cape Cod Healthcare, Inc.*, 2384CV1236; *Jane Doe v. Baystate Health Systems*, 2384CV1949; *John Doe v. UMass Memorial Health Care Inc.*, 2384CV2448; *Lisa Colleton v. UMass Memorial Health Care Inc.*, 2384CV2450

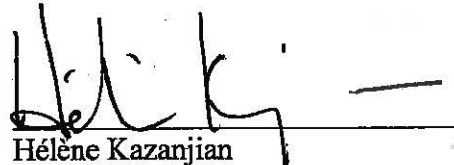
For all of these reasons, this matter should be determined by the Appeals Court before any proceedings continue in this court.

ORDER

For the foregoing reasons, it is hereby **ORDERED** that:

1. BIDMC's motion to dismiss is **DENIED**; and
2. The Court **REPORTS** the correctness of its ruling to the Appeals Court.

Dated: October 31, 2023


Hélène Kazanjian
Justice of the Superior Court

NOTIFY

16

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION
No. 2384CV00857-BLS1

KATHLEEN VITA¹

11/1/23
notice sent
BH (2)

vs.

NEW ENGLAND BAPTIST HOSPITAL

MEMORANDUM OF DECISION AND ORDER ON
DEFENDANT'S MOTION TO DISMISS
AND REPORT TO THE APPEALS COURT

Plaintiff Kathleen Vita ("Plaintiff") commenced this putative class action against defendant New England Baptist Hospital ("NEBH"), alleging that it used internet tracking tools on its website that illegally redirected website users' personal information, and the contents of users' communications with NEBH's website, to third parties Google and Meta. On the basis of these allegations, the Complaint asserts a single claim for violation of the Massachusetts Wiretap Statute, G.L. c. 272, § 99. Presently before the court is NEBH's motion to dismiss. After a hearing on September 19, 2023, and consideration of the parties' submissions, the motion is **DENIED**, and, consistent with the parties' request, the matter is **REPORTED** to the Appeals Court.

BACKGROUND

The Complaint and relevant documents attached to the motion to dismiss set forth the following facts.² NEBH operates a hospital with a main campus in Boston, and several other

¹ For herself and the class.

² NEBH's complete website Privacy Policy, which Plaintiff relies on in framing her Complaint, was attached to the motion to dismiss. *Marram v. Kobrick Offshore Fund, Ltd.*, 442 Mass. 43, 45 n.4 (2004).

locations in the Boston area, focusing on orthopedic care and complex orthopedic procedures. Plaintiff is an individual residing in Revere, Massachusetts.

NEBH maintains and controls a website for its hospital. The website allows users to obtain information about the services NEBH provides, including information about doctors, services, and treatments provided for particular medical conditions. Website users also can access and pay bills, and access private medical information through the website's patient portal. The website contains search bars that aid users in finding specific information on the site, and forms that users may submit to NEBH, such as the "Find a Doctor" form.

As relevant here, NEBH's website privacy policy ("Privacy Policy") states:

New England Baptist Hospital (NEBH) is committed to protecting your privacy. The NEBH website allows you to visit most areas without identifying yourself or providing personal information. For those areas where you elect to provide identifiable information, we assure you that we make every effort to protect your privacy. . . .

New England Baptist Hospital routinely gathers data on website activity, such as how many people visit the site, the pages they visit, where they come from, how long they stay, etc. The data is collected on an aggregate, anonymous basis, which means no personally identifiable information is associated with the data. This data helps us improve site content and overall usage. This information is not shared with other organizations. Except for authorized law enforcement investigations or other facially valid legal processes, we will not share any information we receive with outside parties. . . .

We and our Third Party Service Provider collect and save the default information customarily logged by worldwide web server software. Our logs contain the following information for each request: date and time, originating IP address and domain name (the unique address assigned to your Internet service provider's computer that connects to the Internet), object requested, and completion status of the request. These logs may be kept for an indefinite amount of time, used at any time and in any way necessary to prevent security breaches and to ensure the integrity of the data on our servers.

(Formatting altered). Since 2021, NEBH's website also has included a pop-up notice that references the use of "cookies and other tools to enhance your experience on the

website,” with a link to the Privacy Policy “for more information about these cookies and the data collected.”

Notwithstanding this Privacy Policy, NEBH has implemented multiple software-based internet tracking technologies on its website that contemporaneously record and transmit data about users’ interactions with NEBH’s website to multiple unidentified third parties. The software is unrelated to the website’s functionality and is invisible to users. Two such tracking technologies are Meta Pixel, which transmits data to Meta (the parent company of Facebook), and Google Analytics, which transmits data to Google.

Meta Pixel and Google Analytics operate through the automatic execution of pieces of JavaScript code, embedded in the NEBH website, which cause a website user’s internet browser to record and send information to those third parties when a user visits and interacts with the site. The transmitted information can include: the website address (URL); the title of webpages visited; information about the content of the website; search terms or any other information inputted into a form; selections on drop-down menus and the contents thereof; scrolls down a webpage; and button clicks. A website user’s internet protocol (“IP”) address and web browser configurations are also revealed, which permits Google and Meta to associate the data it receives from the website visit to the identity of a particular individual known to them. The content of the user’s communications with NEBH’s website is added to Google’s and Meta’s collection of information already known about the individual, which can be used to target advertising to that individual. Google, Meta, and NEBH may also use the information collected for other commercial purposes. After a media exposé about the use of Meta Pixel on hospital websites in June 2022, NEBH removed it from its website at some unidentified point in time. As of the date the Complaint was filed, Google Analytics software remained on the NEBH website.

Plaintiff is a NEBH patient. Plaintiff regularly uses the NEBH website to obtain information about NEBH doctors (including their credentials and backgrounds) and to search for information on particular medical procedures.

STANDARD OF REVIEW

Rule 12(b)(6) allows for dismissal of a complaint when the factual allegations contained within it do not suggest a plausible entitlement to relief. *Iannacchino v. Ford Motor Co.*, 451 Mass. 623, 635-636 (2008); *Fraelick v. Perket PR, Inc.*, 83 Mass. App. Ct. 698, 699-700 (2013). In ruling on the motions, the court accepts the factual allegations as true and draws all reasonable inferences in the non-moving party's favor. *Fraelick*, 83 Mass. App. Ct. at 699-700.

DISCUSSION

NEBH argues that Plaintiff's claims must be dismissed due to lack of standing and failure to meet the requirements of the Massachusetts Wiretap Statute. As discussed below, however, under this court's reading of the relevant caselaw and the plain language of the statute, the Complaint states a claim sufficient to survive dismissal under Rule 12(b)(6). Nevertheless, because of the novelty of the issue raised, which also has arisen in several analogous cases before this court, and for the further reasons discussed below, a report to the Appeals Court is appropriate.³

³ On this same date the court also decides a similar motion to dismiss and reports the correctness of its ruling to the Appeals Court in *Kathleen Vita v. Beth Israel Deaconess Medical Center, Inc.*, 2384CV00480-BLS1.

1. Standing⁴

This court recently addressed standing in an analogous wiretap case — *Doe v. Boston Medical Center*, 2384CV00326-BLS1, slip op. at 4-5 (Mass. Super. Ct. Sept. 15, 2023) (“*Boston Medical Center*”). There, the court denied the defendant’s motion to dismiss on standing grounds, concluding that “a properly alleged violation of the [Massachusetts Wiretap Statute], alone, constitute[s] injury sufficient to confer standing.” *Id.* (citing *Pine v. Rust*, 404 Mass. 411, 418 (1989); *In re Lubanski*, 186 B.R. 160, 166-67 (Bankr. D. Mass. 1995)). For the same reasons enunciated in that decision, Plaintiff has standing to sue here, as well.

2. Massachusetts Wiretap Statute

General Laws c. 272, § 99(Q) provides a cause of action for “any aggrieved person whose oral or wire communications were intercepted, disclosed or used . . . or whose personal or property interests or privacy were violated by means of an interception,” except as permitted or authorized by the Wiretap Statute. “Interception” is defined to mean “to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication.” G.L. c. 272, § 99(B)(4).

NEBH argues that the action should be dismissed because, according to it: 1) the statute applies only to “conversations,” not internet tracking; 2) NEBH’s recording of website user activity was not secret; 3) the statutory “ordinary course of business” exception applies; and 4) application of the statute to the facts here would lead to absurd results the Legislature could not have intended. The court addresses each, in turn.

⁴ The standard of review for challenging standing in a motion to dismiss under Rule 12(b)(1) is functionally the same as under Rule 12(b)(6). *Abate v. Fremont Inv. & Loan*, 470 Mass. 821, 828 (2015).

A. Limitation of the statute to human-to-human conversation. In prior analogous cases, this court concluded that the plain language of the statute encompasses the electronic activity alleged here. See *Boston Medical Center*, 2384CV00326-BLS1, slip op. at 6-7; *Doe v. Boston Children's Hospital*, 2384CV00411-BLS1, slip op. at 4-6 (Mass. Super. Ct. Sept. 15, 2023) ("*Boston Children's*"). Accordingly, for the same reasons articulated in those cases, the argument fails here, as well.

B. Secrecy requirement. As noted, an interception under the Massachusetts Wiretap Statute must be "secret." G.L. c. 272, § 99(B)(4). A "secret" recording is one that is "concealed," and "kept hidden or unexplained." *Curtatone v. Barstool Sports, Inc.*, 487 Mass. 655, 658 (2021) (dictionary citations omitted). An interception is not secret for purposes of the Massachusetts Wiretap Statute if the individual communicating has "actual [or constructive] knowledge of the recording," which is proved through "'clear and unequivocal objective manifestations of knowledge' in the [users'] statements or conduct." *Commonwealth v. Morris*, 492 Mass. 498, 515 (2023) (Budd., J., concurring) (quoting *Commonwealth v. Jackson*, 370 Mass. 502, 507 (1976)). See *Commonwealth v. Du*, No. 22-P-870, 2023 WL 652243, at *6 (Mass. App. Ct. Oct. 6, 2023).

NEBH argues that its Privacy Policy and related website pop-up disclose NEBH's collection of data, and its sharing of that data with a third party, such that the internet tracking activity alleged here is not secret. There are two problems with that argument. First, the Privacy Policy is unclear about the exact nature of the website data NEBH shares. The Privacy Policy informs users that NEBH collects certain user data that is kept anonymous and which "is not shared with other organizations," but then notes the existence of an external "Third Party Service Provider" that also collects data, but defines that collected data in a different way. The Privacy

Policy language is technical and obscures whether the NEBH data and the Third Party Service Provider data are related or overlap in some ways, and thus whether some of the purportedly private, unshared, “anonymous” data NEBH collects is nevertheless also shared with the Third Party Service Provider.⁵ Second, the Privacy Policy discloses the existence of only a *single* “Third Party Service Provider,” while the Complaint alleges that the data NEBH collects is contemporaneously shared with *multiple* external organizations (Google, Meta, and others). The existence of these additional third-party “eavesdroppers” are thus kept hidden from NEBH’s website users.

In sum, the Privacy Policy and website pop-up, while disclosing some amount of data sharing, do not establish users’ actual or constructive knowledge of the totality of the internet tracking alleged here.⁶ Accordingly, on the facts as pleaded and taken as true, the Complaint sufficiently alleges a secret interception, i.e. that NEBH “aid[ed] another to secretly hear or secretly record the contents of any wire or oral communication.” G.L. c. 272, § 99(B)(4).⁷

C. “Ordinary course of business” exception. The Massachusetts Wiretap Statute exempts from the definition of “intercepting device”:

any telephone or telegraph instrument, equipment, facility, or a component thereof, (a) furnished to a subscriber or user by a communications common carrier in the ordinary course of its business under its tariff and being used by the subscriber or user in the ordinary course of its business . . .

⁵ Indeed, as a lay reader of the Privacy Policy, the court is unable to determine whether NEBH’s collected data about “how many people visit the site, the pages they visit, where they come from, how long they stay, etc.” includes some of the same information as it and the Third Party Service Provider’s collection of “default information customarily logged by worldwide web server software.”

⁶ That a website user can reveal the internet tracking software code by employing “Developer Mode” also does not establish actual or constructive knowledge of the software code at issue.

⁷ Because this case alleges third-party eavesdropping on website communications by undisclosed, contemporaneous third-parties, this case differs from *Curtatone v. Barstool Sports, Inc.*, 487 Mass. 655 (2023), which involved a consented-to recorded conversation between two people only. *See id.* at 657, 660.

G.L. c. 272, § 99(B)(3). Thus, for the exception to apply, the intercepting device at issue must consist of or include “telephone or telegraph” equipment, instruments, etc. *Id.*

Setting aside whether internet tracking occurs in the ordinary course of NEBH’s business, the electronic software-based internet tracking technology at issue here plainly is not telephone or telegraph equipment. For that reason, in the absence of an appellate decision extending the exception beyond telephones and telegraphs, under the plain language of the statute, the court declines to apply the exception here. *See Alves v. BJ’s Wholesale Club, Inc.*, 2284CV02509-BLS1, slip op. at 10 (Super. Ct. June 21, 2023) (“*Alves*”) (declining to extend exception to software-based session replay code technology).

D. Legislative Intent. Finally, NEBH argues that interpreting the Massachusetts Wiretap Statute to encompass the ubiquitous internet tracking that practically all businesses presently employ would lead to absurd results the Legislature could not have intended when it enacted the statute in 1968. Reading the criminal caselaw that NEBH cites for this proposition does not compel the denial it seeks, however.

Commonwealth v. Morris, 492 Mass. 498 (2023), and *Commonwealth v. Rainey*, 491 Mass. 632 (2023), upon which NEBH relies, each involve statements made to police where the speakers necessarily understood that their statements were being memorialized for future use or presentation in court, despite the lack of explicit disclosure about electronic recording. *Morris*, 492 Mass. at 503-04; *Rainey*, 491 Mass. at 635, 640-41. In that narrow context, the court determined that literal application of the Massachusetts Wiretap Statute would result in absurd and unintended consequences, at odds with the Legislature’s intent in enacting the statute. *See Morris*, 492 Mass. at 506 (“nothing in the statute as a whole, including its codified preamble, supports the conclusion that the Legislature intended to criminalize the police officers’ recording

of the defendant's voluntary statement, which the defendant understood was being preserved for future use in connection with the investigation of the crime about which the defendant was speaking voluntarily"); *Rainey*, 491 Mass. at 643 (same as to victim's voluntarily-provided statement to police).

Here, unlike the criminal defendant and victim in *Morris* and *Rainey*, Plaintiff and NEBH's other website users are not alleged to be proceeding with the implicit understanding that their communications are to be preserved and memorialized, electronically or by handwritten notes, by a government body, for important public safety reasons. Rather, the entire gist of the Complaint is that Plaintiff interacted with the NEBH website with no concept that the data she inputted would be simultaneously and automatically intercepted and externally shared with multiple external parties. These facts alone distinguish this case from *Morris* and *Rainey*.

In further contrast to those cases, the statute's preamble arguably supports the right to freedom from private electronic surveillance at issue here. Its broad language provides:

The general court . . . finds that the uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the commonwealth. Therefore, the secret use of such devices by private individuals must be prohibited.

G.L. c. 272, § 99. In fact, a broad interpretation of the statute's language is endorsed in *Commonwealth v. Moody*, 466 Mass. 196 (2013), a Supreme Judicial Court decision that extended the Massachusetts Wiretap Statute's application to electronic text messages. *See id.* at 209 (“[i]n light of the broad statutory definitions of the terms ‘wire communication’ and

‘interception,’ we conclude that the Massachusetts wiretap statute provides protection for the electronic transmission of text messages”).⁸

For the reasons explained above, and absent an appellate decision interpreting the Massachusetts Wiretap Statute in the narrow way that NEBH suggests, this court concludes that the facts as alleged in the Complaint state a claim for a violation of the statute.

3. Report to Appeals Court

Under Mass. R. Civ. P. 64, a Superior Court judge may report an interlocutory decision “where he or she concludes that the finding or order ‘so affects the merits of the controversy that the matter ought to be determined by the [A]ppeals [C]ourt before any further proceedings in the trial court.’” *Patel v. Martin*, 481 Mass. 29, 32 (2018) (quoting Mass. R. Civ. P. 64(a)). The Supreme Judicial Court has cautioned that “[i]nterlocutory matters should be reported only where it appears that they present serious questions likely to be material in the ultimate decision, and that subsequent proceedings in the trial court will be substantially facilitated by so doing.” *Globe Newspaper Co. v. Massachusetts Bay Transp. Auth. Ret. Bd.*, 412 Mass. 770, 772 (1992) (quoting *John Gilbert Jr. Co. v. C.M. Fauci Co.*, 309 Mass. 271, 273 (1941)). Such is the case here. The parties here also have requested that the court report the matter to the Appeals Court.

Whether the Massachusetts Wiretap Statute applies to the internet tracking alleged here is a novel question unresolved at the appellate level in Massachusetts, and is the central and dispositive issue in this case. Although the Massachusetts Wiretap Statute is broadly drafted, and states the Legislature’s explicit intention to protect citizens from the grave danger of

⁸ The most recent published case interpreting the Massachusetts Wiretap Statute is consistent with this view. See *Commonwealth v. Du*, No. 22-P-870, 2023 WL 6522435, at *6-*7 (Mass. App. Ct. Oct. 6, 2023) (court interpreted statute to prohibit surreptitious audio-visual video recording of drug transaction made by police using cell phone application).

electronic surveillance by private individuals, it was enacted in 1968 — long before the internet, let alone internet tracking, became available. The Legislature did not, therefore, contemplate internet tracking as a form of secretly intercepting communications. NEBH argues that internet tracking is practically ubiquitous across all businesses and organizations with websites, and that NEBH's use of such tracking is a legitimate, ordinary part of its business. Had the Legislature been aware of internet tracking and its possible business uses in 1968, it might have written the statute to allow the type of tracking alleged in this case.

The novel question here has arisen in several other cases. As noted, this court already has denied motions to dismiss in two other internet-tracking wiretap cases. *See Boston Medical Center*, 2384CV00326-BLS1; *Boston Children's*, 2384CV00411-BLS1. Other Superior Court judges have issued similar decisions recently. *See Alves*, 2284CV02509-BLS1; *Doe v. Partners Healthcare System, Inc.*, 1984CV01651-BLS1, endorsement denying motion to dismiss (Super. Ct. Dec. 7, 2020). There are many other analogous cases presently pending in the Superior Court, including in this session.⁹ If, as NEBH argues, the Massachusetts Wiretap Statute does not apply to business-related internet tracking, significant judicial and party resources will be saved by the quick resolution of these cases before discovery and other stages of litigation.

For all of these reasons, this matter should be determined by the Appeals Court before any proceedings continue in this court.

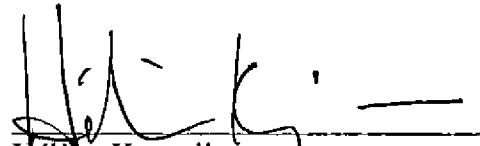
⁹ Other analogous cases pending in BLS1 include: *Progin, Janice v. UMass Memorial Health Care, Inc.*, 2284CV2889; *John Doe v. Boston Medical Center Corp.*, 2384CV326; *Jane Doe v. The Children's Hospital Corp.*, 2384CV411; *Kathleen Vita v. Beth Israel Deaconess Medical Center, Inc.*, 2384CV00480; *Karen McMamus v. Tufts Medical Center, Inc.*, 2384CV930; *Elizabeth Nova v. Boston Medical Center Corporation*, 2384CV1086; *Jane Doe v. Cape Cod Healthcare, Inc.*, 2384CV1236; *Jane Doe v. Baystate Health Systems*, 2384CV1949; *John Doe v. UMass Memorial Health Care Inc.*, 2384CV2448; *Lisa Colleton v. UMass Memorial Health Care Inc.*, 2384CV2450

ORDER

For the foregoing reasons, it is hereby **ORDERED** that:

1. NEBH's motion to dismiss is **DENIED**; and
2. The Court **REPORTS** the correctness of its ruling to the Appeals Court.

Dated: October 31, 2023



Héline Kazanjian
Justice of the Superior Court

Part IV	CRIMES, PUNISHMENTS AND PROCEEDINGS IN CRIMINAL CASES
Title I	CRIMES AND PUNISHMENTS
Chapter 272	CRIMES AGAINST CHASTITY, MORALITY, DECENCY AND GOOD ORDER
Section 99	INTERCEPTION OF WIRE AND ORAL COMMUNICATIONS

Section 99. Interception of wire and oral communications.—

A. Preamble.

The general court finds that organized crime exists within the commonwealth and that the increasing activities of organized crime constitute a grave danger to the public welfare and safety. Organized crime, as it exists in the commonwealth today, consists of a continuing conspiracy among highly organized and disciplined groups to engage in supplying illegal goods and services. In supplying these goods and services organized crime commits unlawful acts and employs brutal and violent tactics. Organized crime is infiltrating legitimate business activities and depriving honest businessmen of the right to make a living. The general court further finds that because organized crime carries on its activities through layers of insulation and behind a wall of secrecy, government has been unsuccessful in curtailing and eliminating it. Normal investigative procedures are not effective in the investigation of

illegal acts committed by organized crime. Therefore, law enforcement officials must be permitted to use modern methods of electronic surveillance, under strict judicial supervision, when investigating these organized criminal activities.

The general court further finds that the uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the commonwealth. Therefore, the secret use of such devices by private individuals must be prohibited. The use of such devices by law enforcement officials must be conducted under strict judicial supervision and should be limited to the investigation of organized crime.

B. Definitions. As used in this section—

1. The term "wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception.
2. The term "oral communication" means speech, except such speech as is transmitted over the public air waves by radio or other similar device.
3. The term "intercepting device" means any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication other than a hearing aid or similar device which is being used to correct subnormal hearing to normal and other than any telephone or telegraph instrument, equipment, facility, or a component thereof, (a) furnished to a subscriber or user by a communications common carrier in the ordinary course of its business under its tariff and being used by the

subscriber or user in the ordinary course of its business; or (b) being used by a communications common carrier in the ordinary course of its business.

4. The term "interception" means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication; provided that it shall not constitute an interception for an investigative or law enforcement officer, as defined in this section, to record or transmit a wire or oral communication if the officer is a party to such communication or has been given prior authorization to record or transmit the communication by such a party and if recorded or transmitted in the course of an investigation of a designated offense as defined herein.

5. The term "contents", when used with respect to any wire or oral communication, means any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication.

6. The term "aggrieved person" means any individual who was a party to an intercepted wire or oral communication or who was named in the warrant authorizing the interception, or who would otherwise have standing to complain that his personal or property interest or privacy was invaded in the course of an interception.

7. The term "designated offense" shall include the following offenses in connection with organized crime as defined in the preamble: arson, assault and battery with a dangerous weapon, extortion, bribery, burglary, embezzlement, forgery, gaming in violation of section seventeen of

chapter two hundred and seventy-one of the general laws, intimidation of a witness or juror, kidnapping, larceny, lending of money or things of value in violation of the general laws, mayhem, murder, any offense involving the possession or sale of a narcotic or harmful drug, perjury, prostitution, robbery, subornation of perjury, any violation of this section, being an accessory to any of the foregoing offenses and conspiracy or attempt or solicitation to commit any of the foregoing offenses.

8. The term "investigative or law enforcement officer" means any officer of the United States, a state or a political subdivision of a state, who is empowered by law to conduct investigations of, or to make arrests for, the designated offenses, and any attorney authorized by law to participate in the prosecution of such offenses.

9. The term "judge of competent jurisdiction" means any justice of the superior court of the commonwealth.

10. The term "chief justice" means the chief justice of the superior court of the commonwealth.

11. The term "issuing judge" means any justice of the superior court who shall issue a warrant as provided herein or in the event of his disability or unavailability any other judge of competent jurisdiction designated by the chief justice.

12. The term "communication common carrier" means any person engaged as a common carrier in providing or operating wire communication facilities.

13. The term "person" means any individual, partnership, association, joint stock company, trust, or corporation, whether or not any of the foregoing is an officer, agent or employee of the United States, a state, or

a political subdivision of a state.

14. The terms "sworn" or "under oath" as they appear in this section shall mean an oath or affirmation or a statement subscribed to under the pains and penalties of perjury.

15. The terms "applicant attorney general" or "applicant district attorney" shall mean the attorney general of the commonwealth or a district attorney of the commonwealth who has made application for a warrant pursuant to this section.

16. The term "exigent circumstances" shall mean the showing of special facts to the issuing judge as to the nature of the investigation for which a warrant is sought pursuant to this section which require secrecy in order to obtain the information desired from the interception sought to be authorized.

17. The term "financial institution" shall mean a bank, as defined in section 1 of chapter 167, and an investment bank, securities broker, securities dealer, investment adviser, mutual fund, investment company or securities custodian as defined in section 1.165-12(c)(1) of the United States Treasury regulations.

18. The term "corporate and institutional trading partners" shall mean financial institutions and general business entities and corporations which engage in the business of cash and asset management, asset management directed to custody operations, securities trading, and wholesale capital markets including foreign exchange, securities lending, and the purchase, sale or exchange of securities, options, futures, swaps, derivatives, repurchase agreements and other similar financial instruments with such financial institution.

C. Offenses.

1. Interception, oral communications prohibited.

Except as otherwise specifically provided in this section any person who

—
willfully commits an interception, attempts to commit an interception, or procures any other person to commit an interception or to attempt to commit an interception of any wire or oral communication shall be fined not more than ten thousand dollars, or imprisoned in the state prison for not more than five years, or imprisoned in a jail or house of correction for not more than two and one half years, or both so fined and given one such imprisonment.

Proof of the installation of any intercepting device by any person under circumstances evincing an intent to commit an interception, which is not authorized or permitted by this section, shall be prima facie evidence of a violation of this subparagraph.

2. Editing of tape recordings in judicial proceeding prohibited.

Except as otherwise specifically provided in this section any person who willfully edits, alters or tampers with any tape, transcription or recording of oral or wire communications by any means, or attempts to edit, alter or tamper with any tape, transcription or recording of oral or wire communications by any means with the intent to present in any judicial proceeding or proceeding under oath, or who presents such recording or permits such recording to be presented in any judicial proceeding or proceeding under oath, without fully indicating the nature of the changes made in the original state of the recording, shall be fined not more than

ten thousand dollars or imprisoned in the state prison for not more than five years or imprisoned in a jail or house of correction for not more than two years or both so fined and given one such imprisonment.

3. Disclosure or use of wire or oral communications prohibited.

Except as otherwise specifically provided in this section any person who

a. willfully discloses or attempts to disclose to any person the contents of any wire or oral communication, knowing that the information was obtained through interception; or

b. willfully uses or attempts to use the contents of any wire or oral communication, knowing that the information was obtained through interception, shall be guilty of a misdemeanor punishable by imprisonment in a jail or a house of correction for not more than two years or by a fine of not more than five thousand dollars or both.

4. Disclosure of contents of applications, warrants, renewals, and returns prohibited.

Except as otherwise specifically provided in this section any person who

willfully discloses to any person, any information concerning or contained in, the application for, the granting or denial of orders for interception, renewals, notice or return on an ex parte order granted pursuant to this section, or the contents of any document, tape, or recording kept in accordance with paragraph N, shall be guilty of a misdemeanor punishable by imprisonment in a jail or a house of correction for not more than two years or by a fine of not more than five thousand dollars or both.

5. Possession of interception devices prohibited.

A person who possesses any intercepting device under circumstances evincing an intent to commit an interception not permitted or authorized by this section, or a person who permits an intercepting device to be used or employed for an interception not permitted or authorized by this section, or a person who possesses an intercepting device knowing that the same is intended to be used to commit an interception not permitted or authorized by this section, shall be guilty of a misdemeanor punishable by imprisonment in a jail or house of correction for not more than two years or by a fine of not more than five thousand dollars or both.

The installation of any such intercepting device by such person or with his permission or at his direction shall be prima facie evidence of possession as required by this subparagraph.

6. Any person who permits or on behalf of any other person commits or attempts to commit, or any person who participates in a conspiracy to commit or to attempt to commit, or any accessory to a person who commits a violation of subparagraphs 1 through 5 of paragraph C of this section shall be punished in the same manner as is provided for the respective offenses as described in subparagraphs 1 through 5 of paragraph C.

D. Exemptions.

1. Permitted interception of wire or oral communications.

It shall not be a violation of this section—

a. for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that

communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the carrier of such communication, or which is necessary to prevent the use of such facilities in violation of section fourteen A of chapter two hundred and sixty-nine of the general laws; provided, that said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

b. for persons to possess an office intercommunication system which is used in the ordinary course of their business or to use such office intercommunication system in the ordinary course of their business.

c. for investigative and law enforcement officers of the United States of America to violate the provisions of this section if acting pursuant to authority of the laws of the United States and within the scope of their authority.

d. for any person duly authorized to make specified interceptions by a warrant issued pursuant to this section.

e. for investigative or law enforcement officers to violate the provisions of this section for the purposes of ensuring the safety of any law enforcement officer or agent thereof who is acting in an undercover capacity, or as a witness for the commonwealth; provided, however, that any such interception which is not otherwise permitted by this section shall be deemed unlawful for purposes of paragraph P.

f. for a financial institution to record telephone communications with its corporate or institutional trading partners in the ordinary course of its business; provided, however, that such financial institution shall establish

and maintain a procedure to provide semi-annual written notice to its corporate and institutional trading partners that telephone communications over designated lines will be recorded.

2. Permitted disclosure and use of intercepted wire or oral communications.

a. Any investigative or law enforcement officer, who, by any means authorized by this section, has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may disclose such contents or evidence in the proper performance of his official duties.

b. Any investigative or law enforcement officer, who, by any means authorized by this section has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may use such contents or evidence in the proper performance of his official duties.

c. Any person who has obtained, by any means authorized by this section, knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may disclose such contents while giving testimony under oath or affirmation in any criminal proceeding in any court of the United States or of any state or in any federal or state grand jury proceeding.

d. The contents of any wire or oral communication intercepted pursuant to a warrant in accordance with the provisions of this section, or evidence derived therefrom, may otherwise be disclosed only upon a showing of good cause before a judge of competent jurisdiction.

e. No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this section shall lose its privileged character.

E. Warrants: when issuable:

A warrant may issue only:

1. Upon a sworn application in conformity with this section; and
2. Upon a showing by the applicant that there is probable cause to believe that a designated offense has been, is being, or is about to be committed and that evidence of the commission of such an offense may thus be obtained or that information which will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit a designated offense may thus be obtained; and
3. Upon a showing by the applicant that normal investigative procedures have been tried and have failed or reasonably appear unlikely to succeed if tried.

F. Warrants: application.

1. Application. The attorney general, any assistant attorney general specially designated by the attorney general, any district attorney, or any assistant district attorney specially designated by the district attorney may apply ex parte to a judge of competent jurisdiction for a warrant to intercept wire or oral communications. Each application ex parte for a warrant must be in writing, subscribed and sworn to by the applicant authorized by this subparagraph.
2. The application must contain the following:
 - a. A statement of facts establishing probable cause to believe that a particularly described designated offense has been, is being, or is about to be committed; and

- b. A statement of facts establishing probable cause to believe that oral or wire communications of a particularly described person will constitute evidence of such designated offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit a designated offense; and
- c. That the oral or wire communications of the particularly described person or persons will occur in a particularly described place and premises or over particularly described telephone or telegraph lines; and
- d. A particular description of the nature of the oral or wire communications sought to be overheard; and
- e. A statement that the oral or wire communications sought are material to a particularly described investigation or prosecution and that such conversations are not legally privileged; and
- f. A statement of the period of time for which the interception is required to be maintained. If practicable, the application should designate hours of the day or night during which the oral or wire communications may be reasonably expected to occur. If the nature of the investigation is such that the authorization for the interception should not automatically terminate when the described oral or wire communications have been first obtained, the application must specifically state facts establishing probable cause to believe that additional oral or wire communications of the same nature will occur thereafter; and
- g. If it is reasonably necessary to make a secret entry upon a private place and premises in order to install an intercepting device to effectuate the interception, a statement to such effect; and

h. If a prior application has been submitted or a warrant previously obtained for interception of oral or wire communications, a statement fully disclosing the date, court, applicant, execution, results, and present status thereof; and

i. If there is good cause for requiring the postponement of service pursuant to paragraph L, subparagraph 2, a description of such circumstances, including reasons for the applicant's belief that secrecy is essential to obtaining the evidence or information sought.

3. Allegations of fact in the application may be based either upon the personal knowledge of the applicant or upon information and belief. If the applicant personally knows the facts alleged, it must be so stated. If the facts establishing such probable cause are derived in whole or part from the statements of persons other than the applicant, the sources of such information and belief must be either disclosed or described; and the application must contain facts establishing the existence and reliability of any informant and the reliability of the information supplied by him. The application must also state, so far as possible, the basis of the informant's knowledge or belief. If the applicant's information and belief is derived from tangible evidence or recorded oral evidence, a copy or detailed description thereof should be annexed to or included in the application. Affidavits of persons other than the applicant may be submitted in conjunction with the application if they tend to support any fact or conclusion alleged therein. Such accompanying affidavits may be based either on personal knowledge of the affiant or information and belief, with the source thereof, and reason therefor, specified.

G. Warrants: application to whom made.

Application for a warrant authorized by this section must be made to a judge of competent jurisdiction in the county where the interception is to occur, or the county where the office of the applicant is located, or in the event that there is no judge of competent jurisdiction sitting in said county at such time, to a judge of competent jurisdiction sitting in Suffolk County; except that for these purposes, the office of the attorney general shall be deemed to be located in Suffolk County.

H. Warrants: application how determined.

1. If the application conforms to paragraph F, the issuing judge may examine under oath any person for the purpose of determining whether probable cause exists for the issuance of the warrant pursuant to paragraph E. A verbatim transcript of every such interrogation or examination must be taken, and a transcription of the same, sworn to by the stenographer, shall be attached to the application and be deemed a part thereof.
2. If satisfied that probable cause exists for the issuance of a warrant the judge may grant the application and issue a warrant in accordance with paragraph I. The application and an attested copy of the warrant shall be retained by the issuing judge and transported to the chief justice of the superior court in accordance with the provisions of paragraph N of this section.
3. If the application does not conform to paragraph F, or if the judge is not satisfied that probable cause has been shown sufficient for the issuance of a warrant, the application must be denied.

I. Warrants: form and content.

A warrant must contain the following:

1. The subscription and title of the issuing judge; and
 2. The date of issuance, the date of effect, and termination date which in no event shall exceed thirty days from the date of effect. The warrant shall permit interception of oral or wire communications for a period not to exceed fifteen days. If physical installation of a device is necessary, the thirty-day period shall begin upon the date of installation. If the effective period of the warrant is to terminate upon the acquisition of particular evidence or information or oral or wire communication, the warrant shall so provide; and
 3. A particular description of the person and the place, premises or telephone or telegraph line upon which the interception may be conducted; and
 4. A particular description of the nature of the oral or wire communications to be obtained by the interception including a statement of the designated offense to which they relate; and
 5. An express authorization to make secret entry upon a private place or premises to install a specified intercepting device, if such entry is necessary to execute the warrant; and
 6. A statement providing for service of the warrant pursuant to paragraph L except that if there has been a finding of good cause shown requiring the postponement of such service, a statement of such finding together with the basis therefor must be included and an alternative direction for deferred service pursuant to paragraph L, subparagraph 2.
- J. Warrants: renewals.

1. Any time prior to the expiration of a warrant or a renewal thereof, the applicant may apply to the issuing judge for a renewal thereof with respect to the same person, place, premises or telephone or telegraph line. An application for renewal must incorporate the warrant sought to be renewed together with the application therefor and any accompanying papers upon which it was issued. The application for renewal must set forth the results of the interceptions thus far conducted. In addition, it must set forth present grounds for extension in conformity with paragraph F, and the judge may interrogate under oath and in such an event a transcript must be provided and attached to the renewal application in the same manner as is set forth in subparagraph 1 of paragraph H.

2. Upon such application, the judge may issue an order renewing the warrant and extending the authorization for a period not exceeding fifteen (15) days from the entry thereof. Such an order shall specify the grounds for the issuance thereof. The application and an attested copy of the order shall be retained by the issuing judge to be transported to the chief justice in accordance with the provisions of subparagraph N of this section. In no event shall a renewal be granted which shall terminate later than two years following the effective date of the warrant.

K. Warrants: manner and time of execution.

1. A warrant may be executed pursuant to its terms anywhere in the commonwealth.

2. Such warrant may be executed by the authorized applicant personally or by any investigative or law enforcement officer of the commonwealth designated by him for the purpose.

3. The warrant may be executed according to its terms during the hours specified therein, and for the period therein authorized, or a part thereof. The authorization shall terminate upon the acquisition of the oral or wire communications, evidence or information described in the warrant. Upon termination of the authorization in the warrant and any renewals thereof, the interception must cease at once, and any device installed for the purpose of the interception must be removed as soon thereafter as practicable. Entry upon private premises for the removal of such device is deemed to be authorized by the warrant.

L. Warrants: service thereof.

1. Prior to the execution of a warrant authorized by this section or any renewal thereof, an attested copy of the warrant or the renewal must, except as otherwise provided in subparagraph 2 of this paragraph, be served upon a person whose oral or wire communications are to be obtained, and if an intercepting device is to be installed, upon the owner, lessee, or occupant of the place or premises, or upon the subscriber to the telephone or owner or lessee of the telegraph line described in the warrant.

2. If the application specially alleges exigent circumstances requiring the postponement of service and the issuing judge finds that such circumstances exist, the warrant may provide that an attested copy thereof may be served within thirty days after the expiration of the warrant or, in case of any renewals thereof, within thirty days after the expiration of the last renewal; except that upon a showing of important special facts which set forth the need for continued secrecy to the satisfaction of the issuing judge, said judge may direct that the attested copy of the warrant be served on such parties as are required by this

section at such time as may be appropriate in the circumstances but in no event may he order it to be served later than three (3) years from the time of expiration of the warrant or the last renewal thereof. In the event that the service required herein is postponed in accordance with this paragraph, in addition to the requirements of any other paragraph of this section, service of an attested copy of the warrant shall be made upon any aggrieved person who should reasonably be known to the person who executed or obtained the warrant as a result of the information obtained from the interception authorized thereby.

3. The attested copy of the warrant shall be served on persons required by this section by an investigative or law enforcement officer of the commonwealth by leaving the same at his usual place of abode, or in hand, or if this is not possible by mailing the same by certified or registered mail to his last known place of abode. A return of service shall be made to the issuing judge, except, that if such service is postponed as provided in subparagraph 2 of paragraph L, it shall be made to the chief justice. The return of service shall be deemed a part of the return of the warrant and attached thereto.

M. Warrant: return.

Within seven days after termination of the warrant or the last renewal thereof, a return must be made thereon to the judge issuing the warrant by the applicant therefor, containing the following:

- a. a statement of the nature and location of the communications facilities, if any, and premise or places where the interceptions were made; and
- b. the periods of time during which such interceptions were made; and

- c. the names of the parties to the communications intercepted if known; and
- d. the original recording of the oral or wire communications intercepted, if any; and
- e. a statement attested under the pains and penalties of perjury by each person who heard oral or wire communications as a result of the interception authorized by the warrant, which were not recorded, stating everything that was overheard to the best of his recollection at the time of the execution of the statement.

N. Custody and secrecy of papers and recordings made pursuant to a warrant.

1. The contents of any wire or oral communication intercepted pursuant to a warrant issued pursuant to this section shall, if possible, be recorded on tape or wire or other similar device. Duplicate recordings may be made for use pursuant to subparagraphs 2 (a) and (b) of paragraph D for investigations. Upon examination of the return and a determination that it complies with this section, the issuing judge shall forthwith order that the application, all renewal applications, warrant, all renewal orders and the return thereto be transmitted to the chief justice by such persons as he shall designate. Their contents shall not be disclosed except as provided in this section. The application, renewal applications, warrant, the renewal order and the return or any one of them or any part of them may be transferred to any trial court, grand jury proceeding of any jurisdiction by any law enforcement or investigative officer or court officer designated by the chief justice and a trial justice may allow them to be disclosed in accordance with paragraph D, subparagraph 2, or paragraph O or any other applicable provision of this section.

The application, all renewal applications, warrant, all renewal orders and the return shall be stored in a secure place which shall be designated by the chief justice, to which access shall be denied to all persons except the chief justice or such court officers or administrative personnel of the court as he shall designate.

2. Any violation of the terms and conditions of any order of the chief justice, pursuant to the authority granted in this paragraph, shall be punished as a criminal contempt of court in addition to any other punishment authorized by law.

3. The application, warrant, renewal and return shall be kept for a period of five (5) years from the date of the issuance of the warrant or the last renewal thereof at which time they shall be destroyed by a person designated by the chief justice. Notice prior to the destruction shall be given to the applicant attorney general or his successor or the applicant district attorney or his successor and upon a showing of good cause to the chief justice, the application, warrant, renewal, and return may be kept for such additional period as the chief justice shall determine but in no event longer than the longest period of limitation for any designated offense specified in the warrant, after which time they must be destroyed by a person designated by the chief justice.

O. Introduction of evidence.

1. Notwithstanding any other provisions of this section or any order issued pursuant thereto, in any criminal trial where the commonwealth intends to offer in evidence any portions of the contents of any interception or any evidence derived therefrom the defendant shall be served with a complete copy of each document and item which make up each application, renewal application, warrant, renewal order, and return

pursuant to which the information was obtained, except that he shall be furnished a copy of any recording instead of the original. The service must be made at the arraignment of the defendant or, if a period in excess of thirty (30) days shall elapse prior to the commencement of the trial of the defendant, the service may be made at least thirty (30) days before the commencement of the criminal trial. Service shall be made in hand upon the defendant or his attorney by any investigative or law enforcement officer of the commonwealth. Return of the service required by this subparagraph including the date of service shall be entered into the record of trial of the defendant by the commonwealth and such return shall be deemed prima facie evidence of the service described therein. Failure by the commonwealth to make such service at the arraignment, or if delayed, at least thirty days before the commencement of the criminal trial, shall render such evidence illegally obtained for purposes of the trial against the defendant; and such evidence shall not be offered nor received at the trial notwithstanding the provisions of any other law or rules of court.

2. In any criminal trial where the commonwealth intends to offer in evidence any portions of a recording or transmission or any evidence derived therefrom, made pursuant to the exceptions set forth in paragraph B, subparagraph 4, of this section, the defendant shall be served with a complete copy of each recording or a statement under oath of the evidence overheard as a result of the transmission. The service must be made at the arraignment of the defendant or if a period in excess of thirty days shall elapse prior to the commencement of the trial of the defendant, the service may be made at least thirty days before the commencement of the criminal trial. Service shall be made in hand upon the defendant or his attorney by any investigative or law enforcement officer of the commonwealth. Return of the service required by this subparagraph

including the date of service shall be entered into the record of trial of the defendant by the commonwealth and such return shall be deemed prima facie evidence of the service described therein. Failure by the commonwealth to make such service at the arraignment, or if delayed at least thirty days before the commencement of the criminal trial, shall render such service illegally obtained for purposes of the trial against the defendant and such evidence shall not be offered nor received at the trial notwithstanding the provisions of any other law or rules of court.

P. Suppression of evidence.

Any person who is a defendant in a criminal trial in a court of the commonwealth may move to suppress the contents of any intercepted wire or oral communication or evidence derived therefrom, for the following reasons:

1. That the communication was unlawfully intercepted.
2. That the communication was not intercepted in accordance with the terms of this section.
3. That the application or renewal application fails to set forth facts sufficient to establish probable cause for the issuance of a warrant.
4. That the interception was not made in conformity with the warrant.
5. That the evidence sought to be introduced was illegally obtained.
6. That the warrant does not conform to the provisions of this section.

Q. Civil remedy.

Any aggrieved person whose oral or wire communications were intercepted, disclosed or used except as permitted or authorized by this section or whose personal or property interests or privacy were violated

by means of an interception except as permitted or authorized by this section shall have a civil cause of action against any person who so intercepts, discloses or uses such communications or who so violates his personal, property or privacy interest, and shall be entitled to recover from any such person—

1. actual damages but not less than liquidated damages computed at the rate of \$100 per day for each day of violation or \$1000, whichever is higher;
2. punitive damages; and
3. a reasonable attorney's fee and other litigation disbursements reasonably incurred. Good faith reliance on a warrant issued under this section shall constitute a complete defense to an action brought under this paragraph.

R. Annual report of interceptions of the general court.

On the second Friday of January, each year, the attorney general and each district attorney shall submit a report to the general court stating (1) the number of applications made for warrants during the previous year, (2) the name of the applicant, (3) the number of warrants issued, (4) the effective period for the warrants, (5) the number and designation of the offenses for which those applications were sought, and for each of the designated offenses the following: (a) the number of renewals, (b) the number of interceptions made during the previous year, (c) the number of indictments believed to be obtained as a result of those interceptions, (d) the number of criminal convictions obtained in trials where interception evidence or evidence derived therefrom was introduced. This report shall be a public document and be made available to the public at the offices of

the attorney general and district attorneys. In the event of failure to comply with the provisions of this paragraph any person may compel compliance by means of an action of mandamus.

before whom the hearing is had shall order. Nothing herein contained shall be construed to prevent the treasurer and receiver-general from deducting at any time the whole or any part of said tax with the interest accrued thereon which shall remain unpaid from any moneys which may be due from the commonwealth to such city or town.

Approved May 28, 1920.

AN ACT TO DEFINE AND PUNISH THE CRIME OF EAVES-
DROPPING. Chap. 558

Be it enacted, etc., as follows:

SECTION 1. Whoever, except when authorized by written permission of the attorney-general of the commonwealth, or of the district attorney for the district, secretly overhears, or attempts secretly to overhear or to have any other person secretly overhear, any spoken words in any building by using a device commonly known as a dictagraph or dictaphone, or however otherwise described, or any similar device or arrangement, or by tapping any wire, with intent to procure information concerning any official matter or to injure another, shall be guilty of the crime of eavesdropping and shall be punished by imprisonment for not more than two years or by a fine of not more than one thousand dollars, or by both such fine and imprisonment.

Penalty for procuring certain information by using a dictagraph or dictaphone, etc.

SECTION 2. Whoever, except when so authorized as aforesaid, either on his own account or as the servant or agent of another, permits or acquiesces in the installing of a device commonly known as a dictagraph or dictaphone or any similar device or arrangement, or the tapping of any wire, with intent to procure or knowing or intending that it will be used to procure information concerning any official matter or to injure another, shall be punished by imprisonment for not more than two years or by a fine of not more than one thousand dollars or by both such fine and imprisonment.

Penalty for permitting, etc., the installing of a dictagraph or dictaphone, etc., to procure certain information.

SECTION 3. Proof of the installation in any building of any device or arrangement which may be used for the purpose of violating the provisions of section one of this act by listening to any spoken words or proof of tapping of any wire, unless authorized as aforesaid and unless done with the consent of the owner or person in control of the building, shall be prima facie evidence of the commission of the crime of eavesdropping; but nothing contained in this act shall

Evidence of committing crime of eavesdropping, etc.

render it unlawful for any person to install and use such a device on premises under his exclusive control.

Form of indictment.

SECTION 4. The following form of complaint or indictment shall be sufficient to charge the offense of eavesdropping as defined in this act: That A. B. did commit the crime of eavesdropping.

Act not to apply to certain corporations, their employees, etc.

SECTION 5. This act shall not apply to a corporation subject to the jurisdiction of the department of public utilities of this commonwealth or to the jurisdiction of the interstate commerce commission, nor shall it apply to the employees of any such corporation while engaged in the conduct of its business.

Approved May 28, 1920.

Chap. 559 AN ACT RELATIVE TO THE PUBLICATION OF LISTS OF CANDIDATES AND FORMS OF QUESTIONS BEFORE STATE AND CITY ELECTIONS.

Be it enacted, etc., as follows:

1913, 835, § 269, etc., amended.

Lists of candidates, etc., state and city elections, to be published.

Section two hundred and sixty-nine of chapter eight hundred and thirty-five of the acts of nineteen hundred and thirteen, as amended by chapter fifty-four of the General Acts of nineteen hundred and nineteen, is hereby further amended by striking out the said section and substituting the following: — *Section 269.* Before every state election, the secretary of the commonwealth shall cause to be published a list of all candidates to be voted for in each senatorial district, except that in the county of Suffolk the publication shall be of all candidates to be voted for therein. He shall also publish with said lists the form of any question to be submitted to the voters. Before every city election, the city clerk, or in Boston the election commissioners, shall cause to be published a list of all candidates to be voted for in their respective cities, and the form of any question to be submitted to the voters at such election. Such lists and questions shall in all cases be in the form, as near as may be, in which they are to appear upon the official ballot, and for state elections shall be printed in at least four newspapers, if there be so many, published in English in each senatorial district, or in the county of Suffolk, as the case may be. Such publication shall, so far as is practicable, be in newspapers representing the two political parties, and at such reasonable cost as the secretary may determine. For city elections the publication shall be made in at least two news-

identification number thereon. Whoever violates this section shall be punished by a fine of five hundred dollars. Each such violation shall constitute a separate offense.

SECTION 16. Section 12B of said chapter 269, as appearing in section 31 of chapter 688 of the acts of 1957, is hereby amended by striking out the third sentence and inserting in place thereof the following sentence:—Whoever violates this section shall be punished by a fine of not more than one hundred dollars, and the air rifle or BB gun or other weapon shall be confiscated.

SECTION 17. Section 12D of said chapter 269, added by section 33 of said chapter 688, is hereby amended by striking out the second sentence and inserting in place thereof the following sentence:—Whoever violates this section shall be punished by a fine of not less than fifty nor more than five hundred dollars, and may be arrested without a warrant.

SECTION 18. The provisions of section one hundred and twenty-nine B of chapter one hundred and forty of the General Laws, inserted by section seven of this act, of section one hundred and thirty of said chapter one hundred and forty, inserted by section eight of this act, and of section ten of chapter two hundred and sixty-nine of the General Laws, inserted by section twelve of this act, shall not apply until January first, nineteen hundred and sixty-nine; provided, however, that any person may apply for the firearm identification card as provided in said section one hundred and twenty-nine B at any time after the effective date of said section seven and, pending the issuance or denial of said firearm identification card, written receipt for the fee paid shall serve as a valid substitute for said firearm identification card.

Approved July 20, 1968.

Chap. 738. AN ACT FURTHER REGULATING WIRETAPPING AND EAVES-DROPPING.

Be it enacted, etc., as follows:

SECTION 1. Chapter 272 of the General Laws is hereby amended by striking out section 99, as amended by chapter 449 of the acts of 1959, and inserting in place thereof the following section:—

Section 99. Interception of wire and oral communications.—

A. Preamble.

The general court finds that organized crime exists within the commonwealth and that the increasing activities of organized crime constitute a grave danger to the public welfare and safety. Organized crime, as it exists in the commonwealth today, consists of a continuing conspiracy among highly organized and disciplined groups to engage in supplying illegal goods and services. In supplying these goods and services organized crime commits unlawful acts and employs brutal and violent tactics. Organized crime is infiltrating legitimate business activities and depriving honest businessmen of the right to make a living.

The general court further finds that because organized crime carries on its activities through layers of insulation and behind a wall of secrecy, government has been unsuccessful in curtailing and eliminat-

ing it. Normal investigative procedures are not effective in the investigation of illegal acts committed by organized crime. Therefore, law enforcement officials must be permitted to use modern methods of electronic surveillance, under strict judicial supervision, when investigating these organized criminal activities.

The general court further finds that the uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the commonwealth. Therefore, the secret use of such devices by private individuals must be prohibited. The use of such devices by law enforcement officials must be conducted under strict judicial supervision and should be limited to the investigation of organized crime.

B. Definitions. As used in this section—

1. The term “wire communication” means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception.

2. The term “oral communication” means speech, except such speech as is transmitted over the public air waves by radio or other similar device.

3. The term “intercepting device” means any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication other than a hearing aid or similar device which is being used to correct subnormal hearing to normal and other than any telephone or telegraph instrument, equipment, facility, or a component thereof, (a) furnished to a subscriber or user by a communications common carrier in the ordinary course of its business under its tariff and being used by the subscriber or user in the ordinary course of its business; or (b) being used by a communications common carrier in the ordinary course of its business.

4. The term “interception” means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication; provided that it shall not constitute an interception for an investigative or law enforcement officer, as defined in this section, to record or transmit a wire or oral communication if the officer is a party to such communication or has been given prior authorization to record or transmit the communication by such a party and if recorded or transmitted in the course of an investigation of a designated offense as defined herein.

5. The term “contents”, when used with respect to any wire or oral communication, means any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication.

6. The term “aggrieved person” means any individual who was a party to an intercepted wire or oral communication or who was named in the warrant authorizing the interception, or who would otherwise have standing to complain that his personal or property interest or privacy was invaded in the course of an interception.

7. The term “designated offense” shall include the following offenses in connection with organized crime as defined in the preamble: arson,

assault and battery with a dangerous weapon, extortion, bribery, burglary, embezzlement, forgery, gaming in violation of section seventeen of chapter two hundred and seventy-one of the general laws, intimidation of a witness or juror, kidnapping, larceny, lending of money or things of value in violation of the general laws, mayhem, murder, any offense involving the possession or sale of a narcotic or harmful drug, perjury, prostitution, robbery, subornation of perjury, any violation of this section, being an accessory to any of the foregoing offenses and conspiracy or attempt or solicitation to commit any of the foregoing offenses.

8. The term "investigative or law enforcement officer" means any officer of the United States, a state or a political subdivision of a state, who is empowered by law to conduct investigations of, or to make arrests for, the designated offenses, and any attorney authorized by law to participate in the prosecution of such offenses.

9. The term "judge of competent jurisdiction" means any justice of the superior court of the commonwealth.

10. The term "chief justice" means the chief justice of the superior court of the commonwealth.

11. The term "issuing judge" means any justice of the superior court who shall issue a warrant as provided herein or in the event of his disability or unavailability any other judge of competent jurisdiction designated by the chief justice.

12. The term "communication common carrier" means any person engaged as a common carrier in providing or operating wire communication facilities.

13. The term "person" means any individual, partnership, association, joint stock company, trust, or corporation, whether or not any of the foregoing is an officer, agent or employee of the United States, a state, or a political subdivision of a state.

14. The terms "sworn" or "under oath" as they appear in this section shall mean an oath or affirmation or a statement subscribed to under the pains and penalties of perjury.

15. The terms "applicant attorney general" or "applicant district attorney" shall mean the attorney general of the commonwealth or a district attorney of the commonwealth who has made application for a warrant pursuant to this section.

16. The term "exigent circumstances" shall mean the showing of special facts to the issuing judge as to the nature of the investigation for which a warrant is sought pursuant to this section which require secrecy in order to obtain the information desired from the interception sought to be authorized.

C. Offenses.

1. Interception, oral communications prohibited.

Except as otherwise specifically provided in this section any person who—

willfully commits an interception, attempts to commit an interception, or procures any other person to commit an interception or to attempt to commit an interception of any wire or oral communication shall be fined not more than ten thousand dollars, or imprisoned in the state prison for not more than five years, or imprisoned in a jail or house of correction for not more than two and one half years, or both so fined and given one such imprisonment.

Proof of the installation of any intercepting device by any person under circumstances evincing an intent to commit an interception, which is not authorized or permitted by this section, shall be prima facie evidence of a violation of this subparagraph.

2. Editing of tape recordings in judicial proceeding prohibited.

Except as otherwise specifically provided in this section any person who—

willfully edits, alters or tampers with any tape, transcription or recording of oral or wire communications by any means, or attempts to edit, alter or tamper with any tape, transcription or recording of oral or wire communications by any means with the intent to present in any judicial proceeding or proceeding under oath, or who presents such recording or permits such recording to be presented in any judicial proceeding or proceeding under oath, without fully indicating the nature of the changes made in the original state of the recording, shall be fined not more than ten thousand dollars (\$10,000.00) or imprisoned in the state prison for not more than five years or imprisoned in a jail or house of correction for not more than two years or both so fined and given one such imprisonment.

3. Disclosure or use of wire or oral communications prohibited.

Except as otherwise specifically provided in this section any person who—

a. willfully discloses or attempts to disclose to any person the contents of any wire or oral communication, knowing that the information was obtained through interception; or

b. willfully uses or attempts to use the contents of any wire or oral communication, knowing that the information was obtained through interception, shall be guilty of a misdemeanor punishable by imprisonment in a jail or a house of correction for not more than two years or by a fine of not more than five thousand dollars or both.

4. Disclosure of contents of applications, warrants, renewals, and returns prohibited.

Except as otherwise specifically provided in this section any person who—

willfully discloses to any person, any information concerning or contained in, the application for, the granting or denial of orders for interception, renewals, notice or return on an ex parte order granted pursuant to this section, or the contents of any document, tape, or recording kept in accordance with paragraph N, shall be guilty of a misdemeanor punishable by imprisonment in a jail or a house of correction for not more than two years or by a fine of not more than five thousand dollars or both.

5. Possession of interception devices prohibited.

A person who possesses any intercepting device under circumstances evincing an intent to commit an interception not permitted or authorized by this section, or a person who permits an intercepting device to be used or employed for an interception not permitted or authorized by this section, or a person who possesses an intercepting device knowing that the same is intended to be used to commit an interception not permitted or authorized by this section, shall be guilty of a misdemeanor punishable by imprisonment in a jail or house of correction for not more than two years or by a fine of not more than five thousand dollars or both.

The installation of any such intercepting device by such person or with his permission or at his direction shall be prima facie evidence of possession as required by this subparagraph.

6. Any person who permits or on behalf of any other person commits or attempts to commit, or any person who participates in a conspiracy to commit or to attempt to commit, or any accessory to a person who commits a violation of subparagraphs 1 through 5 of paragraph C of this section shall be punished in the same manner as is provided for the respective offenses as described in subparagraphs 1 through 5 of paragraph C.

D. Exemptions.

1. Permitted interception of wire or oral communications.

It shall not be a violation of this section—

a. for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the carrier of such communication, or which is necessary to prevent the use of such facilities in violation of section fourteen A of chapter two hundred and sixty-nine of the general laws; provided, that said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

b. for persons to possess an office intercommunication system which is used in the ordinary course of their business or to use such office intercommunication system in the ordinary course of their business.

c. for investigative and law enforcement officers of the United States of America to violate the provisions of this section if acting pursuant to authority of the laws of the United States and within the scope of their authority.

d. for any person duly authorized to make specified interceptions by a warrant issued pursuant to this section.

2. Permitted disclosure and use of intercepted wire or oral communications.

a. Any investigative or law enforcement officer, who, by any means authorized by this section, has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may disclose such contents or evidence in the proper performance of his official duties.

b. Any investigative or law enforcement officer, who, by any means authorized by this section has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may use such contents or evidence in the proper performance of his official duties.

c. Any person who has obtained, by any means authorized by this section, knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may disclose such contents while giving testimony under oath or affirmation in any criminal proceeding in any court of the United States or of any state or in any federal or state grand jury proceeding.

d. The contents of any wire or oral communication intercepted pursuant to a warrant in accordance with the provisions of this section, or evidence derived therefrom, may otherwise be disclosed only upon a showing of good cause before a judge of competent jurisdiction.

e. No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this section shall lose its privileged character.

E. Warrants: when issuable:

A warrant may issue only:

1. Upon a sworn application in conformity with this section; and
2. Upon a showing by the applicant that there is probable cause to believe that a designated offense has been, is being, or is about to be committed and that evidence of the commission of such an offense may thus be obtained or that information which will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit a designated offense may thus be obtained; and
3. Upon a showing by the applicant that normal investigative procedures have been tried and have failed or reasonably appear unlikely to succeed if tried.

F. Warrants: application.

1. Application. The attorney general, any assistant attorney general specially designated by the attorney general, any district attorney, or any assistant district attorney specially designated by the district attorney may apply ex parte to a judge of competent jurisdiction for a warrant to intercept wire or oral communications. Each application ex parte for a warrant must be in writing, subscribed and sworn to by the applicant authorized by this subparagraph.

2. The application must contain the following:

a. A statement of facts establishing probable cause to believe that a particularly described designated offense has been, is being, or is about to be committed; and

b. A statement of facts establishing probable cause to believe that oral or wire communications of a particularly described person will constitute evidence of such designated offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit a designated offense; and

c. That the oral or wire communications of the particularly described person or persons will occur in a particularly described place and premises or over particularly described telephone or telegraph lines; and

d. A particular description of the nature of the oral or wire communications sought to be overheard; and

e. A statement that the oral or wire communications sought are material to a particularly described investigation or prosecution and that such conversations are not legally privileged; and

f. A statement of the period of time for which the interception is required to be maintained. If practicable, the application should designate hours of the day or night during which the oral or wire communications may be reasonably expected to occur. If the nature of

the investigation is such that the authorization for the interception should not automatically terminate when the described oral or wire communications have been first obtained, the application must specifically state facts establishing probable cause to believe that additional oral or wire communications of the same nature will occur thereafter; and

g. If it is reasonably necessary to make a secret entry upon a private place and premises in order to install an intercepting device to effectuate the interception, a statement to such effect; and

h. If a prior application has been submitted or a warrant previously obtained for interception of oral or wire communications, a statement fully disclosing the date, court, applicant, execution, results, and present status thereof; and

i. If there is good cause for requiring the postponement of service pursuant to paragraph L, subparagraph 2, a description of such circumstances, including reasons for the applicant's belief that secrecy is essential to obtaining the evidence or information sought.

3. Allegations of fact in the application may be based either upon the personal knowledge of the applicant or upon information and belief. If the applicant personally knows the facts alleged, it must be so stated. If the facts establishing such probable cause are derived in whole or part from the statements of persons other than the applicant, the sources of such information and belief must be either disclosed or described; and the application must contain facts establishing the existence and reliability of any informant and the reliability of the information supplied by him. The application must also state, so far as possible, the basis of the informant's knowledge or belief. If the applicant's information and belief is derived from tangible evidence or recorded oral evidence, a copy or detailed description thereof should be annexed to or included in the application. Affidavits of persons other than the applicant may be submitted in conjunction with the application if they tend to support any fact or conclusion alleged therein. Such accompanying affidavits may be based either on personal knowledge of the affiant or information and belief, with the source thereof, and reason therefor, specified.

G. Warrants: application to whom made.

Application for a warrant authorized by this section must be made to a judge of competent jurisdiction in the county where the interception is to occur, or the county where the office of the applicant is located, or in the event that there is no judge of competent jurisdiction sitting in said county at such time, to a judge of competent jurisdiction sitting in Suffolk County; except that for these purposes, the office of the attorney general shall be deemed to be located in Suffolk County.

H. Warrants: application how determined.

1. If the application conforms to paragraph F, the issuing judge may examine under oath any person for the purpose of determining whether probable cause exists for the issuance of the warrant pursuant to paragraph E. A verbatim transcript of every such interrogation or examination must be taken, and a transcription of the same, sworn to by the stenographer, shall be attached to the application and be deemed a part thereof.

2. If satisfied that probable cause exists for the issuance of a warrant the judge may grant the application and issue a warrant in accordance with paragraph I. The application and an attested copy of the warrant shall be retained by the issuing judge and transported to the chief justice of the superior court in accordance with the provisions of paragraph N of this section.

3. If the application does not conform to paragraph F, or if the judge is not satisfied that probable cause has been shown sufficient for the issuance of a warrant, the application must be denied.

I. Warrants: form and content.

A warrant must contain the following:

1. The subscription and title of the issuing judge; and
 2. The date of issuance, the date of effect, and termination date which in no event shall exceed thirty days from the date of effect. The warrant shall permit interception of oral or wire communications for a period not to exceed fifteen days. If physical installation of a device is necessary, the thirty-day period shall begin upon the date of installation. If the effective period of the warrant is to terminate upon the acquisition of particular evidence or information or oral or wire communication, the warrant shall so provide; and

3. A particular description of the person and the place, premises or telephone or telegraph line upon which the interception may be conducted; and

4. A particular description of the nature of the oral or wire communications to be obtained by the interception including a statement of the designated offense to which they relate; and

5. An express authorization to make secret entry upon a private place or premises to install a specified intercepting device, if such entry is necessary to execute the warrant; and

6. A statement providing for service of the warrant pursuant to paragraph L except that if there has been a finding of good cause shown requiring the postponement of such service, a statement of such finding together with the basis therefor must be included and an alternative direction for deferred service pursuant to paragraph L, subparagraph 2.

J. Warrants: renewals.

1. Any time prior to the expiration of a warrant or a renewal thereof, the applicant may apply to the issuing judge for a renewal thereof with respect to the same person, place, premises or telephone or telegraph line. An application for renewal must incorporate the warrant sought to be renewed together with the application therefor and any accompanying papers upon which it was issued. The application for renewal must set forth the results of the interceptions thus far conducted. In addition, it must set forth present grounds for extension in conformity with paragraph F, and the judge may interrogate under oath and in such an event a transcript must be provided and attached to the renewal application in the same manner as is set forth in subparagraph 1 of paragraph H.

2. Upon such application, the judge may issue an order renewing the warrant and extending the authorization for a period not exceeding fifteen (15) days from the entry thereof. Such an order shall specify the grounds for the issuance thereof. The application and an attested

copy of the order shall be retained by the issuing judge to be transported to the chief justice in accordance with the provisions of subparagraph N of this section. In no event shall a renewal be granted which shall terminate later than two years following the effective date of the warrant.

K. Warrants: manner and time of execution.

1. A warrant may be executed pursuant to its terms anywhere in the commonwealth.

2. Such warrant may be executed by the authorized applicant, personally or by any investigative or law enforcement officer of the commonwealth designated by him for the purpose.

3. The warrant may be executed according to its terms during the hours specified therein, and for the period therein authorized, or a part thereof. The authorization shall terminate upon the acquisition of the oral or wire communications, evidence or information described in the warrant. Upon termination of the authorization in the warrant and any renewals thereof, the interception must cease at once, and any device installed for the purpose of the interception must be removed as soon thereafter as practicable. Entry upon private premises for the removal of such device is deemed to be authorized by the warrant.

L. Warrants: service thereof.

1. Prior to the execution of a warrant authorized by this section or any renewal thereof, an attested copy of the warrant or the renewal must, except as otherwise provided in subparagraph 2 of this paragraph, be served upon a person whose oral or wire communications are to be obtained, and if an intercepting device is to be installed, upon the owner, lessee, or occupant of the place or premises, or upon the subscriber to the telephone or owner or lessee of the telegraph line, described in the warrant.

2. If the application specially alleges exigent circumstances requiring the postponement of service and the issuing judge finds that such circumstances exist, the warrant may provide that an attested copy thereof may be served within thirty days after the expiration of the warrant or, in case of any renewals thereof, within thirty days after the expiration of the last renewal; except that upon a showing of important special facts which set forth the need for continued secrecy to the satisfaction of the issuing judge, said judge may direct that the attested copy of the warrant be served on such parties as are required by this section at such time as may be appropriate in the circumstances but in no event may he order it to be served later than three (3) years from the time of expiration of the warrant or the last renewal thereof. In the event that the service required herein is postponed in accordance with this paragraph, in addition to the requirements of any other paragraph of this section, service of an attested copy of the warrant shall be made upon any aggrieved person who should reasonably be known to the person who executed, or obtained the warrant as a result of the information obtained from the interception authorized thereby.

3. The attested copy of the warrant shall be served on persons required by this section by an investigative or law enforcement officer of the commonwealth by leaving the same at his usual place of abode, or in hand, or if this is not possible by mailing the same by certified

or registered mail to his last known place of abode. A return of service shall be made to the issuing judge, except, that if such service is postponed as provided in subparagraph 2 of paragraph L, it shall be made to the chief justice. The return of service shall be deemed a part of the return of the warrant and attached thereto.

M. Warrant: return.

Within seven days after termination of the warrant or the last renewal thereof, a return must be made thereon to the judge issuing the warrant by the applicant therefor, containing the following:

a. a statement of the nature and location of the communications facilities, if any, and premise or places where the interceptions were made; and

b. the periods of time during which such interceptions were made; and

c. the names of the parties to the communications intercepted if known; and

d. the original recording of the oral or wire communications intercepted, if any; and

e. a statement attested under the pains and penalties of perjury by each person who heard oral or wire communications as a result of the interception authorized by the warrant, which were not recorded, stating everything that was overheard to the best of his recollection at the time of the execution of the statement.

N. Custody and secrecy of papers and recordings made pursuant to a warrant.

1. The contents of any wire or oral communication intercepted pursuant to a warrant issued pursuant to this section shall, if possible, be recorded on tape or wire or other similar device. Duplicate recordings may be made for use pursuant to subparagraphs 2 (a) and (b) of paragraph D for investigations. Upon examination of the return and a determination that it complies with this section, the issuing judge shall forthwith order that the application, all renewal applications, warrant, all renewal orders and the return thereto be transmitted to the chief justice by such persons as he shall designate. Their contents shall not be disclosed except as provided in this section. The application, renewal applications, warrant, the renewal order and the return or any one of them or any part of them may be transferred to any trial court, grand jury proceeding of any jurisdiction by any law enforcement or investigative officer or court officer designated by the chief justice and a trial justice may allow them to be disclosed in accordance with paragraph D, subparagraph 2, or paragraph O or any other applicable provision of this section.

The application, all renewal applications, warrant, all renewal orders and the return shall be stored in a secure place which shall be designated by the chief justice, to which access shall be denied to all persons except the chief justice or such court officers or administrative personnel of the court as he shall designate.

2. Any violation of the terms and conditions of any order of the chief justice, pursuant to the authority granted in this paragraph, shall be punished as a criminal contempt of court in addition to any other punishment authorized by law.

3. The application, warrant, renewal and return shall be kept for a period of five (5) years from the date of the issuance of the warrant

or the last renewal thereof at which time they shall be destroyed by a person designated by the chief justice. Notice prior to the destruction shall be given to the applicant attorney general or his successor or the applicant district attorney or his successor and upon a showing of good cause to the chief justice, the application, warrant, renewal, and return may be kept for such additional period as the chief justice shall determine but in no event longer than the longest period of limitation for any designated offense specified in the warrant, after which time they must be destroyed by a person designated by the chief justice.

O. Introduction of evidence.

1. Notwithstanding any other provisions of this section or any order issued pursuant thereto, in any criminal trial where the commonwealth intends to offer in evidence any portions of the contents of any interception or any evidence derived therefrom the defendant shall be served with a complete copy of each document and item which make up each application, renewal application, warrant, renewal order, and return pursuant to which the information was obtained, except that he shall be furnished a copy of any recording instead of the original. The service must be made at the arraignment of the defendant or, if a period in excess of thirty (30) days shall elapse prior to the commencement of the trial of the defendant, the service may be made at least thirty (30) days before the commencement of the criminal trial. Service shall be made in hand upon the defendant or his attorney by any investigative or law enforcement officer of the commonwealth. Return of the service required by this subparagraph including the date of service shall be entered into the record of trial of the defendant by the commonwealth and such return shall be deemed prima facie evidence of the service described therein. Failure by the commonwealth to make such service at the arraignment, or if delayed, at least thirty days before the commencement of the criminal trial, shall render such evidence illegally obtained for purposes of the trial against the defendant; and such evidence shall not be offered nor received at the trial notwithstanding the provisions of any other law or rules of court.

2. In any criminal trial where the commonwealth intends to offer in evidence any portions of a recording or transmission or any evidence derived therefrom, made pursuant to the exceptions set forth in paragraph B, subparagraph 4, of this section, the defendant shall be served with a complete copy of each recording or a statement under oath of the evidence overheard as a result of the transmission. The service must be made at the arraignment of the defendant or if a period in excess of thirty days shall elapse prior to the commencement of the trial of the defendant, the service may be made at least thirty days before the commencement of the criminal trial. Service shall be made in hand upon the defendant or his attorney by any investigative or law enforcement officer of the commonwealth. Return of the service required by this subparagraph including the date of service shall be entered into the record of trial of the defendant by the commonwealth and such return shall be deemed prima facie evidence of the service described therein. Failure by the commonwealth to make such service at the arraignment, or if delayed at least thirty days before the commencement of the criminal trial, shall render such service illegally

obtained for purposes of the trial against the defendant and such evidence shall not be offered nor received at the trial notwithstanding the provisions of any other law or rules of court.

P. Suppression of evidence.

Any person who is a defendant in a criminal trial in a court of the commonwealth may move to suppress the contents of any intercepted wire or oral communication or evidence derived therefrom, for the following reasons:

1. That the communication was unlawfully intercepted.
2. That the communication was not intercepted in accordance with the terms of this section.
3. That the application or renewal application fails to set forth facts sufficient to establish probable cause for the issuance of a warrant.
4. That the interception was not made in conformity with the warrant.
5. That the evidence sought to be introduced was illegally obtained.
6. That the warrant does not conform to the provisions of this section.

Q. Civil remedy.

Any aggrieved person whose oral or wire communications were intercepted, disclosed or used except as permitted or authorized by this section or whose personal or property interests or privacy were violated by means of an interception except as permitted or authorized by this section shall have a civil cause of action against any person who so intercepts, discloses or uses such communications or who so violates his personal, property or privacy interest, and shall be entitled to recover from any such person—

1. actual damages but not less than liquidated damages computed at the rate of \$100 per day for each day of violation or \$1000, whichever is higher;
2. punitive damages; and
3. a reasonable attorney's fee and other litigation disbursements reasonably incurred. Good faith reliance on a warrant issued under this section shall constitute a complete defense to an action brought under this paragraph.

R. Annual report of interceptions of the general court.

On the second Friday of January, each year, the attorney general and each district attorney shall submit a report to the general court stating (1) the number of applications made for warrants during the previous year, (2) the name of the applicant, (3) the number of warrants issued, (4) the effective period for the warrants, (5) the number and designation of the offenses for which those applications were sought, and for each of the designated offenses the following: (a) the number of renewals, (b) the number of interceptions made during the previous year, (c) the number of indictments believed to be obtained as a result of those interceptions, (d) the number of criminal convictions obtained in trials where interception evidence or evidence derived therefrom was introduced. This report shall be a public document and be made available to the public at the offices of the attorney general and district attorneys. In the event of failure to comply with the provisions of this paragraph any person may compel compliance by means of an action of mandamus.

SECTION 2. Chapter 166 of the General Laws is hereby amended by adding the following after section 43:—

Section 44. Service Observing, Interception.—Service observing of telephone lines conducted by telephone companies for the purpose of determining the quality of transmission or for any other purpose shall cease as soon as a connection is established between the users of the telephone line. Notwithstanding any other law, the line of any subscriber of a telephone company shall not be monitored by a telephone company for the purpose of service observing or random monitoring, if he shall so request in writing to the telephone company. Any subscriber may seek an injunction in the superior court to prevent such service observing or random monitoring.

The department of public utilities shall require that each telephone company file annually with it a complete report of all service observing activity carried on by any telephone company including the number of calls monitored during the previous calendar year, all rules and regulations of the telephone companies for such service observing, a complete description of the location of each service observing facility, for each past calendar year the number of employees engaged in service observing and a statement of the expenses incurred for such service observing to include salaries, cost of capital equipment and maintenance and replacement costs of such equipment, and administrative expenses incurred. The department shall also conduct periodic inspections at least semiannually of such service observing to determine whether or not it complies with this section and the accuracy of the reports filed. In the event of the failure of any telephone company to comply with this section the department of public utilities must order that the activity cease until compliance is obtained and may seek an enforcement order in the Superior Court of Suffolk County.

SECTION 3. Section 25 of chapter 147, of the General Laws is amended by adding the following sentence after the last sentence of the first paragraph:—No person convicted of a violation of section ninety-nine or ninety-nine A of chapter two hundred and seventy-two of the general laws shall be granted a license and any license previously granted to such person shall be revoked.

SECTION 4. Section one hundred of chapter two hundred and seventy-two of the general laws is hereby repealed.

SECTION 5. Section one hundred and one of chapter two hundred and seventy-two of the general laws is hereby repealed.

SECTION 6. Section one hundred and two of chapter two hundred and seventy-two of the general laws is hereby repealed.

SECTION 7. If any provision of this act or application thereof to any person or circumstances is held invalid, such invalidity shall not affect other provisions or applications of the act which can be given effect without the invalid provision or application, and to this end the provisions of this act are declared to be severable.

Approved July 20, 1968.

SENATE No. 201

By Mr. Umana, a petition of Mario Umana that provision be made for an investigation and study by a special commission (including members of the General Court) relative to illegal use of electronic recording devices, wireless taps or electronic taps or similar devices and arrangements. The Judiciary.

The Commonwealth of Massachusetts

In the Year One Thousand Nine Hundred and Sixty-Four.

RESOLVE PROVIDING FOR AN INVESTIGATION AND STUDY BY A SPECIAL COMMISSION RELATIVE TO ILLEGAL USE OF ELECTRONIC RECORDING DEVICES, WIRELESS TAPS OR ELECTRONIC TAPS OR SIMILAR DEVICES AND ARRANGEMENTS.

1 *Resolved*, That a special commission, to consist of three
2 members of the senate, five members of the house of repre-
3 sentatives and three persons to be appointed by the governor,
4 is hereby established for the purpose of making an investiga-
5 tion and study of the laws relative to eavesdropping and the
6 use of any electronic recording device, or wireless tap or
7 electronic tap, however described, or any similar device or
8 arrangement in connection therewith, and the illegal use of
9 any such devices or arrangements and the extent thereof,
10 with a view to strengthening the laws relative to eavesdrop-
11 ping and the use of wire tapping recording devices.

By Mr. St. Cyr of Millis, petition of Edward W. Brooke and Alan Paul Danovitch for legislation to repeal the present wiretapping statute and providing for a new statute in relation thereto. The Judiciary.

The Commonwealth of Massachusetts

In the Year One Thousand Nine Hundred and Sixty-Seven.

AN ACT REPEALING THE PRESENT WIRETAPPING STATUTE AND PROVIDING FOR A NEW STATUTE IN RELATION THERETO.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

1 Sections 99 and 99A of chapter 272 of the General Laws,
2 as most recently amended by chapter 449 of the acts of 1959,
3 are hereby repealed and the following sections substituted
4 in place thereof:—

5 *Section 99. Eavesdropping.*— Except as otherwise spe-
6 cifically provided in this section, or in section 99B, it shall be
7 unlawful for any person: (1) willfully to overhear, attempt
8 to overhear, or procure any other person to overhear, or at-
9 tempt to overhear any spoken words at any place by using
10 electronic amplifying, transmitting, or recording device, or
11 by any similar device or arrangement, without the consent or
12 knowledge of all parties engaging in the conversation; (2)
13 willfully to disclose, or attempt to disclose, to any person the
14 contents of any conversation if the person disclosing that
15 information knows or has reason to know that that informa-
16 tion was obtained by a procedure which violates paragraph
17 (1); (3) willfully to use, or attempt to use, the contents of
18 any conversation if the person using that information knows
19 or has reason to know that that information was obtained by
20 a procedure which violates paragraph (1); (4) willfully to
21 acquiesce in the installing of any device which is to be used or
22 is used in a manner which violates paragraph (1); provided,
23 that nothing in this section shall be interpreted to prevent a
24 news agency or an employee thereof from using the accepted

25 tools and equipment of that news media in the course of re-
26 porting a public and newsworthy event; and *provided further*,
27 that nothing in this section shall be interpreted to prevent the
28 use by private persons or businesses of any device used for
29 security or business purposes, as long as adequate warning
30 is given to the public that such devices are in operation.

31 A person violating this section shall be guilty of the crime
32 of eavesdropping and shall be punished by imprisonment for
33 not more than five years or by a fine of not more than ten
34 thousand dollars, or both.

35 (B.) *Right of Civil Action.* — Any party to a conversation
36 which is eavesdropped upon in violation of Part A, and who
37 has been damaged due to such violation, may sue the violator
38 or violators therefor and shall recover threefold the damages
39 by him sustained, and the cost of the suit, including a reason-
40 able attorney's fee, and no award shall be less than five hun-
41 dred dollars.

42 *Section 99A. Wiretapping.* — Except as otherwise specifi-
43 cally provided in this section or in section 99B, it shall be
44 unlawful for any person:— (1) willfully to intercept, at-
45 tempt to intercept, or procure any other person to intercept,
46 or attempt to intercept, any wire communication without the
47 consent or knowledge of all parties engaging in the commu-
48 nication; (2) willfully to disclose or attempt to disclose to
49 any other person the contents of any wire communication
50 if the person disclosing that information knows or has reason
51 to know that that information was obtained by a procedure
52 which violates paragraph (1); (3) willfully to use or attempt
53 to use the contents of any wire communication if the person
54 using that information knows or has reason to know that
55 that information was obtained by a procedure which violates
56 paragraph (1); (4) willfully to acquiesce in the installing
57 of any device which is to be used, or is used in a manner
58 which violates paragraph (1); (5) who is an employee of
59 any communications common carrier, and has knowledge ob-
60 tained during the course of his duties for that carrier, of
61 any violation of paragraph (1) to fail to report such knowl-
62 edge to a district attorney or the attorney general of the com-
63 monwealth; provided, that it shall not be unlawful under
64 this section for an operator of a switchboard, or an officer,
65 agent or employee of any communication common carrier,

66 whose facilities are used in the transmission of a wire com-
67 munication to intercept, disclose or use that communication
68 in the normal course of his employment while engaged in any
69 activity which is a necessary incident of the rendition of
70 service.

71 A person violating this section shall be guilty of the crime
72 of Wiretapping and shall be punished by imprisonment for
73 not more than five years, or by a fine of not more than two
74 thousand dollars, or both.

75 (B) *Right of Civil Action.* — Any party to a conversation
76 which is intercepted in violation of Part A, and who has been
77 damaged due to such violation, may sue the violator or vio-
78 lators therefor and shall recover threefold the damages by
79 him sustained, and the cost of the suit, including a reasonable
80 attorney's fee, and no award shall be less than five hundred
81 dollars.

82 *Section 99B. Court Order to Eavesdrop or Wiretap.* —
83 Any justice of the supreme judicial court, or a justice of the
84 superior court, may, upon proper application by either a dis-
85 trict attorney or the district attorney of the commonwealth
86 grant an *ex parte* order allowing such officer to order an elec-
87 tronic eavesdrop or a wiretap.

88 (1) Such application to be proper, must satisfy the judge
89 that the following requirements have been substantially met.

90 (a) It must be personally signed by either a district attor-
91 ney or the attorney general of the commonwealth, unless it
92 can be shown that that official is unavailable and that delay
93 would endanger either human life or the public safety. In
94 such case, the application must be signed by the highest
95 ranking official available.

96 (b) It must contain a full and complete statement of the
97 facts and circumstances relied on by the applicant including
98 but not limited to: the crime or crimes involved; the infor-
99 mation expected to be obtained; the results of previous inves-
100 tigation which led to the application; and the sources of the
101 information leading to the application, unless such sources
102 are confidential.

103 (c) It must state the nature and location of the premises
104 which are to be eavesdropped upon, or the wire to be tapped,
105 and the person or persons whose conversations are to be over-
106 heard or intercepted. In the case of eavesdropping, the appli-

107 cation shall specify as precisely as possible the building, and
108 the particular rooms in a building, to be bugged. In the case of
109 a telephone, the exact number of the line must be specified,
110 as well as the names of the individuals to whom the phone
111 is listed, and who regularly use the phone.

112 (a) It must state all previous applications in the same
113 matter which involved the same premises, facilities or indi-
114 viduals, and the action taken by the judge on each application.

115 (e) It must allege that other methods of investigation have
116 proven to be or are presumptively inadequate and that there
117 is a reasonable cause to believe that eavesdropping or a wire-
118 tap will be successful.

119 (2) If the judge is not satisfied that the application sub-
120 substantially complies with the requirements of Part A, he
121 may require the applicant to furnish additional information
122 in support of the application.

123 (3) If the judge is satisfied that the application sub-
124 stantially complies with Part A, and specifically, that other
125 methods of investigation would be inadequate, he may enter
126 an *ex parte* order granting leave to the applicant to eavesdrop
127 or wiretap in conformance with the terms of the order. Such
128 order shall only be granted where there are reasonable
129 grounds to believe that:—

130 (a) It is necessary to save human life; or,

131 (b) In the case of a wiretap, where communications facil-
132 ity itself is an instrumentality of the crime alleged; or,

133 (c) That evidence of a felony may thus be obtained; or,

134 (d) The security of the commonwealth or the public safety
135 is endangered.

136 (4) Such order shall be limited to sixty days, at which
137 time it shall be renewable, in the discretion of the judge, for
138 additional periods of thirty days. An application for renewal
139 must be filed which shall contain as much information as the
140 judge shall deem necessary.

141 (5) Such order shall describe or identify the person or
142 persons who are authorized to implement it, or the person or
143 persons under whose supervision it shall be implemented.

144 (6) An order to eavesdrop shall specify with as much pre-
145 ciseness as possible, the building, and the particular room or
146 rooms in a building, to be bugged. An order to wiretap shall

147 specify the particular wire to be intercepted, if a telephone,
148 by its number.

149 (7) Such order shall specify the purpose for which it has
150 been granted.

151 (B) When an order is granted in accordance with Part A,
152 it shall be the responsibility of the signer of the application
153 as well as anyone connected with implementing the order, to
154 see that it is implemented in a way entirely consistent with
155 the provisions of the order, and that utmost respect is given
156 to the constitutional rights and the privacy of those persons
157 whose conversations are overheard or intercepted by virtue
158 of the order.

159 (1) When any criminal prosecution is brought which in-
160 volves a defendant who has been the subject of a court order
161 under Part A, the state must furnish the defendant with a
162 copy of the order and an accurate transcript of the material
163 proposed to be used as evidence, at least thirty days before
164 the commencement of the trial. If the defendant has any ob-
165 jctions to the order having been granted, or the manner in
166 which it was implemented, he must make them known to the
167 court at least ten days before the commencement of the trial.

168 (2) No material obtained in a manner inconsistent with
169 the provisions of any court order granted under Part A shall
170 be admissible as evidence in any judicial proceeding in the
171 commonwealth.

172 (3) It shall be unlawful for any person to edit, alter, or
173 tamper with any tape, transcript, or other recording of any
174 kind of any conversation overheard or intercepted by a court
175 order granted under Part A, and then to present such material
176 in any judicial proceeding, or any proceeding under oath,
177 without fully indicating the nature of all changes made and
178 the original state of the material. Any person violating this
179 paragraph shall be punished by imprisonment for not more
180 than one year, or by a fine of not more than five hundred dol-
181 lars, or both.

182 (4) Any law enforcement official who obtains or misuses
183 in a grossly negligent or malicious manner, the powers given
184 him by a court order under this section, shall be liable in an
185 action for damages by any person aggrieved by, or as a result
186 of such action. The minimum award for such injury shall be
187 two hundred and fifty dollars.

188 (c) In order to protect innocent parties it is essential to
189 preserve the secrecy of any tapes, transcripts or other record-
190 ings of any kind intercepted or overheard under a Part A
191 order, and to insulate the entire proceedings from unauthor-
192 ized view.

193 (1) No application or order under Part A shall be made
194 public by the court, or the applicants, or by any person with
195 knowledge of its existence or contents, until a true indict-
196 ment is returned against the individual or individuals named
197 as the subjects in the application or order.

198 (2) The court shall seal and keep in the custody of the
199 court as the official record, a true copy of each application
200 and order. The order itself shall be delivered to and retained
201 by the applicant as authority for its implementation.

202 (3) Any tapes, transcripts or other recordings of any kind
203 of conversations intercepted or overheard under a Part A
204 order shall be deemed to be in the custody of the court, but
205 may be kept in the possession of the applicant at the discre-
206 tion of the court.

207 (4) All tapes, transcripts or other recordings of any kind
208 of conversations intercepted or overheard under a Part A
209 order must be returned to the possession of the court either
210 at the conclusion of the trial of a defendant who was the sub-
211 ject of such order, or at the end of one year from the date of
212 the expiration of the order, whichever is later.

213 (5) All tapes, transcripts or other recordings of any kind
214 of conversations intercepted or overheard under a Part A
215 order shall be destroyed by the court five years after the date
216 on which they are returned to the possession of the court
217 under paragraph 4.

218 (6) Any person who has been damaged by a violation of
219 Part C, may sue the violator or violators therefor and shall
220 recover the damages by him sustained, and the cost of the
221 suit, including a reasonable attorney's fee, and no award
222 shall be less than five hundred dollars.

223 (D) A commission on electronic surveillance shall be
224 created. Its members shall consist of the chief judge of the
225 supreme judicial court, or his appointed representative, who
226 shall be the chairman; the governor, or his appointed repre-
227 sentative; the attorney general, or his appointed representa-
228 tive; a representative appointed by the Massachusetts bar

229 association; and a member of the faculty of a Massachusetts
230 law school, to be appointed by the chairman. The commission
231 shall meet at least once every year following the passage of
232 this section and by the end of the fifth year after passage, it
233 shall file a written report to the general court giving its evalu-
234 ation of how well the provisions of sections 99, 99A and 99B
235 have been carried out in practice, and recommending any
236 changes it believes will improve the functioning of these sec-
237 tions. The commission shall have limited subpoena power,
238 including the power to inspect all applications and orders
239 under Part A. One year from the date of submission of
240 such report, the commission shall terminate as an official body,
241 unless renewed at that time by act of the general court.

242 *Section 99C.* Whoever secretly overhears, or attempts to
243 overhear or to have any other person overhear the delibera-
244 tions of a jury by use of a device commonly known as a dicto-
245 graph or dictaphone, or however otherwise described, or by
246 any similar device or arrangement with intent to procure any
247 information relative to the conduct of such jury or any of
248 its members, shall be punished by imprisonment for not more
249 than five years or by a fine of not more than five thousand
250 dollars, or both.

1 SECTION 2. This act shall take effect ninety days after
2 passage.

The Commonwealth of Massachusetts

INTERIM REPORT

OF THE SPECIAL COMMISSION ON

ELECTRONIC EAVESDROPPING

APRIL, 1967

The Commonwealth of Massachusetts

SEN. MARIO UMANA

Chairman

SEN. WILLIAM X. WALL

Vice Chairman

REP. PHILIP K. KIMBALL

REP. ANDRE R. SIGOURNEY

WILLIAM P. HOMANS, JR.

ELLIOT B. COLE

NORMAN S. WEINBERG

Senator Wall has signed the above report in order that a majority of signatures appear hereon—so that said report may properly be filed for consideration by the General Court. Senator Wall reserves his right on future action concerning the report. Representative Weinberg of Boston also reserves his right

The Special Commission on Electronic Eavesdropping was created to study and investigate "the manner by which communications by wire, radio and word-of-mouth may be overheard or otherwise intercepted without the knowledge, consent, or authorization of either or all parties to a communication."

During the past year, the Commission held three public hearings and a number of executive sessions. The commission has heard testimony on the capabilities of present eavesdropping devices and the prospects of research and development. Also, the commission has conducted an extensive study of service observation and monitoring of the New England Telephone and Telegraph Company.

Part I. Eavesdropping Devices

The Commission heard testimony from Emanuel Mittleman of New York City and Bernard B. Spindel of Holmes, New York.

Mr. Mittleman, president of the Wireless Guitar Company, manufactures devices of a commercial nature primarily for private investigators and private parties. He sells his goods on a cash-and-carry, no-names-no-questions-asked basis. Mittleman told the commission that in the spirit of American capitalism (as he sees it), his only concern "is making a buck." The devices which he demonstrated consisted of a "parasite bug" and a "room bug."

The "parasite bug" is a subminiature transmitter, less than half the size of a pack of cigarettes, which broadcasts *both* sides of a telephone conversation, and derives its power from the telephone itself. Ordinarily these transmitters can last for years, and properly constructed and installed are detectable only by physical inspection of the telephone.

The "room bug" is also a subminiature transmitter but requires a battery as a power-source which lasts up to two weeks. Either device can transmit a very clear signal at least 7 blocks in downtown Boston and can pick up a whisper at 20 feet. The advantage of using a transmitter is that even if detected, which is highly unlikely, one can never learn the identity of the eavesdropper.

Conversations may be monitored by using micro-miniature micro-phones, some of which can pick up a whisper at 50 feet. Hearing-aid microphones may be as small as 3/8" on a side. Under

development are microphones the diameter of a pin-head and less than 1/8" long. If a telephone line is used, amplifiers less than a third of the size of a dime, and just as thin, can amplify the signal as far as 20 miles by using telephone wire. The telephone wires used are called vacant pairs, telephone lines not being used by subscriber. (For technical reasons, it is necessary for the Telephone Company to have "vacant pairs".) Another alternative is to utilize power lines, by using the principal of the wireless intercom, technically called a carrier-transmitter, or transmitting RF signals, i.e., radio waves, down the power line. Also in use is the device hidden in an eagle found in our Moscow Embassy in 1958, activated by ultrasonic waves. In the future, one can expect lasers to be utilized.

Clearly the future is frightening, and beyond the layman's comprehension. Science has a double-edge sword, which can work for the betterment of mankind or for its destruction, depending on how the scientific tools developed are used. Clearly in our age the basic components of eavesdropping devices have many legitimate uses in electronics, communications, aerospace, and medical applications. Even the strictest enforcement of the most all-encompassing statute will not put a stop to electronic eavesdropping. We can only hope to lessen the incidence of eavesdropping by co-operative federalism. (See below.)

Part II. Service observation procedures of the New England Telephone and Telegraph Company

On Sunday, June 12, 1966 the Boston *Herald* in a copyrighted story by Ronald Kessler disclosed to the public the existence of the Bell system's service observation practices. This is believed to be the first public disclosure of the telephone company's practices since its inception. Service observation, according to the representatives of the telephone company, is part of the company's quality control system; specifically, service observation checks the performance of the company's equipment and employees. In so doing, the company intercepts customer-to-customer calls and customer-to-company calls.

Service observation was first instituted in February, 1903. At that time, the operation of the company's equipment could only

be evaluated by listening to phone calls. The company, by its own admission continued to listen in to customer-to-customer calls for periods up to ten minutes up to June 1, 1966. Company employees listened in to conversations in order to hear subscriber comments about company service. Current service observation procedures are contained in the two-volume *Traffic Service Observing Practices*

Manual. A summary of the practices is contained below.

During the course of the investigation, members of the commission met frequently with three company executives: William Hogan, vice-president; Jay H. Whatley, assistant vice-president-operations; George R. Clark, Traffic Supervisor, all of whom gave their full cooperation. However, other officials refused entry to the Commission's Chairman when he accompanied the Boston press corps for a tour of the Company's service observation facilities. Fortunately other officials prevailed and the Chairman accompanied the press.

The three above-mentioned executives spent many hours describing to Commission members the company's service observation practices, which are uniform throughout the Bell System.

The following summary of these practices and objectives is taken from a report prepared by the Telephone Staff Committee of the New England conference of public utility commissioners:

TRAFFIC DEPARTMENT SERVICE OBSERVING

Private

Service Observing on the handling of traffic by the Traffic Department is done as described in the material which follows:

Service Observing is done by trained Service Observers who follow standard System methods and procedures as specified in the Traffic Service Observing Practice.

The observing procedures are contained in eleven measurement plans which have been issued by the Traffic Measurement Group at "195". A brief description of each of these plans is as follows:

Dial Line

This practice measures the effectiveness of the dial system on

local calls and the customer's use of the dial equipment by observing on the customer's lines while he dials the number and the connection is established. The dialed number is recorded on a tape. The observer notes customer dialing errors and equipment malfunctions staying on each connection only long enough to establish that the desired station has been reached. The customer's lines to be observed are picked at random "except for some concentration on heavy DDD users" and the list is completely changed each week. In general, about 30 or 40 lines in a given dial entity are being observed at any one time, although the observer can observe only one call at a time from the group. Presently, about 2,500 dial entities are being observed with the usual number of observations, 300 per month.

DDD Outgoing Trunk

Measurements are made on the effectiveness of customer dialed DDD calls by observing on the trunks outgoing to the tandem toll switching machine from the local office. Items measured are ineffective attempts due to overflows, reorder, and equipment failures. When a trunk is seized, the called number is displayed before the observer who stays on the connection only long enough to determine whether or not the desired station is reached. The calling station is not identified. If a CAMA operator is brought into the connection for calling number identification, the observer checks her handling of the call and the accuracy of keying. Observed trunks are a representative sample of all tandem trunks and are not changed unless a need is apparent. About 500 AMA and CAMA installations are now being observed in accordance with this practice.

DDD Incoming Trunk

Incoming Trunk Observations measure the ability of the dial equipment within a certain area to complete toll calls coming into that area from other areas. The only items measured relate to the disposition of the call: completed, busy, don't answer, reached intercept correctly, or ineffective. Ineffective attempts are separated by cause — reorder, no circuit, or equipment failure.

The observer is connected to trunks incoming to the toll switch-

ing machine from another area. She receives a display of the called number and remains on the connection only long enough to determine the disposition. She has no record of the calling number.

The number of Incoming Trunk Observing locations in the System is about 100. The monthly quota for each installation is 5,000 — 7,000 observations.

Manually Handled Outward Toll and Assistance

Measurements on cord switchboards handling toll and assist traffic are designed to measure operator and equipment performance. Speed of answer is measured mechanically. Both operator accuracy speed and manner are measured by the observer. Most of this observing is done by connecting the observer to a cord pair on the operator's position. This procedure insures a completely random selection of calls to be observed.

The observer stays on the cord pair through the setting up of the connection, recording the order, timing the operator's actions and noting any operator failures, until conversation starts. The observer then cuts out of the connection until conversation is completed as indicated by signals on her position. The observer requisitions the operator's ticket and checks it for accuracy of recording, timing, and the collection of changes on coin calls.

In a minority of locations, the observer is not connected to a cord pair but instead has a duplicate of the operator's switchboard multiple before her. In these cases she selects a recording trunk on which a call is waiting and follows the subsequent action in a manner similar to cord observing.

There are just over 1,000 Outward Toll Chief Operator Units now being observed in the Bell System. The quota is 900 observations obtained in one, two, or three months.

Outward Toll — Traffic Service Position

Traffic Service Position observing is a relatively new measurement. The practice was issued in July, 1965 and at present ten or twelve units are being observed. The observer in this instance is measuring the effectiveness of the TSP operator and the dial switching network.

The observer is connected to a trunk which has been selected by a customer call. She receives a display of the calling number plus the code or number dialed by the customer and any keying by an operator in connection with the call. Similarly as for observing on manually handled toll, the observer observes the initial operator contact and any subsequent contact, cutting out of the connection when conversation takes place. The observer measures the operator's accuracy, speed and manner and the effectiveness of the dial network in completing and timing the customer's call.

Speed of operator answer is obtained mechanically.

Information

Observing on Information service is strictly a measurement of the operator's effectiveness in providing accurate, complete, and pleasing service. The observer is connected to an information trunk which has been selected by an incoming call from a local or distant customer or operator. The observer records the request and checks the details given by the operator for accuracy. The observer has no knowledge of the calling number and there is no conversation other than that between the customer and the operator.

Intercept

Observing on Intercept service is very similar to Information observing. The observer is connected to a trunk incoming to the intercept board and listens to the exchange between the operator and the customer. She measures the operator's accuracy, speed, and manner.

PBX

The PBX measurement plan does not involve separate observing. Instead the observations used in this plan are Dial Line and Outward Toll observations which originate or terminate at PBX's.

CCSA

Common Control Switching Arrangement is the name of the service which provides switching systems furnished customers such as FTS and G.E. to inter-connect their PBX's. Observing is done

on these systems either with dial line observing circuits or by the use of portable observing sets. In either case, the observing circuits are connected to the access lines between the PBX's and the toll switching machines. The observer receives a record of the dialed number to determine whether or not the attempt is effective. If the attempt is ineffective, she records the reason for the failure. She does not stay on the connection after the desired called number is reached.

Dial TWX

A modified dial line circuit is used for dial TWX observing. The observing circuit is attached to dial TWX lines which are selected at random and are completely changed each week. When the TWX customer dials a number, it is recorded on tape for the observer. The observer had a "receive only" TWX machine associated with her position which will duplicate the initial exchange between the calling and called stations. The observer stays on the connection only until the desired station answers. The observer measures the instances of customer dialing irregularities and equipment failures, as in dial line observing.

TWX Outward and Assistance

Observations are made on operator performance at 15 TWX assistance centers in the System. These observations are made from monitoring positions in the central office. The observer is on the connection only during the period the operator is on the connection. The observer receives the same print-out as the operator and records the calls in various classifications. She also makes note of any keypulsing or operating irregularities by the operator or any incorrect reports given to customers. Speed of answer is obtained by mechanical means.

The company also provides service observing equipment for its subscribers pursuant to New England Telephone and Telegraph Tariff DPU Number 10, Part III, Section 15, page 13. "This equipment is provided solely for the purpose of determining the need for training, improving the quality of service rendered by customers' employees in their operation of private branch exchange attendant positions, or in the handling of telephone calls of an

impersonal nature concerning the customers' business." (The word, customers, here refers to the company's subscribers.)

The complexity of today's telephone equipment, taken as an integrated unit defies human comprehension. The commission believes that the company is sincere in its statement that service observation is essential to the proper functioning of the telephone system.

This commission lacks the technical competence to judge the value of service observation with respect to the maintenance and repair of the company's equipment. We therefore accept the conclusions of the Telephone Staff Committee's report, *infra*. The Telephone Staff Committee is composed of one representative from each public utility commission in New England who is familiar with the telephone system's requirements.

The Report on page 6 states "It is our conclusion that, as in industry generally, random sampling of a company's product — *in this case installation and maintenance of communications equipment and the transmission of voice and data* — is vital in maintaining control of quality and performance.

"The magnitude of the data collected and the analysis and summarization thereof seems to indicate beyond reasonable doubt that a high standard of service is the purpose for which this program is maintained. Company regulations pertaining to secrecy of communications as set forth in its booklet entitled 'Protection of Telephone Plant and Service,' seem to further support this contention."

The Telephone Staff Committee's recommendations are the following:

RECOMMENDATIONS

- 1) The company should institute and pursue a program designed to fully acquaint its customers by means of bill inserts and other media with the type of observations being made in its quality control program.
- 2) In order to remove any aura of secrecy and to bring the service observing and monitoring practices directly under regulatory scrutiny we recommend that reference be made

to this matter in the General Regulations of the filed tariffs along the following lines:

- a) *Privacy of Conversation.* It is the policy and practice of the Company not to listen in on any calls between its customers.
 - b) *Service Observing and Monitoring of Calls.* It is the policy and practice of the Company to observe service to its customers by monitoring a random sample of the handling of the calls by its operators and equipment, and to monitor a random sample of conversations involving Information Service, Intercept Service, Repair Service and Business Office contacts. Monitoring and service observing will be done in accordance with stated company practices, available for inspection by appropriate regulatory authorities.
- 3) In order to maintain the privacy of calls between customers and to further insure that there will be no invasion of privacy at any time, we recommend that the service observer's cut-off key be automated by relay or other appropriate means so that the observer will be cut out of the call at the time the calling party reaches the called number.

The Commonwealth's Department of Public Utilities called for an investigation (DPU #15298) of observation practices one week after this commission held its public hearing. The following are the orders of the DPU:

D. ORDERS

After due notice, public hearing and consideration, it is hereby *ORDERED*: That the telephone company pursue a program on a continuing basis that will keep its customers informed by means of bill inserts and other media with its present types and any changes in types of service observing and monitoring made in its quality-control programs, and it is further

ORDERED: That to bring the service observing and monitoring practices directly under regulatory scrutiny, reference be made to these practices in the General Regulations of the Company's filed tariffs along the following lines:

- A. *Privacy of Conversation.* The Company shall not listen in on the conversation of any customer-to-customer calls.
- B. *Service Observing and Monitoring of Calls.*
- (1) The Company may observe service to its customers by monitoring a random sample of the handling of calls by its operators and equipment, but only until the calling customer reaches the called customer.
 - (2) The Company may monitor a random sample of conversations involving Information Service, Intercept Service, Repair Service, and Business Office contacts.
 - (3) Monitoring and service observing will be done in accordance with stated company practices, a current copy of which shall be on file in the Rates and Research Division of the Department, and it is further

ORDERED: That within fourteen days of this order a current copy of the service observing and monitoring practices of the Company be filed with the Rates and Research Division of the Department, and it is further

ORDERED: That there shall be no changes made in service observing and monitoring practices of the Company unless they are made in accordance with statutory provisions and the rules and regulations of the Department governing changes in filed tariffs, and it is further

ORDERED: That the Company make the studies referred to herein and file with the Secretary of the Department within six months of the date of this order a written report summarizing their studies and stating the conclusions of the Company concerning the proposed changes in Company practices as suggested in our findings herein, and it is further

ORDERED: That the following requests for rulings of law by the respondent are denied: Nos. 1, 2, 3, 4, 5, 6, 11, 12, 13. We do not grant requests for rulings of law on the aforementioned Nos. 1, 2, 3, 4 and 5, because they are beyond the scope of our investigation. We do not grant requests for rulings of law Nos. 11, 12 and 13 for the reason that they are inapplicable to this order, and it is further

ORDERED: That the investigation herein be and is hereby continued until further order of the Department.

By order of the Department,

ROY C. PAPALIA, *Chairman*

LUCY M. CARRA, *Commissioner*

DAVID M. BRACKMAN, *Commissioner*

NORMAN MASON, *Commissioner*

JOSEPH F. CLEARY, *Commissioner*

HELEN P. ROSS, *Commissioner*

(Commissioner Andrew Benson dissented.)

CONCLUSIONS

The commission believes that the service observation practices of the telephone company as we understand them are necessary to the rendition of service and that the telephone company is cognizant of its duty to preserve the customer's privacy. The telephone company therefore since June 1, 1966, has ordered its service observers to discontinue their observations as soon as a connection has been made and a conversation between two customers is established. However, as telephone company officials conceded during hearings conducted by the Massachusetts Department of Public Utilities, there is no way for the telephone company to insure that its service observers will discontinue their observations when a conversation ensues.

Therefore, in the interests of the public, we believe an automatic, voice-actuated cut-off device should be installed in all telephone company service observing equipment throughout the Commonwealth to insure that no part of any conversation will be heard by a service observer. The device referred to would automatically disconnect a call from the service observer's equipment as soon

as the first word is spoken after a connection has been made, and this would be accomplished with a voice-actuated cut-off switch.

The DPU has ordered the telephone company to report by June, 1967, what measures can be taken to prevent invasion of privacy in service observance practices. We assume the report will describe the automatic cut-off proposal mentioned above, a recommendation also made by the Telephone Study Committee.

The commission believes that the requirement of a voice-actuated automatic cut-off device should properly be required by the DPU under its regulatory powers. If the DPU fails to exercise its powers, this commission shall report to the General Court with appropriate recommendations.

There are many questions that are raised in relation to the Department of Public Utilities which we think should be aired. We cannot understand why the DPU commission has never studied service observation practices in the past 50 years. We cannot understand why apparently no one in the DPU thought it outrageous that the company would monitor customer-to-customer calls *to gain customer comments on service*. Nor can we understand why the DPU commission took 5 weeks to call for an investigation when this commission and the U.S. Senate's subcommittee on Administrative Practices and Procedures (the Long Committee) were able to determine in but a few days that an investigation was in the public interest. New England Telephone and Telegraph Company is exempted by c. 272. sec. 102 (G.L. Ter. ed.) from the eavesdropping statutes of the Commonwealth. This section was enacted in recognition of the specialized problems of the telephone industry. The same does not hold true for the company's subscribers.

Part III. The Massachusetts Statutes

In *Commonwealth v. Spindel*, recently decided by the Supreme Judicial Court, the court said "the eavesdropping statute is not a paragon of clarity." Chapter 272, Sections 99, 99A, 100, 101 and 102 (G.L. Ter., ed.) deal with eavesdropping. These sections, when taken singly are difficult to construe. Taken together one is hard pressed to find another with the same interpretation.

We therefore think it necessary to enact new legislation this session even though this commission cannot yet advise the general court on the policy issues involved. A number of bills relative to eavesdropping have been filed this session. H. 1435 was filed by then Attorney General Edward Brooke, and is supported by Attorney General Elliot Richardson. As a stop-gap measure this commission recommends enactment of H. 1435. We realize that certain sections of the bill are poorly drafted; we also realize that in all probability a later report by this commission will seek changes in the bill, if it is enacted, in both form and substance. Notwithstanding these considerations, we feel the existing statutes necessitate enactment.

Part IV. Legislative Recommendations

The Public Utilities Commission is authorized to grant tariffs to exempt common carriers of electrical intelligence from the prohibitions of C

Section 1: Chapter 272, section 102, as most recently amended by chapter 48, section 2 of the acts of 1956, is hereby repealed.

Section 2: The following section is inserted following chapter 166, section :

Section : The public utilities commission is authorized to grant tariffs to exempt common carriers of electrical intelligence from the prohibitions of chapter 272, sections 99, 100, and 101 for the purpose of maintenance, repair and development of transmission equipment. Said tariff may be promulgated by the public utilities commission upon a finding that it is necessary for the maintenance, repair, and development of the carrier's transmission equipment. The commission shall take care that a carrier does not intercept substantive portions of communications.

The Commonwealth of Massachusetts

INTERIM REPORT
OF THE
SPECIAL COMMISSION
ON ELECTRONIC EAVESDROPPING

(Established under Chapter 82 of the Resolves of 1964 and
time most recently extended under Chapter 107 of the
Resolves of 1966)

October 26, 1967.

The Commonwealth of Massachusetts

INTERIM REPORT OF THE SPECIAL COMMISSION ON ELECTRONIC EAVESDROPPING

As a result of our investigation into "the manner by which communications by wire, radio, and word of mouth may be overheard or otherwise intercepted without the knowledge, consent or authorization of either or all parties to a communication," the Commission has great concern over the inability of private citizens to receive proper compensation and damages of any kind as a result of the invasion of their personal privacy.

As reported previously, the availability of instruments for overhearing secretly private conversations is immense. The devices are available at low cost and do not have to be specially manufactured and can be used by ordinary people without special training or there are devices available of a very sophisticated nature requiring more skillful operation.

The result is a problem of immense dimensions in terms of control with which the Commission is continuing to deal and concerning which it hopes to offer concrete recommendations in the very near future.

However, at the present time the problem raised by the motion picture produced at the Bridgewater State hospital brings to immediate attention the need for protective legislation in the area of invasion of privacy.

Your Commission staff has prepared a study concerning the present state of the law of invasion of privacy in Massachusetts and in other states. A copy of this study is attached hereto as an appendix.

In summary, the study indicates that compensation for invasion of privacy has been handled by the states by statute or some courts of higher jurisdiction have recognized invasion of privacy as a tort within the meaning of the common law. The Supreme Judicial Court of the Commonwealth of Massachusetts in its latest decision on the subject namely *Frick V. Boyd* 214 N.E. 2d 460, (1966,) has failed to state until this time whether or not a cause of action for

invasion of privacy exists at common law. It is the opinion of this Commission that there should be the right to compensation for invasion of privacy.

Although we recognize that a civil action to allow persons to be compensated for an invasion of their privacy is not a completely effective control of the use of devices to overhear conversations we do feel it is a minimum remedy which should be available to all citizens of Massachusetts due to the tremendous expansion of the problem created by the new technology. In addition, our studies of the laws of Massachusetts make it clear that there are other areas such as those which were raised by the current investigation over the production of the new "Titicut Follies" which cry out for statutory treatment for protection. It is our hope that the development of the law of invasion of privacy will be some aid in compensating persons in the situation of the inmates of Bridgewater State Hospital to some degree for the intrusions made to their privacy. We also see the need for detailed study to produce legislation to more clearly define the areas of confidentiality & invasion of privacy.

Our survey of the present state of the law of invasion of privacy is not meant to imply that it is our intention to limit by our bill, an action of invasion of privacy to the current state of the law. It is our desire that the Supreme Judicial Court shall develop the action of invasion of privacy in the tradition of the Common Law to meet the needs and dangers of the technological society in which we live. Yet, we feel this should be done on a case by case basis rather than to attempt to spell out all the possible situations in legislation.

MEMBERS OF COMMISSION

Senators

MARIO UMANA

WILLIAM X. WALL

WILLIAM I. RANDALL

Representatives

GEORGE L. SACCO, JR.

ANDRE R. SIGOURNEY

NORMAN S. WEINBERG

DANIEL W. CARNEY

PHILIP K. KIMBALL

Governor

HON. WILLIAM P. HOMANS, JR.

ELLIOT B. COLE

[APPENDIX A]

Subject: Invasion of Privacy: The Nature of the Tort and Its Development as a Cause of Action.

I

Nature of the Tort

The law of privacy as it exists today comprises four distinct types of invasion of four different interests of the plaintiff. All four are designated by the term "invasion of privacy," but in fact they have nothing in common other than that each represents an interference with the right of the plaintiff to be let alone.

One of these torts consists of a trespassory intrusion into a private area as by an illegal search and seizure¹, an illegal search of a shopping bag in a store², an invasion of his home³, and illegal eavesdropping.⁴

The key to this tort is that there must be something in the nature of prying or intrusion. It is clear also that the intrusion or prying must be something which would be offensive or objectionable to a reasonable man.⁵ Also for a cause of action to lie it must be established that the intrusion or prying was into a private area.⁶

A second group of cases allow recovery in tort where there has been publicity of a highly objectionable kind to private information, even though it is true and so no action for defamation would lie. A writing is not required for publicity.⁷ Once again the mat-

¹ *Griswald v. Connecticut*, 381 U.S. 479 (1964)

² *Sutherland v. Kroger Co.*, 144 W. Va. 673, 110 S.E. 2d 716 (1959).

³ *Walker v. Whittle*, 83 Ga. App. 445, 64 S.E. 2d 87 (1951); *Ford Motor Co. v. Williams*, 108 Ga. App. 21, 132 S.E. 2d (1963).

⁴ *La Crone v. Ohio Bell Tel. Co.*, 114 Ohio App. 299, 182 N.E. 2d 15 (1961); *Roach v. Harper*, 143 W. Va. 869, 105 S.E. 2d 564 (1958).

⁵ *Horstman v. Newman*, Ky., 291 S.W. 2d 567 (1956); *Harms v. Miami News, Inc.*, Fla., 127 So. 2d 715 (1961).

⁶ *Gotthelf v. Hillcrest Lumber Co.*, 280 App. Div. 668, 116 N.Y.S. 2d 873 (1952); *Voelker v. Tyndall*, 226 Ind. 43, 75 N.E. 2d 548 (1947).

⁷ *Linehan v. Linehan*, 134 Cal. App. 2d 250 P. 2d 326 (1955).

ter made public must be offensive or objectionable to a man of ordinary sensibilities.⁸

The third form of invasion or privacy consists of publicity which places the plaintiff in a false light in the public eye. Examples are wrongfully attributing to the plaintiff authorship of books or articles.⁹ Other instances are false testimonials in advertising, and a picture of an honest man in a newspaper expose of gangsters. Again the published matter must be offensive or objectionable to a reasonable man of ordinary sensibilities.¹⁰

The final defined area where a cause of action will lie for invasion of privacy consists of the appropriation for the benefit of the defendant of the name or picture of the plaintiff. This most frequently occurs where the plaintiff is falsely portrayed in an advertisement as approving of a product.¹¹ Other examples include posing as plaintiff's wife and using plaintiff's identity to obtain credit. The key to recovery under this tort theory is that the defendant must gain some benefit from the appropriation and this usually consists of some economic return.

II

Its Development as a Cause of Action

In many jurisdictions¹² a cause of action lies for invasion of privacy based on common law decisions. Four states¹³ have statutes

⁸ *Samuel v. Curtis Pub. Co.*, 122 F. Supp. 327 (N.D. Cal., 1954);

Meetze v. Associated Press, 230 S.C. 330, 95 S.E. 2d (606 (1956)).

⁹ *D'Altomante v. New York Herald Co.*, 154 App. Div. 453, 139 N.Y. S. 200 (1913); *Kerby v. Hal Roach Studios*, 53 Cal. App. 2d 207, 127 P. 2d (557) (1942).

¹⁰ *Carlisle v. Fawcett Publications, Inc.*, 201 Cal. App. 2d 733, 20 Cal. Repr. 405 (1962).

¹¹ *Lane v. F. W. Woolworth Co.*, 174 Misc. 66, 11 N. Y. S. 2d 199 (1939); *Selsman v. Universal Books, Inc.*, 18 App. Div. 2d 151, 238 N.Y. S. 2d 686 (1963).

¹² Alabama, Alaska, Arizona, Arkansas, California, Connecticut, Delaware, the District of Columbia, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Michigan, Mississippi, Missouri, Montana, Nevada, New Hampshire, New Jersey, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee and West Virginia.

¹³ New York, N. Y. Civil Rights Law SS 50-51; Oklahoma, Okla. Stat. Ann., Title 21, SS 839-40; Utah Code Ann. 1953, S 76-4-8 and S 76-4-9; Virginia, Va. Code Ann. 1957, S 8-650.

expressly dealing with invasion of privacy. These laws are all quite similar; each providing for a civil cause of action where there has been wrongful use of a plaintiff's name or picture.

Massachusetts has been slow in developing any common-law tort for invasion of privacy. The first case in the area, *Thayer v. Worcester Post Co.*, 284 Mass. 160, 187 N.E. 292 (1933) mentions the fact that the right to be free from such invasion existed under the common law in various other jurisdictions but felt it unnecessary to decide the question as to Massachusetts, since the plaintiff there had given consent to any invasion. In the next case dealing with the law of privacy, *Marek v. Zanal Products*, 298 Mass. 1, 9 N.E. 2d 393 (1937) consent was again presumed so that the court again declined to decide the issue. In *Themo v. New England Newspaper Pub. Co.*, 306 Mass. 54, 27 N.E. 2d 753 (1940) the court still again refused to come to grips with the problem by holding there that certain material published in a newspaper was not private matter and so that even if a right to privacy existed, there could be no recovery under the facts presented. A Federal case, *Wright v. R.K.O. Radio Pictures*, 55 F. Supp. (D. Mass., 1944) seizing on dicta in *Themo, supra*, construed the state of the law in Massachusetts to be that an actionable invasion of privacy existed but only such an invasion that would amount to libel. The Massachusetts court rejected this interpretation of its decisions in *Kelly v. Post Publishing Co.*, 327 Mass. 275, 98 N.E. 2d 286 (1951) holding that *Themo, supra* left open the question whether there exists a legally protected right of privacy in Massachusetts. *Kelly* held that even if a right to privacy exists, to publish the gory picture of a dead child is not an invasion of the privacy of the parents. The latest Massachusetts decision on the subject is *Frick v. Boyd*, — Mass. — , 214 N.E. 2d 460 (1966) also declines to answer the issue.

Massachusetts, then, has failed to take a position on the matter, since the courts have felt that no fact pattern before it has shown any invasion of privacy.

[APPENDIX B]

The Commonwealth of Massachusetts

In the Year One Thousand Nine Hundred and Sixty-Seven.

AN ACT CREATING A CIVIL ACTION FOR INVASION OF PRIVACY

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

CHAPTER 231 OF THE GENERAL LAWS OF THE COMMONWEALTH
SHALL BE AMENDED BY INSERTING THEREIN THE
FOLLOWING AS SECTION 90A:

There is a cause of action for invasion of privacy. Compensatory damages, punitive damages, reasonable attorney's fees and other litigation costs reasonably incurred may be awarded. Notwithstanding any provisional law relating to limitations of action, an action for invasion of privacy may commence within two (2) years after the plaintiff learns of the facts upon which the action is grounded.

By Mr. Backman of Brookline, petition of Jack H. Backman for legislation relative to eavesdropping and for the creation of a commission on electronic surveillance and wiretapping. The Judiciary.

The Commonwealth of Massachusetts

In the Year One Thousand Nine Hundred and Sixty-Eight.

AN ACT RELATING TO EAVESDROPPING AND CREATING A COMMISSION ON ELECTRONIC SURVEILLANCE AND WIRETAPPING.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

1 SECTION 1. Section ninety-nine of chapter two hundred and
2 seventy-two of the General Laws is hereby repealed.

1 SECTION 2. The General Laws are hereby amended by in-
2 serting after chapter 272 the following chapter:—

3 CHAPTER 272A.

4 EAVESDROPPING AND ELECTRONIC SURVEILLANCE.

5 *Section 1.* Whoever, except in accordance with an order is-
6 sued as provided herein, secretly or without the consent of
7 either a sender or receiver, overhears, or attempts secretly, or
8 without the consent of either a sender or receiver, to overhear,
9 or to aid, authorize, employ, procure, or permit, or to have
10 any other person secretly, or without the consent of either a
11 sender or receiver, to overhear any spoken words at any place
12 by using any electronic recording device, or a wireless tap
13 or electronic tap, or however otherwise described, or any simi-
14 lar device or arrangement, or by tapping any wire to intercept
15 telephone communications, shall be guilty of the crime of
16 eavesdropping and shall be punished by imprisonment for not
17 more than two years or by a fine of not more than one thousand
18 dollars, or both.

19 *Section 2. (a)* Such order may be issued and shall be signed

20 by any justice of the supreme judicial or superior court upon
21 application made by either a district attorney or the attorney
22 general of the commonwealth to any justice of the supreme
23 judicial court or of the superior court for an ex parte order
24 allowing such officer to order an electronic eavesdrop or a
25 wiretap of a given communication when there are reasonable
26 grounds to believe that

27 (1) the electronic eavesdrop or wiretap requested is neces-
28 sary to save human life; or

29 (2) in the case of a wiretap, the communication itself is an
30 element of the crime alleged; or

31 (3) the communication intercepted will contain evidence of
32 homicide, extortion, kidnapping, armed robbery, rape, or ar-
33 son; or

34 (4) the security of the commonwealth or the public safety
35 is endangered.

36 (b) An application under subsection (a) shall be accompa-
37 nied by an affidavit personally signed by a district attorney or
38 by the attorney general of the commonwealth. Where those
39 officials are unavailable and delay would endanger either hu-
40 man life or the public safety, the affidavit may be signed by
41 the highest ranking official available.

42 The affidavit shall contain the following:

43 (1) a full and complete statement of the facts and circum-
44 stances relied on by the applicant, including but not limited to
45 the crime or crimes involved, the information expected to be
46 obtained, the results of previous investigation which led to the
47 application, and the sources of the information leading to the
48 application, unless such sources are confidential;

49 (2) the precise location and the nature of the premises which
50 are to be eavesdropped upon, or of the wire to be tapped, and
51 the identity of the person or persons whose conversations are
52 to be overheard or intercepted. In the case of eavesdropping,
53 the affidavit shall specify as precisely as possible the building
54 or the particular rooms in a building to be bugged. In the case
55 of a telephone, the affidavit shall specify the number of the
56 line, and the names of the individuals to whom the phone is
57 listed, as well as those who are known regularly to use the
58 phone;

59 (3) a statement of all previous applications in the same

60 matter which involved the same premises, facilities or indi-
61 viduals, and the action taken by the court on each application ;
62 and

63 (4) an allegation that all other methods of investigation
64 have proven to be or will be inadequate or impracticable and
65 that there is reasonable cause to believe that eavesdropping
66 or a wiretap will be successful.

67 (c) If the court is not satisfied that the application sub-
68 stantially complies with the requirements of subsections
69 (a) and (b) above, it may require the applicant to furnish
70 additional information in support of the application.

71 (d) If the court is satisfied that the application substan-
72 tially complies with subsections (a) and (b), it may enter
73 an ex parte order granting leave to the applicant to eaves-
74 drop or to wiretap in conformance with the terms of the or-
75 der.

76 (e) An order to eavesdrop shall specify as precisely as
77 possible the building and the particular room or rooms in
78 that building in which permission to eavesdrop is granted.
79 An order to wiretap shall specify the particular wire to be
80 intercepted. A telephone shall be specified by its number.

81 (f) An order entered under subsection (d) above shall
82 describe or identify the person or persons who are authorized
83 to implement it, or the person or persons under whose super-
84 vision it is to be implemented.

85 (g) Such order shall state with particularity the purpose
86 or purposes for which it has been granted and the grounds
87 for the grant of permission.

88 (h) Such order shall be limited to a period of not more
89 than sixty days, but may be renewed for additional periods of
90 thirty days each, provided that the requirements of subsec-
91 tions (a) and (b) above are satisfied. An application for a
92 second or subsequent renewal must be heard by a panel of
93 three judges of the superior court.

94 *Section 3.* (a) When an order is granted in accordance
95 with section two, it shall be the responsibility of the signer
96 of the application, and all persons connected with implement-
97 ing the order, to see that it is implemented in a way entirely
98 consistent with the provisions of the order, and that utmost
99 respect is given to the constitutional rights and the privacy

100 of those persons whose conversations are overheard or inter-
101 cepted by virtue of the order.

102 (b) When any criminal prosecution is brought which in-
103 volves a defendant who has been the subject of a court order
104 under section two, the state must furnish the defendant with
105 a copy of the order and an accurate transcript of the material
106 proposed to be used as evidence, at least thirty days before
107 the commencement of the trial. If the defendant has any ob-
108 jections to the grounds on which the order was granted, or the
109 manner in which the order was implemented, he must make
110 them known to the court at least ten days before the com-
111 mencement of the trial.

112 (c) Material obtained by means of an eavesdrop or wiretap
113 shall be admissible as evidence in judicial proceedings in the
114 commonwealth only if obtained in a manner consistent with
115 a valid order granted in accordance with the provisions of
116 section two.

117 (d) It shall be unlawful for any person to edit, alter, or
118 tamper with any tape, transcript, or other recording of any
119 kind of any conversation overheard or intercepted by a court
120 order granted under section two, and then to present such
121 material in any judicial proceeding, or any proceeding under
122 oath, without fully indicating the nature of all changes made
123 and the original state of the material. Any violation of this
124 subsection shall be punishable by imprisonment for not more
125 than one year, or by a fine of not more than five hundred dol-
126 lars or both.

127 *Section 4.* (a) No application or order under section two
128 shall be made public by the court, or the applicants, or by
129 any person with knowledge of its existence or contents, until
130 a true indictment is returned against the individual or indi-
131 viduals named as its subjects in the application or order.

132 (b) The court shall seal and keep in the custody of the
133 court as the official record, a true copy of each application
134 and order. The order itself shall be delivered to and retained
135 by the applicant as authority for its implementation.

136 (c) Any tapes, transcripts or other recordings of any kind
137 of conversations intercepted or overhead pursuant to an order
138 granted under section 2 above shall be deemed to be in the
139 custody of the court, but may be kept in the possession of the

140 applicant at the discretion of the court.

141 (d) All such tapes, transcripts or other recordings must be
142 returned to the possession of the court at the conclusion of the
143 trial of a defendant who was the subject of such order for
144 which action the recording is needed as evidence, or at the
145 end of one year from the date of the expiration of the order,
146 whichever is latest.

147 (e) All such tapes, transcripts or other recordings shall
148 be destroyed by the court five years after the date on which
149 they are returned to the possession of the court under para-
150 graph (d) above, unless, prior to the expiration of such period,
151 the supreme judicial court, for good cause shown, issue a
152 stop-order, which may delay the destruction of any such re-
153 cordings for a period not to exceed five years.

154 *Section 5.* A commission on electronic surveillance shall be
155 created. Its members shall consist of the chief judge of the
156 supreme judicial court, who shall be the chairman; the gov-
157 ernor, or his appointed representative; the attorney general;
158 a representative appointed by the Massachusetts Bar Asso-
159 ciation; and a member of the faculty of a Massachusetts law
160 school, to be appointed by the chairman. The commission shall
161 meet at least once every year following the passage of this
162 section and by the end of the fifth year after passage, it shall
163 file a written report to the general court giving its evaluation
164 of how well the provisions hereof have been carried out in
165 practice, and recommending any changes it believes will im-
166 prove the functioning of these parts. The commission shall
167 have subpoena power, including the power to inspect all ap-
168 plications and orders under section two.

169 *Section 6.* Any person damaged by a violation of this chap-
170 ter may, in an action of tort, recover his damages from the
171 person liable therefor, together with costs of suit and rea-
172 sonable attorney's fees. In no event shall the damages as-
173 sessed under this section be less than five hundred dollars.

174 *Section 7.* If any provision of this act or the application
175 thereof to any person or circumstances is held invalid, the
176 invalidity shall not affect other provisions or applications
177 of the act which can be given effect without the invalid pro-
178 visions or applications, and to this end the provisions of this
179 act are severable.

The Commonwealth of Massachusetts

REPORT
OF THE
SPECIAL COMMISSION ON
ELECTRONIC EAVESDROPPING

June, 1968

The Commonwealth of Massachusetts

THE COMMISSION'S MEMBERS

SEN. MARIO UMANA, *Chairman*

SEN. WILLIAM X. WALL, *Vice-Chairman*

SEN. WILLIAM I. RANDALL

REP. GEORGE SACCO

REP. DANIEL CARNEY

REP. NORMAN WEINBERG

REP. PHILIP KIMBALL

REP. ANDRE SIGOURNEY

WILLIAM P. HOMANS, JR.

ELLIOT B. COLE

SANFORD A. KOWAL, *Chief Counsel*

TABLE OF CONTENTS

	PAGE
The commission's Report	5
Mr. Cole and Mr. Homans, concurring	10
Appendix 'A'	14
Appendix 'B'	33
Appendix 'C'	34

DATE

10 11

11 12

12 13

13 14

14 15

INTERIM REPORT OF THE SPECIAL COMMISSION TO
INVESTIGATE ELECTRONIC EAVESDROPPING
AND WIRETAPPING.

INTRODUCTION

A special commission to investigate electronic eavesdropping was created by the Legislature in 1964. During this period the Commission has held numerous public hearings, executive sessions and has directed its counsel to pursue research and investigation into the laws involving privacy, wiretapping and eavesdropping by law enforcement agencies, and problem of wiretapping and eavesdropping as it is committed by members of the general public.

Public hearings have been held by the Commission to demonstrate the type of eavesdropping devices presently available to members of the general public, and those used at the present time for covert wiretapping and eavesdropping. Public hearings were held to determine the extent and need for service observing as carried on by the New England Telephone and Telegraph Company.

RECENT UNITED STATES SUPREME COURT DECISIONS

Two recent cases decided by the United States Supreme Court clearly indicate that Sections 99, 100, 101, and 102 of Chapter 272 of the General Laws are unconstitutional insofar as they describe the methods by which law enforcement officers may be permitted to commit judicially authorized eavesdropping and wiretapping. In the case of *Berger v. State of New York* a statute very similar to the sections described above was held unconstitutional on its face. The Court found the provisions for obtaining a warrant were too broad and that the statute permitted a "continuous search". The United States Supreme Court for the first time made it clear in that case, that a judicially authorized eavesdrop or wiretap must conform to the Fourth Amendment of the United States Constitution.

This requirement means that an application for such a wiretap or eavesdrop order, to be valid under the Fourth Amendment, must conform to the same test of "probable cause" as is required for a search warrant. In addition the Court makes it clear that it desires close judicial supervision over all aspects of the process of

eavesdropping and wiretapping as it is performed by law enforcement officers.

The impact of these decisions is that the Massachusetts statute must be revised if police and law enforcement officials are to be able to lawfully intercept or wiretap any wire or oral conversations by members of the public under any circumstances.

*DEVICES FOR WIRETAPPING AND EAVESDROPPING
BY MEMBERS OF THE PUBLIC.*

Our hearings and studies have made it clear that eavesdropping devices are readily available to members of the public from commercially available stores. A person with a minimal education in electronics can easily install these commercially available devices for purposes of illegally intercepting wire or oral communications. In addition to devices which are easily available on the commercial market, other devices of much greater sophistication are manufactured by persons specializing in covert wiretapping and eavesdropping.

Due to the ease with which these devices may be obtained and manufactured, and the great proliferation of these devices, it is the Commission's conclusion that there is no way to effectively prohibit their sale or manufacture.

As a result, the Commission has revised the present Massachusetts statute to strictly forbid electronic eavesdropping or wiretapping by members of the public. This has been made necessary due to the fact that only two convictions have been obtained in Massachusetts for wiretapping or eavesdropping to the Commission's knowledge.

SERVICE OBSERVING

As a result of an investigation conducted by this Commission, at a public hearing held pursuant to that investigation the first admission by any telephone and telegraph company was made, that for a long period of time, these companies have operated a service by which the telephone company has overheard the conversations of subscribers without their knowledge. Long distance calls were monitored by the telephone company up until 1956. Local calls were monitored up until 15 days prior to the investigation conducted by the Commission in 1966.

“Service observing” was justified by the telephone company in order for it to check the quality of transmission of conversations over its lines, to supervise its operators, to check on the response of its repair personnel to the calls made by subscribers. The testimony further indicated that at the present time there is no necessity to listen to any conversation by a subscriber. In addition, service observing of the operators was said not to be necessary beyond the point that the operator heard the connection made between the parties for the call. This is due to the fact that improved electronic devices enable the same checks to be made without the necessity for overhearing the conversation of the parties.

To this end the Commission recommends the amendment of the Act governing the regulation of telephone companies by the Department of Public Utilities to insure that the privacy of the subscribers’ telephone conversations will be protected. In the system of regulation described by the proposed statute, the Department of Public Utilities is specifically designated to enforce these requirements. The standard of service observing as set forth by the Telephone Company in its testimony before the Commission are incorporated into the provisions of the proposed bill. The scheme of regulation requires an annual report to the Department of Public Utilities of all service observing activities by the Telephone Company, reporting of all rules and regulations of the Telephone Company concerning observing, a report of the amount of money expended for such service, and requires a semi-annual investigation of such service by the Department of Public Utilities.

This Commission feels that past conduct by the Telephone Company indicates that the Telephone Company has clearly favored its business interest against right of the public to have privacy in their telephone conversations. In addition, we take a dim view of a method of supervision which allows an employer to act as “big brother” towards its employees. As a result the Commission feels that a scheme of regulation by a public body with detailed statutory standards is required.

LAW ENFORCEMENT
EAVESDROPPING AND WIRETAPPING

The Commission feels that eavesdropping and wiretapping by

law enforcement officials should be permitted in order to effectively combat the menace of organized crime but only if such wiretapping and eavesdropping is limited by the standards set forth by the United States Supreme Court. This means that law enforcement eavesdropping and wiretapping should be strictly supervised by the judicial branch of the government and applications for eavesdropping and wiretapping must conform to the provisions of the Fourth Amendment.

The statute proposed by the Commission has revised the Massachusetts law to require strict compliance with the probable cause provisions of the Fourth Amendment. Wiretapping and eavesdropping by police officials will be limited to specified conversations and "continuous searches" will be prohibited. Applications for warrants must be made to a Justice of the Superior Court. The time limit of searches and warrants are strictly defined and are limited as required by the directions given in the decided cases.

In addition, the Commission's statute has centralized administration of police and law enforcement wiretapping in the Superior Court. As this is the chief trial court of the Commonwealth, and the tribunal which hears the most serious cases, it is hoped that there will be a better uniformity in the application of the law.

In addition, it is required that the original recording or tape or a sworn statement of the complete contents of the intercepted communication if there is no tape, be returned to the judge who issued the warrant so that he may determine whether or not the warrant has been executed in a manner in which he authorized it. This additional judicial supervision, it is hoped, will eliminate the possibility of abuse and add to the public's confidence in the manner in which this statute is employed by law enforcement officials.

The original tapes and statements are to be kept in the custody of the Chief Justice of the Superior Court. This provision has been added to eliminate the possibility of any editing between the time the tapes are obtained and the time they must be made available for trial. We feel this also aids the prosecutor in that the procedure eliminates false charges by a defendant that the tape had been edited or changed. It was felt by the Commission that this added control over the fruits of an interception will be a means of insuring the competence of the public in the system of judicially au-

thorized eavesdropping and wiretapping and a means of promoting confidence in the fairness of a trial in which such evidence is used.

The right of a defendant to be confronted with the evidence against him is protected in that any wiretap information to be used against the defendant must be shown to him prior to the trial.

Provisions are made for annual reports to the legislature describing the extent of wiretapping and eavesdropping conducted during the previous year by the judicial officers of the Commonwealth authorized to seek warrants for wiretapping under this bill.

*PROHIBITION OF WIRETAPPING
AND EAVESDROPPING BY THE PUBLIC*

The Commission is of the opinion that wiretapping and eavesdropping other than by law enforcement officers should be strictly prohibited. The present Massachusetts laws have been revised in our proposed act to strictly prohibit electronic eavesdropping and wiretapping of other persons' conversations without permission. Penalties have been increased and the crimes have been more strictly defined. Possession of illegal wiretapping devices has been made a crime under circumstances evincing an intent to illegally use those devices.

PRIVATE INVESTIGATORS

It is the Commission's view that private investigators should not be permitted to make use of eavesdropping and wiretapping devices. To this end, the Commission recommends the amendment of the Act regulating private investigators in order that their licenses may be revoked in the event they are convicted of any violation of the new wiretapping and eavesdropping statutes.

Respectfully submitted,

MARIO UMANA, *Chairman*
ELLIOT B. COLE
WILLIAM P. HOMANS, JR.
ANDRE R. SIGOURNEY
NORMAN S. WEINBERG
PHILLIP K. KIMBALL

Commission Member Elliot B. Cole concurs in the Commission's legislative recommendations.

Commission Member William P. Homans, Jr., joins Mr. Cole.

I join the majority of the Commission in their legislative recommendations, but I must add some comments on those provisions dealing with law enforcement eavesdropping and with "all-party consent".

In the past I have been a vigorous opponent of provisions which would permit law enforcement eavesdropping and wiretapping. This opposition has been based on both Constitutional considerations and the lack of information available on law enforcement eavesdropping practices.

Today I know no more than I did when I was appointed to this Commission about the practices and effectiveness of law enforcement eavesdropping. Indeed these two elements — practices and effectiveness — appear to be the most secret of all law enforcement secrets. As Prof. Alan Westin states in his treatise *Privacy and Freedom*.

'There has never been a detailed presentation by any law-enforcement agency, in terms that the educated public could judge, to prove this view (the need for wiretapping and eavesdropping in criminal investigations) on a crime-by-crime analysis.'

This Commission and Attorney General Richardson agree on the necessity of an annual report by the Commonwealth's prosecuting attorneys stating their activities in this area on a crime-by-crime basis. The secrecy of the past I believe is both destructive and alien to a democracy. It is the inclusion of the reporting provision, which was first put forth by the Attorney General, that has caused me to re-evaluate my previous opposition to law enforcement eavesdropping. It is to be hoped that the information contained in the prosecutor's annual report will provide a basis for the General Court to better evaluate its policy on law enforcement eavesdropping.

The other basis of my opposition to law enforcement eavesdropping has been its constitutionality. This controversy has raged within and without the United States Supreme Court since 1927 when that Court first decided the constitutionality of wiretapping.

In 1961, in *Silverman v. United States*, the Court indicated that eavesdropping under certain circumstances was violative of the Constitution. But recently, in *Berger v. New York*, the Court stated its tolerance for law enforcement eavesdropping given specific standards for judicial regulation. This Commission's Bill, as our Report explains, would implement those standards. If the Bill is not Constitutional and is enacted, I am sure that the Court will have an opportunity to so state.

The Commission have decided to recommend to the General Court a provision which would require the consent of all parties to a conversation before that conversation could be recorded or otherwise electronically 'intercepted'. It is the 'all-party consent' provision which is the essence of any protection which the law can afford the public.

But this view has not gained universal acceptance, and is opposed by those who see the possibility — what some of their number describe as the necessity — to secretly record the words of another. These advocates would maintain 'one-party consent', the present statutory standard. Their argument is based on the assumption that any participant in a conversation has the authority to divulge or publish the words and thoughts of his conversational partner. This assumption is ludicrous. If those participating in the conversation were mute and could only communicate via the written word, each participant would himself determine who had access to his thoughts. Furthermore, he could legally enforce his right by enjoining unauthorized publication of those thoughts.

The proponents of 'one-party consent' frequently justify their position by stating that every persons runs the risk that his confidence in the person to whom he is talking may be betrayed. This of course is true. But instead of protecting the individual from being betrayed, these proponents would legitimatize the betrayal. At the very least the individual should himself be able to determine who should have authority to mechanically reproduce his words.

Again I should like to rely on Prof. Westin. The first of the following passages is taken from that section of his book dealing with legislative provisions which would further protect the individual's right of privacy.

'(I) would *not* include an exception to allow wiretapping or eavesdropping with the consent of one party. This has been the basic charter for private-detective taps and bugs, for "owner" eavesdropping on facilities that are used by members of the public, and for much free-lance police eavesdropping. Allowing eavesdropping with the consent of one party would destroy the statutory plan of limiting the offenses for which eavesdropping by device can be used and insisting on a court-order process. And as technology enables every man to carry his micro-miniaturized recorder everywhere he goes and allows every room to be monitored surreptitiously by built-in equipment, permitting eavesdropping with the consent of one party would be to sanction a means of reproducing conversation that could choke off much vital social exchange.' (Emphasis in the original.)

The following passage is excerpted, with permission, from a letter to me from Prof. Westin on the advisability of incorporating the 'one-party consent' provision into a new Massachusetts statute.

'Based on the studies I have made on wiretapping and eavesdropping practices throught the United States, as reflected in my recently published book, *Privacy and Freedom* (New York: Atheneum, 1967), I believe such a provision is unwise. From a public policy standpoint, we must consider what would be the impact in the coming decade, when electronic monitoring devices spread even more widely in the population, of each citizen having to know that the person to whom he is talking in the office, at home, in his car, on the street, in a store, etc., may be recording the conversation with full legal authority and without having to have such clandestine recording authorized in advance by any judicial agency. I think this creates a serious inhibition on freedom of communication, especially because the person who chooses to speak frankly and freely in personal conversation runs the risk, under such a situation, that what he says in jest, with a wink, for its shock value on his conversational partner, or to test some belief held by the other party, can now be produced in evidence against him, with all the impact on the grand or petit jury, that we know such a tape recording exerts. In my book, I call this type of physical surveillance "surveillance by reproducibility." I quote from a 1958 opinion of the Bundesgerichtshof, West Germany's highest civil court, the dangers of this type of surveillance. The court states that "freedom and self-determination" are "essential to the development of [the individual's] personality." This freedom includes the right to decide for himself "whether his words shall be accessible solely to his conversation partner, to a particular group, or to the public, and, *a fortiori*, whether his voice shall be fixed on a record." The opinion notes further that the individual expresses his personality in private conversation, and has a right to do so freely, without distrust and suspicion. This expression of personality would disappear if individuals feared that their conversations, even their tone of voice, were secretly being recorded. Men would no longer be able to engage in natural, free discussion.'

It is clear to me that the passage of the Commissions Bill will protect the privacy of the individual while providing law enforcement agencies with the tools they feel are necessary in this technological era.

ELLIOT B. COLE

WILLIAM P. HOMANS, JR.

The Commonwealth of Massachusetts

APPENDIX A

AN ACT REPEALING THE PRESENT WIRETAPPING AND EAVESDROPPING
STATUTES AND PROVIDING A NEW STATUTE IN RELATION THERETO.

*Be it enacted by the Senate and House of Representatives in General
Court assembled, and by the authority of the same, as follows:*

- 1 Sections 99, 100, 101 and 102 of Chapter 272 of the General
2 Laws are hereby repealed and the following section substituted
3 in place thereof.
- 4 *Section 99.* Interception of wire and oral communications.
- 5 A. *Definitions.* As used in this section —
- 6 1. The term “wire communication” means any communi-
7 cation made in whole or in part through the use of facilities
8 for the transmission of communications by the aid of wire,
9 cable, or other like connection between the point of origin
10 and the point of reception.
- 11 2. The term “oral communications” means speech, except
12 such speech as is transmitted over the public air waves by
13 radio or other similar device.
- 14 3. The term “intercepting device” means any device or
15 apparatus which is capable of transmitting, receiving, ampli-
16 fying, or recording a wire or oral communication other than a
17 hearing aid or similar device which is being used to correct
18 subnormal hearing to normal.
- 19 4. The term “interception” means to secretly hear, secretly
20 record, or aid another to secretly hear or secretly record the
21 contents of any wire or oral communication through the use
22 of any intercepting device by any person other than a person
23 given prior authority by all parties to such communication.
- 24 5. The term “contents,” when used with respect to any
25 wire or oral communication, means any information concern-
26 ing the identity of the parties to such communication or the
27 existence, contents, substance, purport, or meaning of that
28 communication.

29 6. The term "aggrieved person" means any individual who
30 was a party to an intercepted wire or oral communication or
31 who was named in the warrant authorizing the interception
32 or whose personal or property interest or privacy were in-
33 vaded in the course of an interception.

34 7. The term "designated offense" shall include the offenses
35 of murder, armed robbery, prostitution, kidnapping, extortion,
36 suborning perjury, jury tampering, aggravated assault, arson,
37 bribery, gambling, larceny from the commonwealth, lending of
38 money or thing of value in violation of the laws of the com-
39 monwealth, any offense involving commercial dealings in nar-
40 cotics and any violation of the provisions of this section, being
41 an accessory to any of the foregoing offenses, and conspiracy
42 or attempt to commit any of the foregoing offenses.

43 8. The term "investigative or law enforcement officer"
44 means any officer of the United States, a state or a political
45 subdivision of a state, who is empowered by law to conduct
46 investigations of, or to make arrests for the designated of-
47 fenses, any attorney authorized by law to participate in the
48 prosecution of such offenses.

49 9. The term "judge of competent jurisdiction" means any
50 justice of the superior court of the commonwealth.

51 10. The term "chief justice" means the chief justice of
52 the superior court of the commonwealth.

53 11. The term "issuing judge" means any justice of the
54 superior court who shall issue a warrant as provided herein
55 or in the event of his disability or unavailability any other
56 judge of competent jurisdiction designated by the chief justice.

57 12. The term "communication common carrier" means any
58 person engaged as a common carrier in providing or opera-
59 ting wire communication facilities.

60 13. The term "person" means any individual, partnership,
61 association, joint stock company, trust, or corporation, whether
62 or not any of the foregoing is an officer, agent or employee
63 of the United States, a state, or a political subdivision of a
64 state.

65 14. The terms "sworn" or "under oath" as they appear in
66 this section shall mean an oath or by affirmation or a state-

67 ment subscribed to under the pains and penalties of perjury.
68 15. The terms "applicant attorney general" or "applicant
69 district attorney" shall mean the attorney general of the Com-
70 monwealth or a district attorney of the Commonwealth who
71 has made application for a warrant pursuant to this section.

72 16. The term "exigent circumstances" shall mean the show-
73 ing of special facts to the issuing judge as to the nature of the
74 investigation for which a warrant is sought pursuant to this
75 section which require secrecy in order to obtain the informa-
76 tion desired from the interception sought to be authorized.

77 B. *Offenses*

78 1. *Interception, oral communications prohibited.*

79 Except as otherwise specifically provided in this section
80 any person who —

81 willfully commits an interception, endeavors to commit
82 an interception, or procures any other person to commit
83 an interception or endeavor to commit an interception of
84 any wire or oral communication shall be fined not more
85 than ten thousand dollars, or imprisoned in the state prison
86 not more than five years, or imprisoned in a jail or house
87 of correction not more than two and one half years, or both
88 so fined any given one such imprisonment.

89 Proof of the installation of any intercepting device by
90 any person under circumstances evincing an intent to com-
91 mit an interception which is not authorized or permitted by
92 this section, shall be prima facie evidence of a violation of
93 this subparagraph.

94 2. *Editing of tape recordings in judicial proceeding pro-*
95 *hibited*

96 Except as otherwise specifically provided in this section
97 any person who —

98 willfully edits, alters or tampers with any tape, trans-
99 cription or recording of oral or wire communication by any
100 means, or endeavors to edit, alter or tamper with any tape,
101 transcription or recording of oral or wire communication
102 by any means with the intent to present in any judicial
103 proceeding or proceeding under oath, or who presents such
104 recording or permits such recording to be presented in any

105 judicial proceeding or proceeding under oath, without fully
106 indicating the nature of the changes made in the original
107 state of the recording, shall be fined not more than ten
108 thousand dollars (\$10,000.00) or imprisoned in the state
109 prison not more than five years or imprisoned in a jail or
110 house of correction not more than two years or both so
111 fined and given one such imprisonment.

112 3. *Disclosure, or use of wire or oral communications pro-*
113 *hibited.*

114 Except as otherwise specifically provided in this section
115 any person who —

116 a. willfully discloses or endeavors to disclose to any
117 person the contents of any wire or oral communication,
118 knowing that the information was obtained through in-
119 terception; or

120 b. willfully uses or endeavors to use the contents of
121 any wire or oral communication, knowing that the infor-
122 mation was obtained through interception shall be guilty
123 of a misdemeanor punishable by imprisonment in a jail
124 or a house of correction for not more than two years or
125 by a fine of not more than five thousand dollars or both.

126 4. *Disclosure of contents of applications, warrants, re-*
127 *newals, and returns prohibited.*

128 Except as otherwise specifically provided in this section
129 any person who —

130 willfully discloses to any person, any information con-
131 cerning or contained in, the application for, the granting
132 or denial of orders for interception, renewals, notice or
133 return on an ex parte order granted pursuant to this sec-
134 tion, or the contents of any document, tape, or recording
135 kept in accordance with paragraph M, shall be guilty of a
136 misdemeanor punishable by imprisonment in a jail or a
137 house of correction for not more than two years or by a
138 fine of not more than five thousand dollars or both.

139 5. *Duty to report to law enforcement officers.*

140 An employee of any communication common carrier who
141 has knowledge obtained during the course of such employ-
142 ment of any violation of this section and willfully fails to

143 report such knowledge within seven days to a district at-
144 torney general shall be guilty of a misdemeanor punishable
145 by imprisonment in a jail or a house of correction for not
146 more than two years or by a fine of not more than five
147 thousand dollars or both.

148 6. *Possession of Interception Devices Prohibited.*

149 A person who possesses any intercepting device under
150 circumstances evincing an intent to commit an interception
151 not permitted or authorized by this Section, or a person who
152 permits an intercepting device to be used or employed for
153 an interception not permitted or authorized by this Sec-
154 tion, or a person who possesses an intercepting device know-
155 ing that the same is intended to be used to commit an in-
156 terception not permitted or authorized by this Section, shall
157 be guilty of a misdemeanor punishable by imprisonment in
158 a jail or house of correction for not more than two years
159 or by a fine or not more than five thousand dollars or both.

160 The installation of any such intercepting device by such
161 person or with his permission or at his direction shall be
162 prima facie evidence of possession as required by this sub-
163 paragraph.

164 7. Any person who permits or on behalf of any other
165 person commits or endeavors to commit, or any person who
166 participates in a conspiracy to commit or to endeavor to
167 commit, or any accessory to a person who commits a viola-
168 tion of subparagraphs 1 through 6 of paragraph B of this
169 section shall be punished in the same manner as is provided
170 for the respective offenses as described in subparagraph 1
171 through 6 of paragraph B.

172 C. *Exemptions.*

173 1. *Permitted interception of wire or oral communications.*

174 It shall not be a violation of this section —

175 a. for an operator of a switchboard, officer, agent or
176 employee of any communication common carrier, whose
177 facilities are used in the transmission of a wire communi-
178 cation, to intercept, to disclose to officers, agents or em-
179 ployees of a communication common carrier, or use that
180 communication in the normal course of his employment

181 if such interception shall be made necessary in order to
182 repair or test equipment and lines of such communica-
183 tion common carrier, or

184 b. for persons to possess an office intercommunication
185 system which is used in the ordinary course of their
186 business or to use such office intercommunication system
187 in the ordinary course of their business.

188 c. for investigative and law enforcement officers of the
189 United States of America to violate the provisions of this
190 section if acting pursuant to authority of the laws of
191 the United States and within the scope of their authority.

192 d. for any person duly authorized to make specified
193 interceptions by a warrant issued pursuant to paragraph
194 E of this section.

195 2. *Permitted disclosure and use of intercepted wire or*
196 *oral communications.*

197 a. Any investigative or law enforcement officer, who,
198 by any means authorized by this section, has obtained
199 knowledge of the contents of any wire or oral communi-
200 cation, or evidence derived therefrom may disclose such
201 contents or evidence in the proper performance of his
202 official duties.

203 b. Any investigative or law enforcement officer, who,
204 by any means authorized by this section has obtained
205 knowledge of the contents of any wire or oral communi-
206 cation, or evidence derived therefrom, may use such con-
207 tents or evidence in the proper performance of his official
208 duties.

209 c. Any person who has obtained, by any means au-
210 thorized by this section, knowledge of the contents of any
211 wire or oral communication, or evidence derived there-
212 from, may disclose such contents while giving testi-
213 mony under oath or affirmation in any criminal proceed-
214 ing in any court of the United States or of any state or
215 in any Federal or state grand jury proceeding.

216 d. The contents of any wire or oral communication
217 intercepted pursuant to a warrant in accordance with the
218 provisions of this section, or evidence derived therefrom,

219 may otherwise be disclosed only upon a showing of good
220 cause before a judge of competent jurisdiction.

221 D. *Warrants: when issuable.*

222 A warrant may issue only upon sworn application in con-
223 formity with this section and upon a showing by the appli-
224 cant that there is probable cause to believe that the designated
225 offense has been, is being, or is about to be committed and
226 that evidence of the commission of such an offense may thus
227 be obtained or that information which will aid in the appre-
228 hension of a person who the applicant has probable cause to
229 believe has committed, is committing, or is about to commit a
230 designated offense may thus be obtained.

231 E. *Warrants: application.*

232 1. Application. The attorney general, any assistant at-
233 torney general specially designated by the attorney general,
234 any district attorney, or any assistant district attorney
235 specially designated by the district attorney may apply ex
236 parte to a judge of competent jurisdiction for a warrant to
237 intercept wire or oral communications. Each application
238 ex parte for a warrant must be in writing, subscribed and
239 sworn to by the applicant authorized by this subparagraph.

240 2. The application must contain the following:

241 a. A statement of facts establishing probable cause to
242 believe that a particularly described designated offense
243 has been, is being, or is about to be committed; and

244 b. A statement of facts establishing probable cause to
245 believe that oral or wire communications of a particularly
246 described person will constitute evidence of such designa-
247 ted offense or will aid in the apprehension of a person
248 who the applicant has probable cause to believe has com-
249 mitted, is committing, or is about to commit a designated
250 offense; and

251 c. That the oral or wire communication of the par-
252 ticularly described person or persons will occur in a par-
253 ticularly described place and premises or over particularly
254 described telephone or telegraph lines; and

255 d. A particular description of the nature of the con-
256 versation sought to be overheard; and

257 e. A statement that the conversation sought is ma-
258 terial to a particularly described investigation or prose-
259 cution and that such conversation is not legally privileged;
260 and

261 f. a statement of the period of time for which the in-
262 terception is required to be maintained. If practicable,
263 the application should designate hours of the day or night
264 during which the conversation may be reasonably ex-
265 pected to occur. If the nature of the investigation is
266 such that the authorization for the interception should not
267 automatically terminate when the described conversa-
268 tion has been first obtained, the application must specifi-
269 cally state facts establishing probable cause to believe that
270 additional conversation of the same nature will occur
271 thereafter; and

272 g. If it is reasonably necessary to make a secret entry
273 upon a private place and premises in order to install an
274 intercept device to effectuate the purposes of the appli-
275 cation, a statement to such effect; and

276 h. If a prior application has been submitted or a
277 warrant previously obtained for eavesdropping, a state-
278 ment fully disclosing the date, court, applicant, execu-
279 tion, results, and present status thereof; and

280 8. If there is good cause for requiring the postpone-
281 ment of service pursuant to paragraph K, subparagraph
282 2, a description of such circumstances, including reasons
283 for the applicant's belief that secrecy is essential to ob-
284 taining the evidence or information sought.

285 3. Allegations of fact in the application may be based
286 either upon the personal knowledge of the applicant or upon
287 information and belief. If the applicant personally knows
288 the fact alleged, it must be so stated. If the facts estab-
289 lishing such probable cause are derived in whole or part
290 from the statements of persons other than the applicant,
291 the sources of such information and belief must be either
292 disclosed or described, and the application must contain
293 facts establishing the existence and reliability of any in-
294 formant and, the reliability of the information supplied by

295 him. The application must also state, so far as possible,
296 the basis of the informant's knowledge or belief. If the
297 applicant's information and belief is derived from tangible
298 evidence or recorded oral evidence, a copy or detailed de-
299 scription thereof should be annexed to or included in the
300 application. Affidavits of persons other than the applicant
301 may be submitted in conjunction with the application if
302 they tend to support any fact or conclusion alleged therein.
303 Such accompanying affidavits may be based either on per-
304 sonal knowledge of the affiant or information and belief,
305 with the source thereof, and reason therefor, specified.

306 *F. Warrants; application to whom made.*

307 Application for a warrant authorized by this section must
308 be made to a judge of competent jurisdiction in the county
309 where the interception is to occur, or the county where
310 the office of the applicant is located, or in the event that
311 there is no judge of competent jurisdiction sitting in said
312 county at such time, to a judge of competent jurisdiction
313 sitting in Suffolk County; except that for these purposes
314 the office of the attorney general shall be deemed to be
315 located in Suffolk County.

316 *G. Warrants; application how determined.*

317 1. If the application conforms to paragraph E, the issuing
318 judge may examine under oath any person for the purpose
319 of determining whether probable cause exists for the is-
320 suance of the warrant pursuant to paragraph D. A verbatim
321 transcript of every such interrogation or examination must
322 be taken and a transcription of the same sworn to by the
323 stenographer shall be attached to the application and be
324 deemed a part thereof.

325 2. If satisfied that probable cause exists for the issuance
326 of a warrant the judge may grant the application and issue
327 a warrant in accordance with paragraph H. The applica-
328 tion and an attested copy of the warrant shall be retained
329 by the issuing judge and transported to the chief justice
330 of the superior court in accordance with the provisions of
331 paragraph M of this section.

332 3. If the application does not conform to paragraph E,

333 or if the judge is not satisfied that probable cause has
334 been shown sufficient for the issuance of a warrant, the
335 application must be denied.

336 H. *Warrants; form and content.*

337 A warrant must contain the following:

338 1. The subscription and title of the issuing judge; and

339 2. The date of issuance, the date of effect, and termina-
340 tion date which in no event shall exceed thirty days from
341 the date of effect. The warrant shall permit interception
342 for a period not to exceed fifteen days. If physical instal-
343 lation of a device is necessary, the thirty day period shall
344 begin upon the date of installation. If the effective period
345 of the warrant is to terminate upon the acquisition of
346 particular evidence or information, the warrant shall so
347 provide; and

348 3. A particular description of the person and the place,
349 premises or telephone or telegraph line upon which inter-
350 ception may be conducted; and

351 4. A particular description of the nature of the conversa-
352 tion to be obtained by the interception including a state-
353 ment of the designated offense to which it relates; and

354 5. An express authorization to make secret entry upon
355 a private place or premises to install a specified intercepting
356 device, if such entry is necessary to execute the warrant;
357 and

358 6. A statement providing for service of the warrant
359 pursuant to Paragraph K, except that if there has been a
360 finding of good cause shown requiring the postponement of
361 such service, a statement of such finding together with
362 the basis therefor must be included and an alternative
363 direction for deferred service pursuant to Paragraph K,
364 Subparagraph 2.

365 I. *Warrants; renewals.*

366 1. Any time prior to the expiration of a warrant or a
367 renewal thereof, the applicant may apply to the issuing
368 judge for a renewal thereof with respect to the same
369 person, place, premises or telephone or telegraph line. An
370 application for renewal must incorporate the warrant sought

371 to be renewed together with the application therefor and
372 any accompanying papers upon which it was issued. The
373 application for renewal must set forth the results of the
374 interceptions thus far conducted. In addition it must set
375 forth present grounds for extension in conformity with
376 paragraph E.

377 2. Upon such application, the judge may issue an order
378 renewing the warrant and extending the authorization for
379 a period not exceeding fifteen (15) days from the entry
380 thereof. Such an order shall specify the grounds for the
381 issuance thereof. An attested copy of the order shall be
382 retained by the issuing judge to be transported to the chief
383 justice in attendance with the provisions of sub-paragraph
384 M of this section.

385 *J. Warrants; manner and time of execution.*

386 1. A warrant may be executed pursuant to its terms
387 anywhere in the Commonwealth.

388 2. Such warrant may be executed by the authorized
389 applicant personally or by any investigative or law enforce-
390 ment officer of the Commonwealth designated by him for
391 the purpose.

392 3. The warrant may be executed according to its terms
393 during the hours specified therein, and for the period there-
394 in authorized, or a part thereof. The authorization shall
395 terminate upon the acquisition of the conversations de-
396 scribed in the warrant. Upon termination of the authoriza-
397 tion in the warrant and any renewals thereof, the inter-
398 ception must cease at once, and any device installed for
399 the purpose of the interception must be removed as soon
400 thereafter as practicable. Entry upon private premises for
401 the removal of such device is deemed to be authorized
402 by the warrant.

403 *K. Warrants; service thereof.*

404 1. Prior to the execution of a warrant authorized by this
405 section or any renewal thereof, an attested copy of the
406 warrant or the renewal, must, except as otherwise provided
407 in subparagraph 2 of paragraph K, be served upon a per-
408 son whose conversation is to be obtained, and if an inter-

409 cepting device is to be installed upon the owner, lessee,
410 or occupant of the place or premises, or upon the sub-
411 scriber to the telephone or owner or lessee of the
412 telegraph line described in the warrant.

413 2. If the application specially alleges exigent circum-
414 stances requiring the postponement of service and the
415 issuing judge finds that such circumstances exist, the war-
416 rant may provide that an attested copy thereof may be
417 served within thirty days after the expiration of the war-
418 rant or, in case of any renewals thereof, within thirty
419 days after the expiration of the last renewal; except that
420 upon a showing of important special facts which set forth
421 the need for continued secrecy to the satisfaction of the
422 issuing judge, said judge may direct that the attested copy
423 of the warrant be served on such parties as are required
424 by this section at such time as may be appropriate in the
425 circumstances but in no event may he order it to be
426 served later than two (2) years from the time of expi-
427 ration of the warrant or the last renewal thereof. In the
428 event that the service required herein is postponed in ac-
429 cordance with this paragraph, in addition to the require-
430 ments of any other paragraph of this section, service of
431 an attested copy of the warrant shall be made upon any
432 aggrieved person who should reasonably be known to the
433 person who executed or obtained the warrant as a result
434 of the information obtained from the interception author-
435 ized thereby.

436 3. The attested copy of the warrant shall be served on
437 persons required by this section by any investigative or
438 law enforcement officer of the commonwealth authorized
439 to serve criminal process by leaving the same at his usual
440 place of abode, or in hand, or if this is not possible by
441 mailing the same by certified or registered mail to his
442 last known place of abode. A return of service shall be
443 made to the issuing judge, except, that if such service is
444 postponed as provided in sub-paragraph 2 of paragraph K,
445 and in such event to the chief justice. The return of service

446 shall be deemed a part of the return of the warrant and
447 attached thereto.

448 *L. Warrant; return.*

449 Within twenty-one days after termination of the warrant
450 or the last renewal thereof, a return must be made there-
451 on to the judge issuing the warrant by the applicant
452 therefor, containing the following:

- 453 a. a statement of the nature and location of the com-
454 munications facilities, if any, and premises or places
455 where the interceptions were made; and
456 b. The periods of time during which such interceptions
457 were made; and
458 c. the names of the parties to the communications inter-
459 cepted if known; and
460 d. the original recording of the oral or wire communica-
461 tions intercepted, if any; and,
462 e. a verbatim transcript of any recording made pursuant
463 to the warrant attested under the pains and penalties of
464 perjury as a true transcript of the oral or wire com-
465 munications contained in the recording to the best
466 ability of the person who so transcribed it and a
467 statement attested under the pains and penalties of
468 perjury by each person who heard oral or wire com-
469 munications as a result of the interception authorized
470 by the warrant which was not recorded stating every-
471 thing that was overheard to the best of their recollec-
472 tion at the time of the execution of the statement.

473 *M. Custody and Secrecy of papers and recordings made*
474 *pursuant to a warrant.*

475 1. The contents of any wire or oral communication in-
476 tercepted pursuant to a warrant issued pursuant to this
477 section shall, if possible be recorded on tape or wire or
478 other similar device. Duplicate recordings may be made
479 for use pursuant to subparagraphs 2(a) and (b) of para-
480 graph C for investigations. Upon examination of the re-
481 turn and a determination that it complies with this sec-
482 tion, the issuing judge shall forthwith order that the appli-
483 cation, warrant, all renewal orders and the return thereof

484 be transmitted to the chief justice by such persons as he
485 shall designate. Their contents shall not be disclosed ex-
486 cept as provided in this section. The application, warrant,
487 the renewal order and the return or any one of them or
488 any part of them may be transferred to any trial court,
489 grand jury proceeding of any jurisdiction by any law en-
490 forcement or investigative officer designated by the chief
491 justice upon application made as provided herein and a
492 trial justice may allow them to be disclosed in accordance
493 with paragraph C, subparagraph 2, or paragraph N or
494 any other applicable provision of this section.

495 The application, warrant, all renewal orders and the
496 return, shall be stored in a secure place which shall be
497 designated by the chief justice, to which access shall be
498 denied to all persons except the chief justice or such court
499 officers or administrative personnel of the court as he shall
500 designate.

501 2. Upon application to the chief justice,

502 a. ex parte by the applicant district attorney or his suc-
503 cessor or the applicant attorney general or his successor,
504 the application, warrant, renewal orders, or return, shall
505 be made available for their use under such conditions as
506 will comply with the provisions of this section.

507 b. ex parte by any person or his attorney who is named
508 in the application, warrant, any renewal orders or the re-
509 turn or who can offer evidence sufficient to show that
510 his oral or wire communications have been intercepted
511 pursuant to a warrant, an attested copy of the application,
513 and statement, which are a part of the return as required
513 and statement, which are a part of the return as required
514 by this section shall be made available without charge
515 upon oath or affirmation by the person or his attorney
516 that the items described herein or any one of them, or
517 information contained therein is to be used in any criminal
518 proceeding in any jurisdiction where the person is a de-
519 fendant.

520 c. to any other person who shall have need in the interest
521 of justice and in accordance with the purposes of this act,

522 the original or copies of the application, warrant, renewal
523 orders, and return, or all of them under such terms or
524 conditions as the chief justice shall determine. Such appli-
525 cation shall be upon oath or affirmation by the person
526 and shall state sufficient reliable facts to enable the chief
527 justice to determine from its face the interception sought.
528 In the event the application does not so state such facts
529 the chief justice shall deny it. In the event the application
530 shall state such sufficient facts the chief justice shall cause
531 the applicant district attorney or attorney general or their
532 their respective successors to be notified of the application
533 pursuant to this sub-paragraph. If the district attorney
534 or attorney general submit to the chief justice a statement
535 in writing upon oath or affirmation within thirty (30)
536 days following notification stating that the information
537 sought must remain secret for investigative purposes, the
538 chief justice must refuse to grant an application pursuant
539 to this sub-paragraph. In such event he may require the
540 district attorney or attorney general to designate a date
541 at which time the information may be made available
542 to the person making the application in the event the
543 chief justice shall determine that the person has need in
544 the interests of justice and in accordance with the pur-
545 poses of this act. Such a date may not exceed three (3)
546 years from the date of an application pursuant to the sub-
547 paragraph nor may it exceed thirty (30) days prior to
548 the date of destruction of the respective document or
549 items as required by this section whichever is sooner.
550 Determination of the need of the person applying pursuant
551 to this sub-paragraph shall be in the discretion of the chief
552 justice.

553 d. Except as provided by other provisions of this section,
554 in no event until an application is granted pursuant to
555 sub-paragraphs a, b, c of paragraph M by the chief justice
556 or upon order granted by the Supreme Judicial Court
557 after appeal, shall the person applying pursuant to sub-
558 paragraphs a, b or c of Paragraph M or any person on
559 his behalf at any time or for any reason have any right

560 nor be granted permission to examine any of the applica-
561 tions, warrants, renewals orders, or returns in the custody
562 of the chief justice.

563 e. In addition to any other appeal provided by law,
564 failure by the chief justice to grant an application pursuant
565 to sub-paragraph a, b, or c of Paragraph M may be ap-
566 pealed within twenty (20) days to the Supreme Judicial
567 Court in Suffolk County by the applicant or his attorney.
568 The granting of an application pursuant to sub-paragraph
569 c of section M may be appealed by the applicant district
570 attorney or attorney general or their respective successors
571 within twenty (20) days to the supreme judicial court in
572 Suffolk County. The supreme judicial court may take ad-
573 ditional testimony, may order the production for its use
574 of any of the applications, renewal orders, warrants or
575 returns or copies thereof as it may require for determina-
576 tion of the issues by it.

577 f. Any violation of the terms and conditions of the chief
578 justice or any order of the supreme judicial court pursuant
579 to the authority granted in Paragraph M or the conditions
580 set forth in Paragraph M shall be punished as a criminal
581 contempt of court in addition to any other punishment
582 authorized by law.

583 g. The application, warrant, renewal and return shall be
584 kept for a period of five (5) years from the date of the
585 issuance of the warrant or the last renewal thereof at
586 which time they shall be destroyed by a person designated
587 by the chief justice. Notice of the destruction shall be
588 given to the applicant attorney general or his successor
589 or the applicant district attorney or his successor and upon
590 a showing of good cause to the chief justice, the applica-
591 tion, warrant, renewal, and return may be kept for such
592 additional period as the chief justice shall determine but
593 in no event longer than the longest period of limitation
594 for any designated offense specified in the warrant, after
595 which time they must be destroyed by a person designated
596 by the chief justice.

597 *N. Introduction of evidence.*

598 Notwithstanding any other provisions of this section or
599 any order issued pursuant thereto, in any criminal trial
600 where the Commonwealth intends to offer in evidence any
601 portions of the contents of any interception or any evidence
602 derived therefrom, the defendant shall be served with a
603 complete copy of each document and item which make
604 up each application, warrant, renewal orders, and return
605 pursuant to which the information was obtained, except
606 that he shall be furnished a copy of any recording instead
607 of the original. The service must be made at the arraigh-
608 ment of the defendant or, if a period in excess of thirty
609 (30) days shall elapse prior to the commencement of the
610 trial of the defendant, the service may be made at least
611 thirty (30) days before the commencement of the criminal
612 trial. Service shall be made in hand upon the defendant
613 or his attorney by any investigative or law enforcement
614 officer of the Commonwealth authorized to serve criminal
615 process. Return of the service required by this sub-para-
616 graph including the date of service shall be entered into
617 the record of trial of the defendant by the Commonwealth
618 and such return shall be deemed prima facie evidence
619 of the service described therein. Failure by the Common-
620 wealth to make such service at the arraignment or if de-
621 layed at least thirty (30) days before the commencement
622 of the criminal trial shall render such evidence illegally
623 obtained for purposes of the trial against the defendant
624 and such evidence shall not be offered nor received at
625 the trial notwithstanding the provisions of any other law
626 or Rules of Court.

627 *P. Suppression of evidence.*

628 Any aggrieved person who is a defendant in a criminal
629 trial in a court of the commonwealth may move to sup-
630 press the contents of any intercepted wire or oral com-
631 munication or evidence derived therefrom, for the follow-
632 ing reasons:

633 1. That the communication was unlawfully intercepted.

634 2. That the communication was not intercepted in ac-
635 cordance with the terms of this section.

636 3. That the application or renewal application fails to
637 set forth facts sufficient to establish probable cause for
638 the issuance of a warrant.

639 4. That the interception was not made in conformity
640 with the warrant.

641 5. That the evidence sought to be introduced was illegally
642 obtained.

643 6. That the warrant does not conform to the provisions
644 of this section.

645 Q. *Civil Remedy.*

646 Any aggrieved person whose oral or wire communica-
647 tions were intercepted, disclosed or used except as permit-
648 ted or authorized by this section or whose personal
649 or property interests or privacy were violated by means
650 of an interception except as permitted or authorized by
651 this section shall have a civil cause of action against any
652 person who so intercepts, discloses or uses such communi-
653 cations or who so violates personal, property or privacy
654 interest and shall be entitled to recover from any such
655 person —

656 1. actual damages but not less than liquidated damages
657 computed at the rate of \$100 per day for each day of
658 violation or \$1000, whichever is higher;

659 2. punitive damages; and

660 3. a reasonable attorney's fee and other litigation dis-
661 bursements reasonably incurred. Good faith reliance on a
662 warrant issued under this section shall constitute a com-
663 plete defense to an action brought under this paragraph.

664 R. *Annual Report of Interceptions of the General Court.*

665 On the second Friday of January, each year, the attorney
666 general and each district attorney shall submit a report
667 to the general court stating (1) the number of applications
668 made for warrants during the previous year, (2) the name
669 of the applicant, (3) the number of warrants issued, (4)
670 the effective period for the warrants, (5) the number and
671 designation of the offenses for which those applications

672 were sought, and for each of the designated offenses the
673 following: (a) the number of renewals, (b) the number
674 of intercepts made during the previous year, (c) the num-
675 ber of indictments believed to be obtained as a result of
676 those intercepts, (d) the number of criminal convictions
677 obtained in trials where interception evidence was intro-
678 duced. This report shall be a public document and be
679 made available to the public at the offices of the attorney
680 general and district attorneys. In the event of failure to
681 comply with the provisions of this paragraph any person
682 may compel compliance by means of an action of manda-
683 mus.

684 *S. Severability.*

685 If any provision of this section or application thereof
686 to any person or circumstances is held invalid, such inval-
687 idity shall not affect other provisions of applications of the
688 section which can be given effect without the invalid pro-
689 vision or application, and to this end the provisions of this
690 section are declared to be severable.

The Commonwealth of Massachusetts

APPENDIX B

1 CHAPTER 166 OF THE GENERAL LAWS IS HEREBY
2 AMENDED BY ADDING THE FOLLOWING AFTER SEC-
3 TION 43:

4 *Section 44. Service Observing, Interception.* — Service ob-
5 serving of telephone lines conducted by telephone companies
6 for the purpose of determining the quality of transmission or
7 for any other purpose shall cease as soon as a connection is es-
8 tablished between the users of the telephone line. In the event
9 of any interception or any recording of the conversation of
10 users by any telephone company to repair or test the equip-
11 ment and lines of the company, the telephone company shall
12 cause to be emitted a "beep" tone or other identifying signal
13 in order to inform the users of the interception or recording.
14 The Department of Public Utilities shall require that each
15 telephone company file annually with it a complete report of
16 all service observing activity carried on by any telephone com-
17 pany to indicate the number of calls monitored during the
18 previous calendar year, all rules and regulations of the tele-
19 phone companies for such service observing, a complete de-
20 scription of the location of each service observing facility, the
21 number of employees engaged in service observing and a state-
22 ment of the expenses incurred for such service observing to
23 include salaries, cost of capital equipment and maintenance
24 and replacement costs of such equipment, and administrative
25 expenses incurred. The Department shall also conduct peri-
26 odic inspections at least semi-annually of such service ob-
27 serving to determine whether or not it complies with this sec-
28 tion and the accuracy of the reports filed. In the event of the
29 failure of any telephone company to comply with this section
30 the Department of Public Utilities must order that the activity
31 cease until compliance is obtained and may seek an enforce-
32 ment order in the Superior Court of Suffolk County.

The Commonwealth of Massachusetts

APPENDIX "C"

AMENDMENT TO THE PRIVATE DETECTIVE BUSINESS ACT

1 Chapter 147, Section 25 of the General Laws is amended by
2 adding the following sentences after the last sentence of the
3 first paragraph:

4 "No person convicted of a violation of Section 99 or 99A of
5 Chapter 272 of the General Laws shall be granted a license
6 and any license previously granted to such person shall be
7 revoked."

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION
No. 2384CV00411-BLS-1JANE DOE,¹vs.

THE CHILDREN'S HOSPITAL CORPORATION

MEMORANDUM OF DECISION AND ORDER ON
DEFENDANT'S MOTION TO DISMISS

Plaintiff Jane Doe commenced this putative class action against defendant The Children's Hospital Corporation ("Boston Children's"), alleging that it used internet tracking tools on its website that illegally redirected website users' personal information, and the contents of their communications with Boston Children's website, to Google, Meta, and other third parties. On the basis of these allegations, the Complaint asserts a single claim for violation of the Massachusetts Wiretap Statute, G.L. c. 272, § 99. Presently before the court is Boston Children's motion to dismiss. After a hearing on July 26, 2023, and consideration of the parties' submissions, the motion is **DENIED**.

BACKGROUND

The Complaint sets forth the following facts. Boston Children's provides pediatric medical services at locations in Boston and surrounding communities, including seven hospital campuses and four physician offices. All of Boston Children's facilities share a website, which Boston Children's maintains and controls. Plaintiff is an individual residing in Burlington, Massachusetts.

¹ For herself and the class.

The Boston Children's website allows users to obtain information about the services Boston Children's provides, including information about doctors, services, and treatments provided for particular medical conditions. Website users can also book appointments, access and pay bills, and access private medical information through the MyChildren's Patient Portal. The website contains search bars that aid users in finding specific information on the site, and forms that users may submit to Boston Children's, such as the "Request an Appointment" form.

The Boston Children's "Web Site User Privacy Rights" notice ("Privacy Notice") states that:

Boston Children's Hospital is strongly committed to protecting the privacy of its online users: patients, families, donors, the media, and others. We do not collect personally identifiable information about individuals, except when it is knowingly provided by such individuals (e.g., web forms). We do not share voluntarily provided, personally identifiable information for any purpose other than its intended use.

(formatting altered). The Privacy Notice also discloses that Boston Children's collects "some basic web log file data about site visitors . . . includ[ing] domain names, website traffic patterns and server usage statistics [which] is used for site management and administration and to improve the overall performance and user experience on our site." The Privacy Notice further states that any web forms a user submits "are located on a secure site," and informs users that Boston Children's does "not sell visitors' personal information to third parties, such as marketers."

Notwithstanding this Privacy Notice, Boston Children's has implemented multiple software-based internet tracking technologies on its website that contemporaneously record and transmit data about users' interactions with Boston Children's website to third parties. The software is unrelated to the website's functionality and is invisible to users. Two such tracking

technologies are Meta Pixel, which transmits data to Meta (the parent company of Facebook), and Google Analytics, which transmits data to Google.

Meta Pixel and Google Analytics operate through the automatic execution of pieces of JavaScript code, embedded in the Boston Children's website, which cause a website user's internet browser to record and send information to those third parties when a user visits the site. The transmitted information can include: the website address (URL); the title of webpages visited; information about the content of the website; search terms or any other information inputted into a form; selections on drop-down menus and the contents thereof; scrolls down a webpage; and button clicks. A website user's internet protocol ("IP") address and web browser configurations are also revealed, which permits Google and Meta to associate the data it receives from the website visit to the identity of a particular individual known to them. The content of the user's communications with Boston Children's website is added to Google's and Meta's collection of information already known about the individual, which can be used to target advertising to that individual. After a media exposé about the use of Meta Pixel on hospital websites, Boston Children's removed it from its website in June 2022. As of the date the Complaint was filed, Google Analytics software remains on the Boston Children's website.

In addition to Meta Pixel and Google Analytics, Boston Children's also employs other software-based internet tracking technologies that work in a similar fashion. Those include Bing Ads, Doubleclick, and LinkedIn Insight. Boston Children's also uses Hotjar, which is a "session replay" provider that allows Boston Children's to "replay" a particular individual's visit to its website, including every mouse move, click, and page loaded.

Plaintiff regularly uses the Boston Children's website to obtain information about Boston Children's doctors (including their credentials and backgrounds); search for information on

particular symptoms, conditions, and medical procedures, both for herself and her children; and obtain and review her children's medical records through the MyChildren's Patient Portal.

STANDARD OF REVIEW

Rule 12(b)(6) allows for dismissal of a complaint when the factual allegations contained within it do not suggest a plausible entitlement to relief. *Iannacchino v. Ford Motor Co.*, 451 Mass. 623, 635-636 (2008); *Fraelick v. Perket PR, Inc.*, 83 Mass. App. Ct. 698, 699-700 (2013). In ruling on the motions, the court accepts the factual allegations as true and draws all reasonable inferences in the non-moving party's favor. *Fraelick*, 83 Mass. App. Ct. at 699-700.

DISCUSSION

The Massachusetts Wiretap Statute, G.L. c. 272, § 99(Q), provides a cause of action for "any aggrieved person whose oral or wire communications were intercepted, disclosed or used . . . or whose personal or property interests or privacy were violated by means of an interception," except as permitted or authorized by the Wiretap Statute. "Interception" is defined to mean "to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication." G.L. c. 272, § 99(B)(4).

Boston Children's argues that dismissal is required because the website interactions alleged were not "communications" under the statute, and because software code is not a qualifying "intercepting device." It further argues that internet tracking is not a secret, and that the Complaint fails to plead that the "contents" of a communication were intercepted where only hypothetical rather than actual website usage was alleged. None of the arguments are availing.

1. Communications

Boston Children's argues that because the Massachusetts Wiretap Statute was enacted in 1968, the Legislature only could have meant for it to prohibit the interception of communications consisting of human-to-human speech and/or conversation, not the modern website interactions at issue here. The claim is unsupported, both by the statute itself, and the relevant caselaw interpreting it.

To begin, the term "communication" is undefined in the statute. Its common dictionary definition, however, is not limited to human-to-human speech or conversation, but, as common sense would dictate, includes writing and signs. *See Webster's College Dictionary 274 (1991)* ("communication" defined, in part, as "the imparting or interchange of thoughts, opinions, or information by speech, writing, or signs").

An analysis of legislative intent likewise points to the inclusion of the website interactions here as communications under the statute. The preamble to the Massachusetts Wiretap Statute states that it was enacted "to curtail two 'grave dangers': (1) 'the increasing activities of organized crime' and (2) 'the uncontrolled development and unrestricted use of modern electronic surveillance devices,' which the Legislature termed a danger 'to the privacy of all citizens.'" *Commonwealth v. Ennis*, 439 Mass. 64, 68 (2003) (quoting G.L. c. 272, § 99(A)). Nothing in this stated intent or in the remaining statutory language limits its reach to human-to-human speech or conversation as Boston Children's argues. Indeed, the Supreme Judicial Court has established that the statute is to be interpreted broadly, and consistent with that principle, has applied it to electronic text messages, a technology that did not exist in 1968. *See*

Commonwealth v. Moody, 466 Mass. 196, 209 (2013).² Online searches for doctors and requests for appointment also did not exist in 1968, but, similar to texting, are the modern equivalent of telephone inquiries and conversations with doctors' offices that would have occurred then.³ As such, they are protected under the statute.

2. Intercepting Device

Boston Children's next argues that the statutory term "intercepting device" does not encompass the Meta Pixel and Google Analytics software at issue. Again, the argument is unavailing. As relevant here, the Massachusetts Wiretap Statute broadly defines an "intercepting device" as "any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication." G.L. c. 272, § 99(B)(3). Nothing in this language limits intercepting devices to being physical, tangible objects; neither does the common dictionary definition of "device" so limit that term. See Webster's College Dictionary 370 (1991) ("device" defined as "a thing made for a particular purpose, esp. a mechanical, electric, or electronic invention or contrivance"). Moreover, where cell phone, tablet, and computer applications and programs, and their interfacing with the internet, all rely on software for their operation, its use is practically implicit in any modern electronic communication. Thus, to restrict software code from being considered an intercepting device as Boston Children's suggests would essentially nullify the statute's application.⁴

² The court is unpersuaded by Boston Children's citation to *Commonwealth v. Connolly*, 454 Mass. 808, 825 (2009), particularly in light of the above holding in *Moody*.

³ Boston Children's argues that the website interactions alleged are more like old-fashioned library research than telephone calls with another party. While that might be true of a general internet search of a medical condition, the allegations here include other more targeted online inquiries, as discussed, and also involve a medical provider's website.

⁴ For this reason, in the context of the Massachusetts Wiretap Statute, the court does not consider persuasive the more restricted Black's Law Dictionary definition of "device" that Boston Children's cites.

Because the software code at issue is alleged to have recorded and transmitted the contents of Plaintiff's communications with Boston Children's website and her personal information to third parties, the Complaint sufficiently alleges the use of an intercepting device. *See Alves v. BJ's Wholesale Club, Inc.*, 22-2509-BLS1, slip op. at 10 (Super. Ct. June 21, 2023) (citing *United States v. Hutchins*, 361 F. Supp. 3d 779, 795 (E.D. Wis. 2019)) ("The majority of courts to consider this issue have entertained the notion that software may be considered a device for the purposes of the [Federal] Wiretap Act"); *Rich v. Rich*, 2011 WL 3672059, at *6 (Mass. Super. 2011) (key logger software program deemed to be "intercepting device" under Massachusetts Wiretap Statute).⁵

3. Secret Recording

Boston Children's argues that Plaintiff consented to the disclosure of information when she visited the Boston Children's website because its Privacy Notice informs users that it gathers information "to enhance the useability of its website." For this reason, Boston Children's asserts that any interception was not secret, as required. *See* G.L. c. 272, § 99(B)(4). The relevant standard under the Massachusetts Wiretap Statute for showing an interception was not secret is "actual [or constructive] knowledge," which is proved through "clear and unequivocal objective manifestations of knowledge" in the [users'] statements or conduct." *Commonwealth v. Morris*, 492 Mass. 498, 515 (2023) (Budd., J., concurring) (quoting *Commonwealth v. Jackson*, 370 Mass. 502, 507 (1976)). *See Curtatone v. Barstool Sports, Inc.*, 487 Mass. 655, 658 (2021) ("secret" recording under statute means that it is "concealed", and "kept hidden or unexplained" [dictionary citations omitted]).

⁵ This conclusion is also consistent with the result reached in *Doe v. Partners Healthcare System, Inc.*, 1984CV01651-BLS1, endorsement denying motion to dismiss (Super. Ct. Dec. 7, 2020).

The Privacy Notice here does not prove, as a matter of law, the existence of Plaintiff's actual or constructive knowledge. First, the notice is not alleged to be a prominent disclaimer that requires acknowledgment before website use is allowed. Thus, it is doubtful Plaintiff or other users read it or knew about it before interacting with the Boston Children's website. Second, even if Plaintiff had read it, it likely would not have alerted her to the interceptions alleged. The Privacy Notice's express statement that: "We do not collect personally identifiable information about individuals, except when it is knowingly provided by such individuals (e.g. web forms)" conflicts with the actual interceptions alleged — i.e., that they went far beyond the contents of web form submissions. Likewise, transmitting essentially all website interactions to third parties for advertising purposes is arguably different from collecting some data to enhance website useability. In sum, the Complaint plausibly alleges that the interceptions occurred in secret, without users' knowledge, as they interacted with the Boston Children's website.⁶

4. Hypothetical Allegations

Boston Children's argues that the Complaint fails to allege that the "contents" of a communication were intercepted because none of Plaintiff's actual interactions with the website were specified or described. Rather, the site visits the Complaint describes are all hypothetical. The Massachusetts Wiretap Statute broadly defines the "contents" of a communication to include "any information concerning *the identity of the parties to such communication* or the existence, contents, substance, purport, or meaning of that communication." G.L. c. 272, § 99(B)(5)

⁶ Boston Children's argument that Plaintiff consented to Facebook and Google monitoring through her accounts with those companies assumes facts that are not in the Complaint. Regardless, even assuming Plaintiff had so consented, fact issues nevertheless remain about Plaintiff's actual or constructive knowledge of that consent and the interceptions alleged.

(emphasis added). *See District Attorney for Plymouth Dist. v. New England Tel. & Tel. Co.*, 379 Mass. 586, 592 (1980).

The Complaint alleges that Plaintiff's children are Boston Children's patients, and that Plaintiff regularly uses the Boston Children's website, including to log into the patient portal. The Complaint also alleges that the Boston Children's website has embedded software code that intercepts users' website interactions and shares with third parties those users' identifying information, including IP addresses and unique browser configurations. Viewing the Complaint as a whole, the court accordingly may infer that during Plaintiff's regular visits to its website, Boston Children's shared her identifying information with third parties. Where the information shared is alleged to have been detailed enough that the third parties could identify a user for targeted advertising purposes, it falls within the meaning of "contents" under the statute. *See generally District Attorney for Plymouth Dist.*, 379 Mass. at 592 (telephone number considered "contents" under statute).⁷ In other words, that the Complaint includes several hypothetical website visits to explain the technology and interceptions at issue does not detract from the allegation that Plaintiff herself regularly used the website, and accordingly was subjected to analogous interceptions.

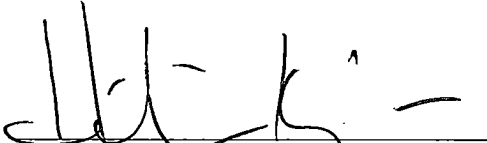
For all of these reasons, Boston Children's motion to dismiss is **DENIED**.

⁷ The federal cases Boston Children's cites are unpersuasive where the meaning of "contents" materially differs between the Federal Wiretap Statute and the Massachusetts Wiretap Statute. See 18 U.S.C.A. § 2510(8) (defining "contents" to only include "any information concerning the substance, purport, or meaning of that communication").

ORDER

For the foregoing reasons, Boston Children's motion to dismiss is **DENIED**.

Dated: September 14, 2023



Hélène Kazanjian
Justice of the Superior Court

COMMONWEALTH OF MASSACHUSETTS

ESSEX, ss.

SUPERIOR COURT
CIVIL ACTION
NO. 2277CV01000

JOHN DOE¹

vs.

EMERSON HOSPITAL

**MEMORANDUM OF DECISION AND ORDER ON
DEFENDANT’S MOTION TO DISMISS**

Plaintiff John Doe commenced this putative class action against defendant Emerson Hospital (“Emerson”), alleging that it used digital marketing tools on its website, including Facebook’s Meta Pixel, that illegally transmitted website users’ personal health information and the contents of their communications with Emerson’s website to Facebook and other third parties. Based on these allegations, the First Amended Complaint (“FAC”) asserts claims for breach of fiduciary duty, breach of implied contract, unjust enrichment, violation of the Massachusetts Wiretap Statute, G. L. c. 272, § 99, and invasion of privacy under G. L. c. 214, § 1B. Presently before the Court is Emerson’s motion to dismiss. After a hearing and consideration of the parties’ submissions, the motion is **DENIED**.

BACKGROUND

The FAC alleges the following.

At some point prior to October 2023, Emerson installed Facebook’s Meta Pixel without informing its patients.² The Meta Pixel is a snippet of software code that gathers information

¹ Individually and on behalf of all others similarly situated

² Meta Platforms, Inc. is the parent company of Facebook.

from a user when they are on a website and sends it to Facebook. If the website user is a Facebook subscriber, Facebook can use the data gathered, in conjunction with other information it collects from its subscribers, to identify the website user and target ads to them. Emerson has since removed the Meta Pixel from its website.

During the period the Meta Pixel was on the Emerson website, it recorded a user's IP address, the buttons clicked, as well as the information entered in the website's pages, including the "Find a Doctor," "Site Search," and "Request an Appointment" pages, the last of which features a questionnaire that contains information such as the doctor's name, the patient's name, telephone number, physical address, and email address. The website's "Notice of Privacy Practices" did not inform users that it was utilizing the Meta Pixel but instead promised that it would never share patient health information with marketing companies without express authorization from patients. In exchange for installing its Meta Pixel, Facebook provided Emerson with enhanced online advertising services, including retargeting (a form of online targeted advertising) and enhanced analytics functions.

Plaintiff is an individual with a Facebook account as well as an Emerson patient who received treatment at the hospital's Cantu Concussion Center. In 2022, Plaintiff used Emerson's website to transmit information about his treatment at Emerson, which included queries about treatment for a concussion. Plaintiff's communications contained information about his status as an Emerson patient, including information about his doctors, conditions, treatment, and appointments. Plaintiff was unaware that this information was being shared with Facebook through the Meta Pixel.

STANDARD OF REVIEW

Rule 12(b)(6) of the Massachusetts Rules of Civil Procedure allows for dismissal of a complaint when the factual allegations contained within it do not suggest a plausible entitlement to relief. Iannacchino v. Ford Motor Co., 451 Mass. 623, 635-636 (2008); Fraelick v. PerketPR, Inc., 83 Mass. App. Ct. 698, 699-700 (2013). In ruling on a motion to dismiss, the court accepts the factual allegations as true and draws all reasonable inferences in the non-moving party's favor. Fraelick, 83 Mass. App. Ct. at 699-700. In addition to the complaint's factual allegations, the court may consider matters of public record, orders, items appearing in the record of the case, exhibits attached to the complaint, and documents of which the plaintiff had notice and on which they relied in framing the complaint. Golchin v. Liberty Mut. Ins. Co., 460 Mass. 222, 224 (2011); Schaer v. Brandeis Univ., 432 Mass. 474, 477 (2000).

DISCUSSION

In moving to dismiss, Emerson argues that Plaintiff lacks standing to bring his common law claims and that none of his claims are adequately supported by the FAC's allegations. As explained below, the court concludes that Plaintiff's claims survive.³

A. Standing to Bring Common Law Claims

Proof of standing requires that a plaintiff "allege sufficient facts to show that he has suffered a nonspeculative, direct injury." Pugsley v. Police Dep't of Boston, 472 Mass. 367, 373 (2015). Emerson argues that Plaintiff cannot assert his claims for breach of fiduciary duty, implied contract, and unjust enrichment because he has not suffered any cognizable injury from

³ In its memorandum in support, Emerson briefly argues that the claims are preempted by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). This argument is without merit. See R.K. v. St. Mary's Med. Ctr., Inc., 229 W. Va. 712, 718 (2012) ("HIPAA does not preempt state-law causes of action for the wrongful disclosure of health care information."); Hidalgo-Semlek v. Hansa Med., Inc., 498 F. Supp. 3d 236, 258 n.40 (D.N.H. 2020) ("HIPAA provides a floor of privacy protections for a person's individually identifiable health information and does not preempt state privacy laws that provide greater protection than HIPAA.").

Emerson's alleged conduct. Specifically, Emerson argues that Plaintiff (as a Facebook user) consented to the very conduct complained of because, when he signed up for a Facebook account, he agreed to Meta's Terms of Service, Privacy Policy, and Cookie Policy ("Meta Policies").

Plaintiff's argument is unsound for two reasons. First, it depends on documents, see Wong Decl., Exs. 2-4, that the court cannot consider because it is doubtful that they were relied upon in framing the FAC. Neither Plaintiff's allegations regarding Facebook's collection and use of user data nor his passing reference to Facebook's 2009 terms of service, see FAC, ¶ 144, is sufficient for these purposes.⁴ Second, even if the court could take these documents into consideration, it is unclear how accepting the Meta Policies could constitute consent to *Emerson's* interception and disclosure of Plaintiff's private healthcare information, particularly where Emerson allegedly promised on its website never to share a patient's personal information for marketing purposes without specific authorization.⁵ Thus, at this stage of the litigation, the court cannot conclude that the Meta Policies establish consent as a matter of law such that Plaintiff suffered no injuries.

⁴ Prior to the hearing on the matter, Plaintiff moved to strike Exhibits 1-5 attached to the Declaration of Alan Y. Wong, which Emerson submitted in support of its motion to dismiss. Plaintiff did not move to strike Exhibit 6 (the Emerson Hospital Patient Privacy Policy), which is referenced in the FAC. Plaintiff argued that Exhibits 1-5 cannot be considered by the court on a motion to dismiss. In response, Emerson filed an opposition in which it argued that the motion should be denied: (1) for failure to comply with Superior Court Rule 9C; and (2) because Exhibits 1-4 are properly before the court (it agreed to strike Exhibit 5). See Docket No. 18.5. The court denied the motion for failure to comply with Rule 9C. At the hearing, the court vacated the denial but counsel for Emerson was not prepared to argue. The parties subsequently agreed that the court could rule on the motion without argument and based on the briefing alone. Accordingly, the court allows the motion to strike. Exhibits 1 (a press release) and 2-4 (the Meta Policies) are stricken for the reason stated above; it is not evident that they were relied upon by Plaintiff in framing the FAC. The Court strikes Exhibit 5 as agreed to by Emerson.

⁵ Emerson argues that this purported promise only concerned the use of medical and treatment records, which are not at issue here. However, the relevant section on Emerson's website promises not to share "health information" without authorization. See Wong Decl., Ex. 6. At this stage, it is unclear whether a user of the website would read the phrase "health information" so narrowly.

To the extent that Emerson otherwise argues that Plaintiff fails to allege cognizable harm, the court concludes that this is not the case. Plaintiff alleges he was injured because his private medical information was disclosed to Facebook without his consent, FAC, ¶¶ 85-104, and because Emerson and Facebook monetized his personal health information without compensating him. FAC, ¶¶ 128-140, 257-264. Drawing every reasonable inference in Plaintiff's favor, the court concludes that these are sufficient allegations of injury to avoid dismissal.⁶

B. Breach of Fiduciary Duty

To assert a claim for breach of fiduciary duty, a plaintiff must allege “(1) the existence of a fiduciary duty; (2) breach of that duty; (3) damages; and (4) a causal connection between breach of the duty and the damages.” Baker v. Wilmer Cutler Pickering Hale & Dorr LLP, 91 Mass. App. Ct. 835, 842 (2017). “A fiduciary duty exists when one reposes faith, confidence, and trust in another’s judgment and advice.” Doe v. Harbor Sch., Inc., 446 Mass. 245, 252 (2006) (internal quotes omitted).

Emerson argues that the FAC fails to allege plausibly that a fiduciary duty exists between Emerson and Plaintiff because it does not make clear whether Plaintiff’s communications with Emerson’s website related to any treatment at the hospital or even if he had a physician-patient relationship at the time of his visit. The court does not agree. Plaintiff alleges that Emerson “disclosed information relating to Plaintiff and Class Members’ medical treatment to third parties without their knowledge, consent, or authorization,” and “[t]he information disclosed included . .

⁶ At the hearing, Emerson heavily relied on Dinerstein v. Google, LLC, 73 F.4th 502, 516-518 (7th Cir. 2023) in arguing that Plaintiff lacked standing. However, the case contains many distinguishing facts, including that the plaintiff there expressly consented to the use of his medical information. Moreover, it is unclear whether our appellate courts would adopt many of the views expressed therein. Emerson has failed to cite to any case in the Commonwealth supporting its argument, suggesting this issue is better assessed on a fuller record.

. Plaintiff and Class Members' statuses as *patients* of Defendant, and the exact contents of communications exchanged between Plaintiff and/or Class Members with Defendant, including but not limited to information about treating doctors, potential doctors, conditions, *treatments*, appointments, search terms, bill payment, and logins to Defendant's website." FAC, ¶¶ 203–204 (emphasis added). See also *id.* at ¶ 103 ("The information that Plaintiff John Doe transmitted included queries about treatment for his concussion."); ¶ 11 (Plaintiff "is a patient of Defendant who has received treatment at Defendant at Cantu Concession Center").

Emerson alternatively argues that a fiduciary relationship cannot exist between a health system (as opposed to a specific doctor) and a patient. However, the cases from the Commonwealth it cites for this proposition are not directly on point. See Petrell v. Rakoczy, 2005 WL 1683600, at *4 (Mass. Super. July 11, 2005); Van Brode Grp., Inc. v. Bowditch & Dewey, 36 Mass. App. Ct. 509, 516 (1994).⁷ Moreover, "the determination of whether a fiduciary duty exists is largely fact specific," Baker, 91 Mass. App. Ct. at 846, and therefore such an argument is best addressed on a more complete record. See Shedd v. Sturdy Mem'l Hosp., Inc., No. 2173CV00498C, 2022 WL 1102524, at *9 (Mass. Super. Apr. 5, 2022) (Squires-Lee, J.) (on motion to dismiss in data breach case against hospital, rejecting argument that fiduciary duty did not exist given fact intensive nature of that determination).⁸

C. Implied Contract

⁷ Emerson also cites two cases from other jurisdictions in its Reply and Notice of Supplemental Authority. See Kurowski v. Rush Sys. for Health, 2023 WL 2349606 (N.D. Ill. Mar. 3, 2023); Cousin v. Sharp Healthcare, No. 22-CV-2040-MMA (DDL), 2023 WL 4484441, at *4-5, *10 (S.D. Cal. July 12, 2023). The Court is not persuaded by these decisions at this stage of the litigation.

⁸ The Court notes that at least two trial court decisions have indicated that a pharmacy may owe its customers a fiduciary duty, which suggests Emerson's position is not correct. See Kelley v. CVS Pharmacy, Inc., No. CIV. A. 98-0897-BLS2, 2007 WL 2781163, at *5-6 (Mass. Super. Aug. 24, 2007) (Gants, J.); Weld v. CVS Pharmacy, Inc., No. CIV. A. 98-0897F, 1999 WL 494114, at *5 (Mass. Super. June 29, 1999) (Fremont-Smith, J.) (same).

“In the absence of an express agreement, an implied contract may be inferred from (1) the conduct of the parties and (2) the relationship of the parties.” T.F. v. B.L., 442 Mass. 522, 526–527 (2004). To prove the existence of an implied contract, a plaintiff must show that “there was a benefit to the defendant, that the plaintiff expected the defendant to pay for that benefit, and that the defendant expected, or a reasonable person should have expected, that he or she would have to pay for that benefit.” Id. at 527. Emerson argues that the claim fails because the FAC does not allege a meeting of the minds or that there was any consideration for the purported implied contract. The court concludes that drawing every reasonable inference in favor of Plaintiff, the FAC plausibly alleges the existence of an implied contract, including the element of consideration.

In the FAC, Plaintiff alleges the following. See FAC, ¶¶ 223-256. Through their course of conduct, Emerson and Plaintiff entered into an implied contract for the provision of medical care and treatment, which included an implied agreement for Emerson to retain and protect, as part of the physician-patient relationship, the privacy of Plaintiff’s health information. A portion of the price of each payment that Plaintiff made to Emerson for medical services was intended to ensure the confidentiality of his health information. The implied promise was evidenced by Emerson’s privacy policies, codes of conduct, company security practices, and other conduct, including the statement on its website that it would not share health information for advertising purposes without consent.

Although Emerson has cited case law from other jurisdictions indicating that such an implied contract claim is not viable, other case law suggests that, at least at the motion to dismiss stage, the claim should be permitted to proceed. See Doe v. Regents of Univ. of California, No. 23-CV-00598-WHO, 2023 WL 3316766, at *6-7 (N.D. Cal. May 8, 2023) (in case involving

defendant's use of the Meta Pixel, concluding that it was plausible that the parties entered into an implied contract by their actions); Shedd, 2022 WL 1102524, at *9-10 (in data breach case, denying motion to dismiss implied contract claim); Rudolph v. Hudson's Bay Co., No. 18-CV-8472 (PKC), 2019 WL 2023713, at *10-11 (S.D.N.Y. May 7, 2019) (same); Castillo v. Seagate Tech., LLC, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016) (same).⁹ In light of these decisions and the absence of case law from the Commonwealth clearly on point, the court concludes that the better course is to assess this claim on a fuller record. The allegations sufficiently suggest that Emerson may have entered into an implied contract which included an agreement not to disclose health information to third parties, like Facebook, without consent.¹⁰

D. Unjust Enrichment

"In order to recover for unjust enrichment, a plaintiff must prove that (1) it conferred a measurable benefit upon the defendant; (2) it reasonably expected compensation from the defendant; and (3) the defendant accepted the benefit with the knowledge, actual or chargeable, of the plaintiff's reasonable expectation." See Stewart Title Guar. Co. v. Kelly, 97 Mass. App. Ct. 325, 335 (2020). "Unjust enrichment, as a basis for restitution, requires more than benefit. The benefit must be *unjust*, a quality that turns on the reasonable expectations of the parties." Santagate v. Tower, 64 Mass. App. Ct. 324, 336 (2005), quoting Community Builders, Inc. v. Indian Motorcycle Assocs., 44 Mass. App. Ct. 537, 560 (1998) (emphasis in original).

⁹ The Court acknowledges that, as Emerson argues, these data breach decisions are not entirely analogous to the situation presented here.

¹⁰ At the hearing, Emerson contended that the claim fails because it is based on Emerson's HIPAA obligations and there can be no consideration for doing what the law requires. At this stage of the litigation, the Court is not persuaded by this argument.

Emerson argues that the unjust enrichment claim must be dismissed because Plaintiff has failed to allege adequately that he conferred a measurable benefit upon Emerson or that Emerson's use of the Meta Pixel was unjust. These arguments are unavailing.

Plaintiff alleges that he conferred a benefit on Emerson in the form of his health information, which, given its confidential nature, has significant value in the marketplace. FAC, ¶¶ 260, 128-135. Plaintiff also alleges that he provided his health information to Emerson with the expectation that Emerson would protect it, that Emerson's website promised not to share health information for marketing purposes without authorization, but that Emerson used the information in return for advertising benefits. *Id.* at ¶¶ 104-111, 136, 239, 260-261. Plaintiff further alleges that part of the payment for his medical services was intended to compensate for Emerson's protection of his health information. *Id.* at ¶¶ 194, 231. These allegations plausibly suggest that Emerson retained a measurable benefit and that the retention of that benefit was unjust.¹¹

E. Invasion of Privacy

An invasion of privacy claim under G. L. c. 214, § 1B may be based either on the public disclosure of private facts or an intrusion upon a plaintiff's solitude or seclusion, i.e., an infringement upon the right to be left alone. *Polay v. McMahan*, 468 Mass. 379, 382 (2014). In either case, a plaintiff must put forward allegations plausibly suggesting that the invasion is both unreasonable and substantial or serious. *Id.* In determining whether a violation occurred, the court should consider "the location of the intrusion, the means used, the frequency and duration of the intrusion, and the underlying purpose behind the intrusion" while balancing the extent of

¹¹ Emerson makes two additional arguments. First, it suggests that the claim fails because Plaintiff had no reasonable expectation of compensation. Second, it argues that Emerson reasonably understood Plaintiff's payments to be for healthcare services. The parties' reasonable expectations are a disputed fact issue inappropriate for resolution on a motion to dismiss.

any intrusion “against any legitimate purpose” therefor. *Id.* at 383. Typically, whether an intrusion is unreasonable, substantial, or serious is a question of fact. *Id.*

Emerson argues that the claim fails because the FAC reveals little about the information that Plaintiff entered on its website and fails to identify how the data, once sent to Facebook, was used. The court is not persuaded. Plaintiff alleges that in order to obtain advertising benefits, Emerson disclosed information relating to Plaintiff’s medical treatment to third parties without his knowledge, consent, or authorization, including information about Plaintiff’s status as an Emerson patient, and the exact content of communications exchanged between Plaintiff and Emerson (e.g., information about treating doctors, potential doctors, conditions, treatments, appointments, search terms, bill payment). These allegations suffice to advance Plaintiff’s claim for invasion of privacy. See generally *Ayash v. Dana-Farber Cancer Inst.*, 443 Mass. 367, 383 (2005) (“statute . . . proscribes disclosure of facts about an individual that are of a highly personal or intimate nature when there exists no legitimate countervailing interest”) (internal quotes omitted). See also *Doe v. Boston Med. Ctr. Corp.*, No. 2384CV00326-BLS-1, 2023 WL 7105628, at *5 (Mass. Super. Sep. 14, 2023) (Kazanjian, J.) (declining to dismiss invasion of privacy claim based on similar allegations).¹²

F. Wiretap Claim

General Laws c. 272, § 99(Q) provides a cause of action for “[a]ny aggrieved person whose oral or wire communications were intercepted, disclosed or used . . . or whose personal or property interests or privacy were violated by means of an interception,” except as permitted or authorized by the Wiretap Statute. “Interception” is defined to mean “to secretly hear, secretly

¹² At the hearing, Emerson suggested that this decision is distinguishable because the plaintiff allegedly used a patient portal, which is not the alleged here. The Court does not read the decision and other recent decisions from this Court on the same subject as limited to interactions with patient portals.

record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication[.]” G. L. c. 272, § 99(B)(4).

Emerson argues that the claim fails because the FAC (1) fails to allege that it used an intercepting device; and (2) Plaintiff consented to Facebook’s tracking of his off-Facebook activities and, therefore, Emerson did not secretly record his communications. These arguments are without merit.

The first argument has been rejected in other recent Superior Court decisions analyzing similar allegations and the court sees no reason to diverge from those rulings. See, e.g., Doe, 2023 WL 7105628, at *4.

The second argument fails for two reasons. First, as noted above, the Meta Policies relied upon by Emerson are not properly considered by the court on a motion to dismiss. Second, even if the court could consider them, it would not conclude that the policies demonstrate consent as a matter of law. To establish that an interception is not secret for purposes of the Wiretap Statute, a defendant must show that the plaintiff had “actual [or constructive] knowledge” of the interception, which is proved through “clear and unequivocal objective manifestations of knowledge” either through statements or conduct. Commonwealth v. Morris, 492 Mass. 498, 515 (2023) (Budd. , J., concurring), quoting Commonwealth v. Jackson, 370 Mass. 502, 507 (1976). See Curtatone v. Barstool Sports, Inc., 487 Mass. 655, 658 (2021) (“secret” recording under statute means that it is “concealed”, and “kept hidden or unexplained” [dictionary citations omitted]). It is not at all clear how Plaintiff’s purported acceptance of *Facebook’s* policies could constitute actual or constructive knowledge that *Emerson* was intercepting Plaintiff’s communications, particularly where Emerson’s website promised not to share patient’s personal

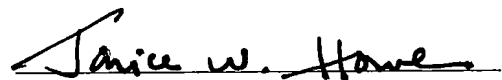
information for marketing purposes without specific authorization and the Meta Policies do not disclose that the Meta Pixel had been installed on the Emerson website.

In so ruling, the Court notes that two recent Superior Court cases involving similar wiretap claims were reported to the Appeals Court under Mass. R. Civ. P. 64, seeking clarification on a motion to dismiss as to whether the Wiretap Statute applies to the internet tracking alleged. See Vita v. New England Baptist Hosp., 2384CV00857 (Kazanjian, J.); Vita v. Beth Israel Deaconess Med. Ctr., Inc., 2384CV00480 (Kazanjian, J.). Depending on the outcome of the appellate review, the court's ruling here may have to be revisited.

ORDER

Defendant's motion to dismiss is **DENIED.**

SO ORDERED.



Janice W. Howe
Justice of the Superior Court

Date: November 22, 2023

10.23

NOTIFY

11/25

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT DEPARTMENT
CIVIL ACTION NO. 1984CV01651-BLS1

NOTICE SENT
12.07.20

H.K.
C.A.M.
C.M.I.
M.T.M.
K.B.

K.F.C.
J.M.C.

S.H.C.
F.S.J.

T.A.V.T.

MA

MICHAEL JOSEPH DONOVAN
CLERK / MAGISTRATE

1 2019 OCT 18 P 2:44

SUFFOLK SUPERIOR COURT
CIVIL CLERK'S OFFICE

JOHN DOE AND JANE DOE,
INDIVIDUALLY AND ON BEHALF OF
ALL OTHERS SIMILARLY SITUATED,

Plaintiffs,

v.

PARTNERS HEALTHCARE SYSTEM, INC.,
THE GENERAL HOSPITAL
CORPORATION D/B/A MASSACHUSETTS
GENERAL HOSPITAL, BRIGHAM,
HEALTH INC., DANA-FARBER CANCER
INSTITUTE, INC., DANA-FARBER/
PARTNERS CANCER CARE, INC., AND
DANA-FARBER, INC.,

Defendants.

DEFENDANTS' MOTION TO DISMISS THE FIRST AMENDED COMPLAINT

Defendants Partners Healthcare System, Inc. ("Partners"), The General Hospital Corporation ("Massachusetts General Hospital" or "MGH"), Brigham Health, Inc. ("Brigham and Women's Hospital" or "BWH"), Dana-Farber Cancer Institute, Inc. ("Dana-Farber" or "DFCI"), Dana-Farber, Inc., and Dana-Farber/Partners Cancer Care, Inc. (collectively, "the Hospitals"),¹ through their undersigned counsel, move under Massachusetts Rule of Civil Procedure 12(b)(6) to dismiss this case in its entirety for failure to state a claim upon which relief can be granted. As grounds for this motion, the Hospitals state as follows:

¹ Defendants contend that the Complaint misnames Dana-Farber/Partners Cancer Care, Inc. and Dana-Farber, Inc. as parties in this case.

③ core mission, and, "In most circumstances, a charitable institution will not be engaged in trade or commerce when it undertakes activities in furtherance of its core mission." Linkage Corp. v. Trustees of Boston Univ., 425 Mass. 1, 26 (1997).

② 11/20/20

① After a virtual hearing, this motion is allowed in part. The motion is denied as to Counts I and II of the Plaintiff's First Amended Complaint. The reasons stated on the record at the hearing. The motion also is denied as to Count III of the Complaint alleging breach of fiduciary duty. The Massachusetts Supreme Judicial Court has held that a physician has a "fiduciary obligation to hold in trust confidential information of his or her patient." Alberty v. Devine, 395 Mass. 159, 69 (1983). See also Forper v. Weinstein, 57 Mass. App. Ct. 433, (cont. below).

11/25 ✓
An individual's duty to maintain the confidentiality of a plaintiff's medical records. An individual who is a member, officer, or director of an organization of which he or she is a member, officer, or director is also an officer of the organization of which he or she is a member, officer, or director. Bohner v. Wilmer, 2019 Mass. App. Ct. 855, 847 (2019) (L10) (L11) (L12) (L13) (L14) (L15) (L16) (L17) (L18) (L19) (L20) (L21) (L22) (L23) (L24) (L25) (L26) (L27) (L28) (L29) (L30) (L31) (L32) (L33) (L34) (L35) (L36) (L37) (L38) (L39) (L40) (L41) (L42) (L43) (L44) (L45) (L46) (L47) (L48) (L49) (L50) (L51) (L52) (L53) (L54) (L55) (L56) (L57) (L58) (L59) (L60) (L61) (L62) (L63) (L64) (L65) (L66) (L67) (L68) (L69) (L70) (L71) (L72) (L73) (L74) (L75) (L76) (L77) (L78) (L79) (L80) (L81) (L82) (L83) (L84) (L85) (L86) (L87) (L88) (L89) (L90) (L91) (L92) (L93) (L94) (L95) (L96) (L97) (L98) (L99) (L100) (L101) (L102) (L103) (L104) (L105) (L106) (L107) (L108) (L109) (L110) (L111) (L112) (L113) (L114) (L115) (L116) (L117) (L118) (L119) (L120) (L121) (L122) (L123) (L124) (L125) (L126) (L127) (L128) (L129) (L130) (L131) (L132) (L133) (L134) (L135) (L136) (L137) (L138) (L139) (L140) (L141) (L142) (L143) (L144) (L145) (L146) (L147) (L148) (L149) (L150) (L151) (L152) (L153) (L154) (L155) (L156) (L157) (L158) (L159) (L160) (L161) (L162) (L163) (L164) (L165) (L166) (L167) (L168) (L169) (L170) (L171) (L172) (L173) (L174) (L175) (L176) (L177) (L178) (L179) (L180) (L181) (L182) (L183) (L184) (L185) (L186) (L187) (L188) (L189) (L190) (L191) (L192) (L193) (L194) (L195) (L196) (L197) (L198) (L199) (L200) (L201) (L202) (L203) (L204) (L205) (L206) (L207) (L208) (L209) (L210) (L211) (L212) (L213) (L214) (L215) (L216) (L217) (L218) (L219) (L220) (L221) (L222) (L223) (L224) (L225) (L226) (L227) (L228) (L229) (L230) (L231) (L232) (L233) (L234) (L235) (L236) (L237) (L238) (L239) (L240) (L241) (L242) (L243) (L244) (L245) (L246) (L247) (L248) (L249) (L250) (L251) (L252) (L253) (L254) (L255) (L256) (L257) (L258) (L259) (L260) (L261) (L262) (L263) (L264) (L265) (L266) (L267) (L268) (L269) (L270) (L271) (L272) (L273) (L274) (L275) (L276) (L277) (L278) (L279) (L280) (L281) (L282) (L283) (L284) (L285) (L286) (L287) (L288) (L289) (L290) (L291) (L292) (L293) (L294) (L295) (L296) (L297) (L298) (L299) (L300) (L301) (L302) (L303) (L304) (L305) (L306) (L307) (L308) (L309) (L310) (L311) (L312) (L313) (L314) (L315) (L316) (L317) (L318) (L319) (L320) (L321) (L322) (L323) (L324) (L325) (L326) (L327) (L328) (L329) (L330) (L331) (L332) (L333) (L334) (L335) (L336) (L337) (L338) (L339) (L340) (L341) (L342) (L343) (L344) (L345) (L346) (L347) (L348) (L349) (L350) (L351) (L352) (L353) (L354) (L355) (L356) (L357) (L358) (L359) (L360) (L361) (L362) (L363) (L364) (L365) (L366) (L367) (L368) (L369) (L370) (L371) (L372) (L373) (L374) (L375) (L376) (L377) (L378) (L379) (L380) (L381) (L382) (L383) (L384) (L385) (L386) (L387) (L388) (L389) (L390) (L391) (L392) (L393) (L394) (L395) (L396) (L397) (L398) (L399) (L400) (L401) (L402) (L403) (L404) (L405) (L406) (L407) (L408) (L409) (L410) (L411) (L412) (L413) (L414) (L415) (L416) (L417) (L418) (L419) (L420) (L421) (L422) (L423) (L424) (L425) (L426) (L427) (L428) (L429) (L430) (L431) (L432) (L433) (L434) (L435) (L436) (L437) (L438) (L439) (L440) (L441) (L442) (L443) (L444) (L445) (L446) (L447) (L448) (L449) (L450) (L451) (L452) (L453) (L454) (L455) (L456) (L457) (L458) (L459) (L460) (L461) (L462) (L463) (L464) (L465) (L466) (L467) (L468) (L469) (L470) (L471) (L472) (L473) (L474) (L475) (L476) (L477) (L478) (L479) (L480) (L481) (L482) (L483) (L484) (L485) (L486) (L487) (L488) (L489) (L490) (L491) (L492) (L493) (L494) (L495) (L496) (L497) (L498) (L499) (L500) (L501) (L502) (L503) (L504) (L505) (L506) (L507) (L508) (L509) (L510) (L511) (L512) (L513) (L514) (L515) (L516) (L517) (L518) (L519) (L520) (L521) (L522) (L523) (L524) (L525) (L526) (L527) (L528) (L529) (L530) (L531) (L532) (L533) (L534) (L535) (L536) (L537) (L538) (L539) (L540) (L541) (L542) (L543) (L544) (L545) (L546) (L547) (L548) (L549) (L550) (L551) (L552) (L553) (L554) (L555) (L556) (L557) (L558) (L559) (L560) (L561) (L562) (L563) (L564) (L565) (L566) (L567) (L568) (L569) (L570) (L571) (L572) (L573) (L574) (L575) (L576) (L577) (L578) (L579) (L580) (L581) (L582) (L583) (L584) (L585) (L586) (L587) (L588) (L589) (L590) (L591) (L592) (L593) (L594) (L595) (L596) (L597) (L598) (L599) (L600) (L601) (L602) (L603) (L604) (L605) (L606) (L607) (L608) (L609) (L610) (L611) (L612) (L613) (L614) (L615) (L616) (L617) (L618) (L619) (L620) (L621) (L622) (L623) (L624) (L625) (L626) (L627) (L628) (L629) (L630) (L631) (L632) (L633) (L634) (L635) (L636) (L637) (L638) (L639) (L640) (L641) (L642) (L643) (L644) (L645) (L646) (L647) (L648) (L649) (L650) (L651) (L652) (L653) (L654) (L655) (L656) (L657) (L658) (L659) (L660) (L661) (L662) (L663) (L664) (L665) (L666) (L667) (L668) (L669) (L670) (L671) (L672) (L673) (L674) (L675) (L676) (L677) (L678) (L679) (L680) (L681) (L682) (L683) (L684) (L685) (L686) (L687) (L688) (L689) (L690) (L691) (L692) (L693) (L694) (L695) (L696) (L697) (L698) (L699) (L700) (L701) (L702) (L703) (L704) (L705) (L706) (L707) (L708) (L709) (L710) (L711) (L712) (L713) (L714) (L715) (L716) (L717) (L718) (L719) (L720) (L721) (L722) (L723) (L724) (L725) (L726) (L727) (L728) (L729) (L730) (L731) (L732) (L733) (L734) (L735) (L736) (L737) (L738) (L739) (L740) (L741) (L742) (L743) (L744) (L745) (L746) (L747) (L748) (L749) (L750) (L751) (L752) (L753) (L754) (L755) (L756) (L757) (L758) (L759) (L760) (L761) (L762) (L763) (L764) (L765) (L766) (L767) (L768) (L769) (L770) (L771) (L772) (L773) (L774) (L775) (L776) (L777) (L778) (L779) (L780) (L781) (L782) (L783) (L784) (L785) (L786) (L787) (L788) (L789) (L790) (L791) (L792) (L793) (L794) (L795) (L796) (L797) (L798) (L799) (L800) (L801) (L802) (L803) (L804) (L805) (L806) (L807) (L808) (L809) (L810) (L811) (L812) (L813) (L814) (L815) (L816) (L817) (L818) (L819) (L820) (L821) (L822) (L823) (L824) (L825) (L826) (L827) (L828) (L829) (L830) (L831) (L832) (L833) (L834) (L835) (L836) (L837) (L838) (L839) (L840) (L841) (L842) (L843) (L844) (L845) (L846) (L847) (L848) (L849) (L850) (L851) (L852) (L853) (L854) (L855) (L856) (L857) (L858) (L859) (L860) (L861) (L862) (L863) (L864) (L865) (L866) (L867) (L868) (L869) (L870) (L871) (L872) (L873) (L874) (L875) (L876) (L877) (L878) (L879) (L880) (L881) (L882) (L883) (L884) (L885) (L886) (L887) (L888) (L889) (L890) (L891) (L892) (L893) (L894) (L895) (L896) (L897) (L898) (L899) (L900) (L901) (L902) (L903) (L904) (L905) (L906) (L907) (L908) (L909) (L910) (L911) (L912) (L913) (L914) (L915) (L916) (L917) (L918) (L919) (L920) (L921) (L922) (L923) (L924) (L925) (L926) (L927) (L928) (L929) (L930) (L931) (L932) (L933) (L934) (L935) (L936) (L937) (L938) (L939) (L940) (L941) (L942) (L943) (L944) (L945) (L946) (L947) (L948) (L949) (L950) (L951) (L952) (L953) (L954) (L955) (L956) (L957) (L958) (L959) (L960) (L961) (L962) (L963) (L964) (L965) (L966) (L967) (L968) (L969) (L970) (L971) (L972) (L973) (L974) (L975) (L976) (L977) (L978) (L979) (L980) (L981) (L982) (L983) (L984) (L985) (L986) (L987) (L988) (L989) (L990) (L991) (L992) (L993) (L994) (L995) (L996) (L997) (L998) (L999) (L1000) (L1001) (L1002) (L1003) (L1004) (L1005) (L1006) (L1007) (L1008) (L1009) (L1010) (L1011) (L1012) (L1013) (L1014) (L1015) (L1016) (L1017) (L1018) (L1019) (L1020) (L1021) (L1022) (L1023) (L1024) (L1025) (L1026) (L1027) (L1028) (L1029) (L1030) (L1031) (L1032) (L1033) (L1034) (L1035) (L1036) (L1037) (L1038) (L1039) (L1040) (L1041) (L1042) (L1043) (L1044) (L1045) (L1046) (L1047) (L1048) (L1049) (L1050) (L1051) (L1052) (L1053) (L1054) (L1055) (L1056) (L1057) (L1058) (L1059) (L1060) (L1061) (L1062) (L1063) (L1064) (L1065) (L1066) (L1067) (L1068) (L1069) (L1070) (L1071) (L1072) (L1073) (L1074) (L1075) (L1076) (L1077) (L1078) (L1079) (L1080) (L1081) (L1082) (L1083) (L1084) (L1085) (L1086) (L1087) (L1088) (L1089) (L1090) (L1091) (L1092) (L1093) (L1094) (L1095) (L1096) (L1097) (L1098) (L1099) (L1100) (L1101) (L1102) (L1103) (L1104) (L1105) (L1106) (L1107) (L1108) (L1109) (L1110) (L1111) (L1112) (L1113) (L1114) (L1115) (L1116) (L1117) (L1118) (L1119) (L1120) (L1121) (L1122) (L1123) (L1124) (L1125) (L1126) (L1127) (L1128) (L1129) (L1130) (L1131) (L1132) (L1133) (L1134) (L1135) (L1136) (L1137) (L1138) (L1139) (L1140) (L1141) (L1142) (L1143) (L1144) (L1145) (L1146) (L1147) (L1148) (L1149) (L1150) (L1151) (L1152) (L1153) (L1154) (L1155) (L1156) (L1157) (L1158) (L1159) (L1160) (L1161) (L1162) (L1163) (L1164) (L1165) (L1166) (L1167) (L1168) (L1169) (L1170) (L1171) (L1172) (L1173) (L1174) (L1175) (L1176) (L1177) (L1178) (L1179) (L1180) (L1181) (L1182) (L1183) (L1184) (L1185) (L1186) (L1187) (L1188) (L1189) (L1190) (L1191) (L1192) (L1193) (L1194) (L1195) (L1196) (L1197) (L1198) (L1199) (L1200) (L1201) (L1202) (L1203) (L1204) (L1205) (L1206) (L1207) (L1208) (L1209) (L1210) (L1211) (L1212) (L1213) (L1214) (L1215) (L1216) (L1217) (L1218) (L1219) (L1220) (L1221) (L1222) (L1223) (L1224) (L1225) (L1226) (L1227) (L1228) (L1229) (L1230) (L1231) (L1232) (L1233) (L1234) (L1235) (L1236) (L1237) (L1238) (L1239) (L1240) (L1241) (L1242) (L1243) (L1244) (L1245) (L1246) (L1247) (L1248) (L1249) (L1250) (L1251) (L1252) (L1253) (L1254) (L1255) (L1256) (L1257) (L1258) (L1259) (L1260) (L1261) (L1262) (L1263) (L1264) (L1265) (L1266) (L1267) (L1268) (L1269) (L1270) (L1271) (L1272) (L1273) (L1274) (L1275) (L1276) (L1277) (L1278) (L1279) (L1280) (L1281) (L1282) (L1283) (L1284) (L1285) (L1286) (L1287) (L1288) (L1289) (L1290) (L1291) (L1292) (L1293) (L1294) (L1295) (L1296) (L1297) (L1298) (L1299) (L1300) (L1301) (L1302) (L1303) (L1304) (L1305) (L1306) (L1307) (L1308) (L1309) (L1310) (L1311) (L1312) (L1313) (L1314) (L1315) (L1316) (L1317) (L1318) (L1319) (L1320) (L1321) (L1322) (L1323) (L1324) (L1325) (L1326) (L1327) (L1328) (L1329) (L1330) (L1331) (L1332) (L1333) (L1334) (L1335) (L1336) (L1337) (L1338) (L1339) (L1340) (L1341) (L1342) (L1343) (L1344) (L1345) (L1346) (L1347) (L1348) (L1349) (L1350) (L1351) (L1352) (L1353) (L1354) (L1355) (L1356) (L1357) (L1358) (L1359) (L1360) (L1361) (L1362) (L1363) (L1364) (L1365) (L1366) (L1367) (L1368) (L1369) (L1370) (L1371) (L1372) (L1373) (L1374) (L1375) (L1376) (L1377) (L1378) (L1379) (L1380) (L1381) (L1382) (L1383) (L1384) (L1385) (L1386) (L1387) (L1388) (L1389) (L1390) (L1391) (L1392) (L1393) (L1394) (L1395) (L1396) (L1397) (L1398) (L1399) (L1400) (L1401) (L1402) (L1403) (L1404) (L1405) (L1406) (L1407) (L1408) (L1409) (L1410) (L1411) (L1412) (L1413) (L1414) (L1415) (L1416) (L1417) (L1418) (L1419) (L1420) (L1421) (L1422) (L1423) (L1424) (L1425) (L1426) (L1427) (L1428) (L1429) (L1430) (L1431) (L1432) (L1433) (L1434) (L1435) (L1436) (L1437) (L1438) (L1439) (L1440) (L1441) (L1442) (L1443) (L1444) (L1445) (L1446) (L1447) (L1448) (L1449) (L1450) (L1451) (L1452) (L1453) (L1454) (L1455) (L1456) (L1457) (L1458) (L1459) (L1460) (L1461) (L1462) (L1463) (L1464) (L1465) (L1466) (L1467) (L1468) (L1469) (L1470) (L1471) (L1472) (L1473) (L1474) (L1475) (L1476) (L1477) (L1478) (L1479) (L1480) (L1481) (L1482) (L1483) (L1484) (L1485) (L1486) (L1487) (L1488) (L1489) (L1490) (L1491) (L1492) (L1493) (L1494) (L1495) (L1496) (L1497) (L1498) (L1499) (L1500) (L1501) (L1502) (L1503) (L1504) (L1505) (L1506) (L1507) (L1508) (L1509) (L1510) (L1511) (L1512) (L1513) (L1514) (L1515) (L1516) (L1517) (L1518) (L1519) (L1520) (L1521) (L1522) (L1523) (L1524) (L1525) (L1526) (L1527) (L1528) (L1529) (L1530) (L1531) (L1532) (L1533) (L1534) (L1535) (L1536) (L1537) (L1538) (L1539) (L1540) (L1541) (L1542) (L1543) (L1544) (L1545) (L1546) (L1547) (L1548) (L1549) (L1550) (L1551) (L1552) (L1553) (L1554) (L1555) (L1556) (L1557) (L1558) (L1559) (L1560) (L1561) (L1562) (L1563) (L1564) (L1565) (L1566) (L1567) (L1568) (L1569) (L1570) (L1571) (L1572) (L1573) (L1574) (L1575) (L1576) (L1577) (L1578) (L1579) (L1580) (L1581) (L1582) (L1583) (L1584) (L1585) (L1586) (L1587) (L1588) (L1589) (L1590) (L1591) (L1592) (L1593) (L1594) (L1595) (L1596) (L1597) (L1598) (L1599) (L1600) (L1601) (L1602) (L1603) (L1604) (L1605) (L1606) (L1607) (L1608) (L1609) (L1610) (L1611) (L1612) (L1613) (L1614) (L1615) (L1616) (L1617) (L1618) (L1619) (L1620) (L1621) (L1622) (L1623) (L1624) (L1625) (L1626) (L1627) (L1628) (L1629) (L1630) (L1631) (L1632) (L1633) (L1634) (L1635) (L1636) (L1637) (L1638) (L1639) (L1640) (L1641) (L1642) (L1643) (L1644) (L1645) (L1646) (L1647) (L1648) (L1649) (L1650) (L1651) (L1652) (L1653) (L1654) (L1655) (L1656) (L1657) (L1658) (L1659) (L1660) (L1661) (L1662) (L1663) (L1664) (L1665) (L1666) (L1667) (L1668) (L1669) (L1670) (L1671) (L1672) (L1673) (L1674) (L1675) (L1676) (L1677) (L1678) (L1679) (L1680) (

1. In their First Amended Complaint, Plaintiffs attempt to allege claims individually and on behalf of the unsubstantiated Class and Subclasses against the Hospitals for: interception of wire communications in violation of G.L. c. 272, § 99 (Count I); invasion of privacy in violation of G.L. c. 214, § 1B (Count II); breach of fiduciary duty (Count III); and, unfair and deceptive business practices in violation of G.L. c. 93A, § 9 (Count IV).

2. Plaintiffs fail to allege any “secret interception” of communications that would allow them to recover under G.L. c. 272, § 99. Indeed, the actions that Plaintiffs describe in their First Amended Complaint do not amount to “interception” at all.

3. Plaintiffs’ allegations do not support an “unreasonable, substantial, or serious interference with [their] privacy,” as required to recover under G.L. c. 214, § 1B. The Hospitals’ disclosures amply rebut any idiosyncratic, unrealistic privacy expectation Plaintiffs may now claim to have had.

4. Plaintiffs do not – and cannot – establish a breach of fiduciary duty. Massachusetts law has never recognized a fiduciary duty owed by hospitals to patients.

5. Plaintiffs also fail to state a claim under G.L. c. 93A, § 9 because, among other reasons, the Hospitals are nonprofit, charitable institutions that are not engaged in “trade or commerce,” as required under the statute, and Plaintiffs’ claims fall short of showing that they have suffered any legally cognizable injury.

For the foregoing reasons, explained in detail in the accompanying Memorandum of Law, the Court should (A) grant this Motion, (B) dismiss all counts of the First Amended Complaint with prejudice and without leave to amend, (C) award the Hospitals costs and reasonable attorney’s fees, and (D) grant such further relief as justice requires.

REQUEST FOR ORAL ARGUMENT

The Hospitals respectfully request a hearing on this Motion at the Court's earliest convenience.

PARTNERS HEALTHCARE SYSTEM, INC.,
THE GENERAL HOSPITAL
CORPORATION D/B/A MASSACHUSETTS
GENERAL HOSPITAL, BRIGHAM
HEALTH, INC., DANA-FARBER CANCER
INSTITUTE, INC., DANA-FARBER/
PARTNERS CANCER CARE, INC., AND
DANA-FARBER, INC.,

By their attorneys,



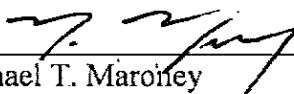
Adam J. Bookbinder (BBO No. 566590)
Michael T. Maroney (BBO No. 653476)
Holland & Knight LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700
michael.maroney@hklaw.com
adam.bookbinder@hklaw.com

Mark S. Melodia (*pro hac vice* pending)
Holland & Knight LLP
31 West 52nd Street
New York, NY 10019
(212) 513-3200
mark.melodia@hklaw.com

Dated: September 20, 2019

SUPERIOR COURT RULE 9C CERTIFICATION

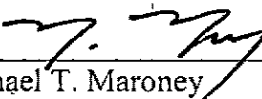
Pursuant to Mass. Sup. Ct. R. 9C(a) and (b), Adam J. Bookbinder (counsel for Defendants) and J. Michael Conley (counsel for Plaintiffs) met and conferred on August 14, 2019 by telephone. Despite good faith efforts, the parties were unable to eliminate or narrow the issues of dispute.



Michael T. Maroney

CERTIFICATE OF SERVICE

I, Michael T. Maroney, hereby certify that on September 20, 2019, I served, via email and first class mail, a copy of the foregoing document upon counsel for Plaintiffs, J. Michael Conley, 100 Grandview Road, Suite 218, Post Office Box 9139, Braintree, Massachusetts 02185, michael@kenneyconley.com.



Michael T. Maroney

Volume: I
Pages: 1-88
Exhibits: 0

SUFFOLK, SS COMMONWEALTH OF MASSACHUSETTS SUPERIOR COURT

* * * * *
* JOHN DOE, *
* * * * *
* Plaintiff, *
* * * * * No. 1984CV01651
* v. *
* * * * *
* PARTNERS HEALTHCARE SYSTEM INC*
* * * * *
* Defendant *
* * * * *

RULE 12 HEARING
BEFORE THE HONORABLE BRIAN A. DAVIS

APPEARANCES:

For the Plaintiffs, Mr. J. Michael Conley, Esquire
For the Plaintiffs, Mr. Jason Barnes, Esquire
For the Defendants, Mr. Michael Maroney, Esquire
For the Defendants, Mr. Mark Melodia, Esquire
(Full Appearance list on Page 2)

Boston, Massachusetts
November 20, 2020

(Transcript prepared from Audio Recording)
Reporter: Raymond F. Catuogno, Jr.

APPEARANCES:

For the Plaintiffs John & Jane Doe:

Kenney & Conley, P.C.
100 Grandview Road
Post Office Box 9139
Braintree, Massachusetts 02185
By: J. Michael Conley, Esquire

Simmons Hanly Conroy
One Court Street
Alton, Illinois 62002
By: Jason Barnes, Esquire

For the Defendants Partners Healthcare System Inc.; The General Hospital Corporation Doing Business as Massachusetts General Hospital; Brigham Health Inc.; Dana-Farber Cancer Institute Inc.; Dana-Farber Partners Cancer Center Inc.; Dana-Farber Inc.:

Holland & Knight LLP
10 Saint James Avenue
Boston, Massachusetts 02116
By: Michael T. Maroney, Esquire
Mark Melodia, Esquire

1 (Court in session.)

2 (2:01 p.m.)

3 THE CLERK: Good afternoon, your Honor. Calling
4 Docket No. 1984CV1651; John Doe versus Partners
5 Healthcare System Incorporated. This matter is
6 before the Court for a Rule 12 hearing.

7 Counsel, will you please state your name for the
8 record beginning with plaintiff's counsel, followed
9 by the defense counsel.

10 THE COURT: Good afternoon. You can hear me?

11 MR. BARNES: Yes, your Honor.

12 MR. CONLEY: Yes, your Honor. Mike Conley for
13 the plaintiffs.

14 THE COURT: Okay. Welcome.

15 Again, who's here on behalf of plaintiffs?

16 MR. CONLEY: In addition to me Mike Conley, Jay
17 Barnes is present, and -- Jay, who else is --

18 MR. BARNES: Your Honor, Eric Johnson is on the
19 phone. And Mitchell Bright is here. Mr. Bright has
20 not entered his appearance in the case. But of
21 course I want to note his presence --

22 THE COURT: Okay.

23 MR. BARNES: -- on the call.

24 THE COURT: Welcome. So who will be arguing on
25 behalf of plaintiffs?

1 MR. BARNES: I will, your Honor --

2 THE COURT: Mr. Barnes.

3 MR. BARNES: -- Jay Barnes.

4 THE COURT: Mr. Barnes. Got it.

5 All right. And who's here on behalf of
6 defendants?

7 MR. MARONEY: Good afternoon, your Honor.
8 Michael Maroney on behalf of defendants. And my
9 colleague Mr. Melodia will be arguing. I'll let him
10 introduce himself.

11 MR. MELODIA: Good afternoon, your Honor. Mark
12 Melodia from Holland and Knight on behalf of all of
13 the defendants on this motion. And I'll just note
14 that a number of my colleagues who are not
15 necessarily needed in the case but who are attending
16 arguments are in attendance; Chris Iaquinto, Teresa
17 Lahoy, Ester Clovitz, Courtney Grow and Chelsea
18 Rogan.

19 THE COURT: Mm-hm. All right.

20 MR. MELODIA: But I'll be arguing, your Honor.

21 THE COURT: Got it. So counsel, for those of you
22 who are, you know, interested but not arguing, would
23 you be kind enough to turn off your microphones and
24 your cameras. It does reduce the Hollywood Squares
25 effect for me during the course of the argument. So

1 I appreciate that. Thank you.

2 Counsel, we're here -- I think we're here
3 officially on the motion to dismiss. However, we
4 still have the motion for preliminary injunction that
5 I need to address which is -- and you should note
6 I've read all the materials on the motion to dismiss
7 and I've gone through the stack of materials that
8 were sent to me, some of which I asked for, some of
9 which I didn't necessarily ask for, with respect to
10 the preliminary injunction. So I have submissions
11 from both sides; defendant's response on the
12 preliminary order, I received the plaintiff's
13 response to preliminary order, and then I received a
14 series of letters with attachments. And I've
15 reviewed those materials.

16 So what I intend to do here today is I'd like to
17 start with the motion to dismiss. And then I --
18 don't worry, I intend to circle back on the motion
19 for the preliminary injunction.

20 So we're going to start with the motion to
21 dismiss. All right, folks, again I've read the
22 papers. So we've got four counts here that we're
23 fighting over, correct? We've got a count -- first
24 count is wiretap act, the Massachusetts Wiretap Act.
25 Then we've got the invasion of privacy claim which is

1 | also officially statutory in Mass. We've got the
2 | breach of fiduciary duty claim. And we have the 93A
3 | claim. And defendants are moving forward to dismiss
4 | all of those claims. Okay.

5 | MR. MELODIA: Correct, your Honor.

6 | THE COURT: All right. So again I've read the
7 | papers Mr. Melodia. I've -- recognizing that I've
8 | read your papers and I've reviewed the arguments, is
9 | there information that isn't in your papers that you
10 | wish to share with me or anything that you want to
11 | highlight at this point in time?

12 | MR. MELODIA: I think there are some fundamental
13 | things, your Honor, that cut across each of the
14 | counts. And I would be happy to address each of the
15 | specific counts as well. But I do recognize that the
16 | (inaudible -- indecipherable at 2:05:10) plaintiff.
17 | But let me focus on some of the fundamental reasons
18 | that really require dismissal of this case in its
19 | entirety as reflected in the first amended complaint.

20 | Is anybody else getting an echo? Perhaps --

21 | THE COURT: No.

22 | MR. MELODIA: -- somebody's not on mute.

23 | THE COURT: No. And again, and I'll give you an
24 | opportunity to speak Mr. Melodia. I am going to --
25 | if you're going to jump into all the fundamental

1 aspects, again a reminder -- so I read the papers. I
2 read the papers. And I have questions for both
3 sides. And again it's an -- and let me remind you as
4 well as you address the issues this is a motion to
5 dismiss. So I accept the factual allegations as
6 true. There seems to be some back and forth with
7 respect to voracity of some of the factual
8 allegations, but I have to accept the factual
9 allegations as true. So what we're really doing here
10 is we're testing the legal viability of the claims.
11 That's all that this proceeding is about. And I make
12 no determination at the motion to dismiss stage
13 regarding the merits of the claims, just their legal
14 viability.

15 MR. MELODIA: Yes, your Honor. And this
16 complaint is legally not viable for fundamental
17 reasons that can assume the truth of the properly
18 pled parts of the first amended complaint. And I say
19 properly pled because there are some things that this
20 court can see and take judicial notice of from the
21 websites themselves which are I think fair game on a
22 motion to dismiss under Massachusetts State case law.

23 The privacy cases always need to be about an
24 identifiable person. And here we don't have an
25 identifiable person. We have at most an (inaudible

1 -- indecipherable at 2:06:54) which as the Court
2 knows really just identifies a machine and really
3 identifies the random physical numbers that changes
4 every few months. And any one of those devices can
5 in fact be held by any number of people at any given
6 moment using it, but doesn't identify a person.

7 And similarly, even the Facebook ID and the
8 Google ID that are used to somehow identify a person,
9 even identify a patient according to plaintiff's
10 theory don't, because a web point visitor has to
11 first allow, set up their browser in a way that would
12 allow for that information to pass to Facebook and
13 Google, and would have to have a relationship with
14 Facebook and Google ahead of time with their own
15 terms and condition.

16 So I'm just talking about a privacy case needs to
17 be about identifiable people. And this one, even if
18 you take the first amended complaint as true, legally
19 and technically is not.

20 Second, successful privacy cases like the cases
21 that the plaintiff cite in this case; "Pharmatrak",
22 "Google Cookies" from the third circuit, the
23 "Nickelodeon" case in the third circuit, each and
24 every one of those cases had deception by the
25 defendant at their core. And we have no deception or

1 | secrecy here. Instead we have website privacy
2 | policies that were and are on each of these hospital
3 | websites. And each and every one of those discloses
4 | the use of cookies, and discloses (inaudible --
5 | indecipherable at 2:08:38.)

6 | Third, you need a private space to be intruded
7 | upon in some way in a privacy case. And here we have
8 | public websites, literally public websites that
9 | anybody with an internet connection anywhere in the
10 | world can access.

11 | And so I think it's important, your Honor, given
12 | that you've already mentioned the preliminary
13 | injunction motion -- I'm going to reference your
14 | Honor's order from April on that motion, there's a
15 | reference in the factual summary on page one of that
16 | order that talks about the hospital websites as
17 | providing direct portals that allow for access to
18 | health records and services. That is factually
19 | incorrect. And not because I say so or because an
20 | expert says so, but because it's obvious from the
21 | face of the websites which are specifically
22 | referenced in the first amended complaint and
23 | therefore are properly considered by the Court on a
24 | motion to dismiss. The three hospital websites
25 | referenced in the first amended complaint do not

1 | share personal and protected health information. And
2 | the only way the plaintiff's counsel confuses the
3 | issue repeatedly in the first amended complaint is by
4 | referencing information pages on each hospital
5 | website that are about the patient gateway, your
6 | Honor, about it, descriptive of it. Not --

7 | THE COURT: Pause for a moment Mr. Melodia.

8 | MR. MELODIA: -- allowing --

9 | THE COURT: So the allegation is -- pause. And
10 | here's one thing -- I apologize in advance to
11 | everyone. One thing I don't like about Zoom is it's
12 | difficult -- it's more difficult to sort of modulate
13 | the back and forth between counsel and -- between me
14 | and counsel. So I apologize if at some points in
15 | time I feel like I'm barging in. But unfortunately
16 | unless I mute you, which I think is even more
17 | offensive, I have no choice but to sort of get your
18 | attention.

19 | So what's alleged in the complaint -- and here's
20 | what I recall from our discussion around the
21 | preliminary injunction, is that it is possible -- so
22 | someone can go on what you call the informational
23 | website -- and I recognize that there's a separate
24 | patient portal. That really doesn't seem to be in
25 | dispute in this proceeding. I got that.

1 MR. MELODIA: Correct.

2 THE COURT: I think. I recognize that. So what
3 we're talking about is what the defendants refer to
4 as the informational websites. What plaintiffs
5 allege is that someone can go on the informational
6 websites. They claim -- they're representing
7 patients; existing patients, go on the informational
8 website, look at information, pull down information.
9 For example, look at the information about specific
10 medical providers, say a particular doctor at MGH or
11 the like, and that that information gets conveyed --
12 it's what's alleged, gets conveyed through Facebook
13 in such a way that Facebook can match that
14 information perhaps with its own Facebook identifier.
15 So Facebook can put together, do a, you know, one and
16 one, they can conclude that that individual who has a
17 Facebook page -- which isn't -- is not that unusual,
18 that person is cruising for for example a breast
19 cancer specialist or something for that, looking for
20 information about breast cancer on the MGH website.
21 So Facebook can say this particular person -- you
22 have someone in the waiting room with you? Would you
23 mind? Thank you. This particular person is looking
24 for information about breast cancer specialists,
25 which -- and doesn't say it for sure, but it could

1 | lead to an inference that that person has a real
2 | concern or perhaps a diagnosis of breast cancer,
3 | which would be confidential information perhaps. So
4 | that's what I understand to be the allegations. And
5 | again, it seems to me I have to take those
6 | allegations as true for purposes of the motion to
7 | dismiss.

8 | I understand that there are disputes about
9 | whether in fact that information gets conveyed or how
10 | useful it is to Facebook. But at this point in time
11 | I've got to accept the allegations if that
12 | information flows to Facebook that they can match it
13 | with an individual, and therefore that there is a
14 | disclosure of patient confidential information.

15 | Don't I have to look at it that way?

16 | MR. MELODIA: You do have to look at it in terms
17 | of taking the allegations are true, your Honor, but
18 | no, you don't have to pile supposition upon
19 | supposition, and inference and possibility upon
20 | possibility to perhaps find some probability. We're
21 | not in a, you know, (inaudible -- indecipherable at
22 | 2:13:15) state. I mean (inaudible -- indecipherable
23 | at 2:13:20) standard of pleading. And these do need
24 | to be probable allegations, and these are not.
25 | Number one, because it's not personally identifiable.

1 THE COURT: If there's one thing plaintiffs
2 didn't do in this case is under-plead, okay?

3 MR. MELODIA: Well certainly --

4 THE COURT: Actually they're not guilty of under-
5 pleading. But go ahead.

6 MR. MELODIA: -- well, in some senses that's
7 true, your Honor. It's a 111 page complaint. It's
8 over 400 paragraphs. True enough. However,
9 literally page 67 is the only page that deals with
10 the named plaintiffs in this case. So they
11 absolutely did under-plead with respect to the only
12 two people who are before this Court. And they do
13 not state anything about themselves. They don't tell
14 us about their browser settings. They don't tell us
15 whether they're Google and Facebook members. They
16 don't tell us whether they had information accessed.
17 They don't tell us whether they took privacy
18 protective measures like trying to block cookies and
19 that somehow those were overcome by something the
20 defendant did. They don't even say if they ever
21 looked at the privacy policy or the notice of privacy
22 practices; the NPP, which I want to make sure we talk
23 about, which is inapplicable to this website because
24 it only deals with protected health information as
25 required by HIPAA and OCR.

1 So we know nothing actually, notwithstanding the
2 111 pages, about the actual named plaintiffs and
3 their claims in this case. And ultimately they have
4 to stand, as this court knows, on their own two feet
5 before they can claim to represent other people with
6 similar claims.

7 But let me go back to the IP address idea that
8 somehow that identifies a person. It doesn't.

9 THE COURT: So you -- no, I get -- I picked up on
10 that argument in your papers Mr. Melodia.

11 MR. MELODIA: Okay.

12 THE COURT: So I did go back and I took a look at
13 the amended complaint because I wanted to see what
14 was -- specifically was alleged. And I look at for
15 example page 74 of the complaint which is part of the
16 Count One interception of wire communications, the
17 wiretap act claim. Paragraph 327 says "Defendants
18 engaged in and continue to engage in an interception
19 by aiding others including Facebook and Google to
20 secretly record the contents of plaintiff's and class
21 member's wire communications."

22 So that's what's alleged. And I read your
23 argument about that there isn't much meat on the bone
24 with respect to these individual plaintiffs.

25 MR. MELODIA: Okay.

1 THE COURT: Again but I look at the -- so that's
2 why I pulled the complaint to see what allegations
3 were made with respect to these individual
4 plaintiffs. And it looks like they covered their
5 bases in terms of making allegations that these
6 plaintiffs are representative with respect to at
7 least the complaints that are made in this amended
8 complaint.

9 MR. MELODIA: Yes, I was just responding to your
10 Honor's sense of volume. That the volume is mostly
11 generalized pleadings discussed in almost like a
12 white paper about the internet, as opposed to about
13 what happened to identifiable people. But I'll move
14 on --

15 THE COURT: Let me -- can I -- can we talk about
16 the claims one at a time?

17 MR. MELODIA: Sure.

18 THE COURT: So wiretap act claim, really you have
19 two arguments. One of the arguments is that it's not
20 an interception, but -- and there are various cases
21 cited, but I'm dealing with the Massachusetts statute
22 which is Chapter 272, Section 99. And that defines
23 an interception as among other things -- and I'm
24 inserting some letters in here, but aiding another to
25 secretly hear or secretly record a wire

1 | communication.

2 | And I'm going to come back to the secret piece
3 | for a second.

4 | But the Massachusetts Wiretap Act alleges -- it
5 | prohibits aiding someone else in secretly hearing or
6 | secretly recording.

7 | So doesn't that address the arguments in your
8 | papers that it's not an interception because what
9 | they're -- what's alleged in this case is that these
10 | defendants have configured their websites in such a
11 | way as to aid Facebook and Google? And I just read
12 | you the allegation in Google and others --

13 | MR. MELODIA: But --

14 | THE COURT: -- and secretly recording or
15 | listening and to hearing the communications between
16 | MGH and its patients.

17 | So doesn't that, at least for purposes of this
18 | statute, qualify as an interception?

19 | MR. MELODIA: No, it doesn't, your Honor.
20 | Putting aside the secrecy issue for the moment and
21 | just focusing on the interception, there needs to be
22 | a third party at some point while the communication
23 | is in transit between person number one and person
24 | number two. There needs to be a third person --

25 | THE COURT: The statute doesn't say that. The

1 statute doesn't say that. The statute says aiding --

2 MR. MELODIA: Well --

3 THE COURT: -- aiding somebody. It doesn't say
4 if it has to be contemporaneous or the like. It
5 simply says aiding a third party in hearing or -- in
6 secretly hearing or secretly recording.

7 MR. MELODIA: -- right. But we don't -- even by
8 the allegation the hospital's website does not aid in
9 the interception. It does not in any way allow
10 Facebook to eavesdrop or get in the middle of in the
11 way that one can intercept a passing football or
12 intercept anything else. You need to get in the
13 middle of a communication that is ongoing. That
14 communication has already finished. The get
15 communication, communication number one -- may I
16 share my screen, your Honor? We have a couple of
17 demonstratives that I've shown to Mr. Barnes a couple
18 of days ago.

19 THE COURT: Yes. I'll let you share a screen.
20 One moment. All right, you should have that
21 capability now.

22 MR. BARNES: Your Honor, Mr. Melodia did share
23 them with me. I have no objection -- assuming
24 they're the same, and I assume they are going to be
25 the same, particularly in regards to the preliminary

1 injunction. I would note however on the motion to
2 dismiss, to the extent they go beyond anything in the
3 motion itself, that's not entirely proper. But I've
4 seen them. They're fine for the Court to consider.
5 Particularly that we're taking up both motions here
6 today. Thank you, your Honor.

7 THE COURT: Mr. Melodia?

8 MR. MELODIA: So what we've tried to do, your
9 Honor, is just diagram based upon the way it's
10 described in the complaint and the way it's described
11 in the plaintiff's expert's report, the so-called get
12 communication; communication number one, and the so-
13 called post communication; communication number two.
14 And there are two distinct communications here. One
15 is between the hospital's website and the visitor's
16 browser -- that is the plaintiff, if the plaintiff
17 has configured their browser in a way that allows
18 that communication to occur. And --

19 THE COURT: Meaning if they allow third-party
20 cookies?

21 MR. MELODIA: To allow third-party cookies, your
22 Honor.

23 THE COURT: Yes.

24 MR. MELODIA: And so in that case there's a
25 communication there that Facebook is not a part of.

1 | So there is no interception or aiding and abetting.
2 | And then that communication complete --

3 | THE COURT: So pause for a moment. Mr. Melodia,
4 | would it be possible for Facebook to gain access to
5 | that communication if for example defendants did not
6 | include Facebook, did not permit Facebook to post
7 | cookies through their website?

8 | MR. MELODIA: -- I don't believe so.

9 | THE COURT: You don't believe it would be
10 | possible?

11 | MR. MELODIA: I don't believe it would be
12 | possible. But of course --

13 | THE COURT: So isn't that -- doesn't that at
14 | least qualify as aiding?

15 | MR. MELODIA: -- it's aiding, but not aiding a
16 | communication that is communication number two, the
17 | post communication, yes.

18 | THE COURT: Got it.

19 | MR. MELODIA: Aiding an interception, no.

20 | THE COURT: But again, we're talking about --

21 | MR. MELODIA: An interception --

22 | THE COURT: -- an interception is defined as
23 | aiding another party in its ability to hear --

24 | MR. MELODIA: -- hearing, hearing.

25 | THE COURT: -- or secretly -- to hear or secretly

1 record. And here --

2 MR. MELODIA: To hear or secretly record.

3 THE COURT: -- yes.

4 MR. MELODIA: But there is no -- let me show you
5 the next slide, your Honor, which -- okay, these are
6 the actual communications. This is the code, your
7 Honor, in the Smith affidavit that shows the actual
8 communication. These are not the same
9 communications. So you can't aid and abet somebody
10 either hearing or recording something they don't hear
11 or record. Communication number one is neither heard
12 nor recorded by Facebook.

13 THE COURT: So you read "hear" -- and the
14 definition of interception you mean it really has to
15 be audibly heard as opposed to communicated --

16 MR. MELODIA: No.

17 THE COURT: -- no? I see.

18 MR. MELODIA: No. I accept -- I'm not taking
19 some luddite approach to the wiretap act, even though
20 it's been around 40 years and has not been applied to
21 this exact scenario. Nonetheless, I'm not taking
22 that approach. I'm saying that these are separate
23 communications. And one way we know they're separate
24 communications, not just a (inaudible --
25 indecipherable at 2:22:43) but it is the actual

1 | separateness, the content of the communication as
2 | reflected on these slides from the Smith affidavit.

3 | The next is you can see communication number one
4 | is over and communication number two continues. You
5 | cannot aid and abet somebody in intercepting
6 | something that is neither heard in any technological
7 | sense, or recorded by Facebook. They're simply not a
8 | part of communication number one. In the same way
9 | hospital is not a part of communication number two.
10 | So there is true separateness in the way that they're
11 | -- so in other words, using the football analogy, you
12 | know, here's -- if there's no completion, you know,
13 | if there's a completion of a transmission, a
14 | completion of a pass, and then the other team gets
15 | it, that's called a fumble. And the difference is
16 | there has -- there's a complete transmission in
17 | communication number one. And then communication
18 | number two occurs, and that is a different
19 | communication. It's a communication between the
20 | individual plaintiff; the website visitor and Google
21 | and Facebook, or any other third party. And that's
22 | the way the internet works across the internet;
23 | healthcare companies and all sorts of other companies
24 | including law firms.

25 | So your Honor, again this whole theory, I mean

1 every --

2 THE COURT: Mr. Melodia, let me -- if you don't
3 mind, let me jump in here and help you with your
4 argument which is I don't buy this argument. Okay.
5 I don't buy it. The language of the wiretap act in
6 Mass is broad, is different than what I -- I looked
7 at the language of some of the other jurisdictions
8 that were cited.

9 So it seems to me that what you're describing is
10 aiding. And so -- and let me just -- I'll help you
11 along by saying you're not going to win that one.
12 I'm not persuaded.

13 I want to talk briefly about the secret piece.
14 Which is I did -- this is another situation where I
15 went back to see what was alleged, because again I've
16 got to -- I'm bound by the allegations of the
17 complaint, the amended complaint. And it's alleged,
18 at least in paragraph 327, among other places, I
19 think, that there was a secret recording of
20 plaintiff's wire communications by Facebook, Google
21 and others. So again, if I'm dealing with a motion
22 to dismiss, and I have to accept that allegation as
23 true, why are we fighting about whether it's secret?

24 MR. MELODIA: Because that's a legal label, your
25 Honor, that plaintiffs added. That's not a factual

1 | statement. That is not something the Court has to
2 | accept as true. That is a legal conclusion. The
3 | word "secret" is in the wiretap act, and they have
4 | merely (inaudible -- indecipherable at 2:25:30) back
5 | to the Court. That is not a sufficient pleading.
6 | There is no secret here. In addition to these being
7 | -- this is the way in which the internet works.
8 | Literally this hasn't been secret for 20 years. The
9 | "Double-Click" case in 2001 acknowledged that the use
10 | of cookies and the use of tracking on websites is not
11 | secret.

12 | In this particular case each hospital disclosed
13 | the use of cookies and disclosed tracking on the
14 | website, including references to Google analytics, as
15 | well as the pixels. So where is the secret? There
16 | can't be a secret by people who are using a free
17 | website from a device and looking at -- and clicking
18 | around. In the same way that if somebody visited a
19 | law firm website, your Honor, they don't become a
20 | client. These people don't become patients by virtue
21 | of simply clicking around on a public website.
22 | There's no secrecy going on.

23 | THE COURT: Right, but these plaintiffs allege
24 | they are patients. They're already patients.

25 | MR. MELODIA: It doesn't matter, your Honor. If

1 a client of a law firm who is a client goes on to the
2 general website of a law firm and clicks around and
3 searches anti-trust law, or searches breach of
4 contract, or fraud, and then looks at attorney bios,
5 and looks at email addresses and phone numbers for
6 contacting, that does not make that person a client
7 in that setting. They are not for example -- the
8 clicking and the searching is not for example
9 attorney/client privilege, is it? That can't be
10 attorney/client privilege. Does the law firm have a
11 duty all of a sudden -- for example, if they looked
12 up breach of contract and then they missed a statute
13 of limitations, can the law firm be sued for
14 malpractice because they missed the statute of
15 limitations on behalf of somebody who was a client
16 but didn't tell the law firm in engagement that they
17 are a client for purposes of a contract claim? No.
18 Those --

19 THE COURT: See the problem with that --
20 actually, Mr. Melodia, that's interesting that you
21 choose that analogy, because I've been bouncing that
22 one around in my head for some time. And here's the
23 problem I ran into with that analogy, which is assume
24 for the moment that the person who's using the
25 website is a client of the law firm. And they're

1 getting on and looking at some of the law firm
2 materials about their particular legal problem, which
3 is confidential. And the law firm then takes that
4 communication and makes it available to Facebook,
5 such that Facebook can then match the fact that that
6 client of the law firm has been rummaging around the
7 law firm's website with respect to a particular legal
8 issue that's confidential, and can match that
9 information with the identity of the user? So that's
10 more like what we have here. And in those
11 circumstances would that be deemed again -- there are
12 a number of claims here that are made with respect to
13 that type of activity, but it seems to me that at
14 least again -- and I understand you have an argument
15 with respect to disclosure, I've got that, but the
16 allegation is it's done secretly. It seems to me
17 that in those circumstances that's potentially a
18 violation of the wiretap act.

19 Let me also mention yet again this is a motion to
20 dismiss. You read the prologue to the wiretap act --
21 and the wiretap act is designed really for different
22 circumstances I'll have to say. And so again the --
23 let me pull up the actual language in the act. But
24 the preamble says, "The general court finds that
25 organized crime exists within the Commonwealth and

1 that the increasing activities of organized crime
2 constitute a grave danger to the public welfare and
3 safety."

4 So I agree with you this statute I think was
5 targeted towards a different set of problems. But
6 what I have to deal with in this context is how does
7 it apply here, and does plaintiff state a viable
8 claim? And I have to say under the wiretap act, I
9 think they do, based on the allegations of the
10 complaint. I recognize you disagree. I recognize
11 that. But I'm bound by what the allegations of the
12 complaint are in a motion to dismiss. And it seems
13 to me that they do, they state a viable claim under
14 the wiretap act. Whether that claim will succeed or
15 not is a completely different matter. But I'm --

16 MR. MELODIA: Understood, your Honor, but --

17 THE COURT: -- yes?

18 MR. MELODIA: -- the Court respectfully does not
19 need to take as true the secrecy allegation when the
20 secrecy is how the internet works across the entire
21 internet. Logically, just realistically,
22 sociologically, technically, there is no secret here.
23 This is all public information that anybody who is
24 using the internet ought to know and is charged with
25 knowing. And our law all the time charges people

1 with knowing things they may or may not actually in
2 fact know, but that doesn't make it secret and that
3 doesn't make it improper. And even the "Pharmatrak"
4 case, your Honor, which is the one case they can
5 point to that applies to in the Federal Wiretap Act
6 context apply, you know, these types of statutes to
7 facts that are somewhat similar in the sense that
8 they're happening on a website and they involve
9 deflection of information. But they're still
10 different. I mean "Pharmatrak", it was an anonymous
11 party. There was absolutely no disclosure whatsoever
12 of a PII being collected. PII being collected was
13 name, and address, and gender, and insurance
14 information, and medical conditions and medications.
15 And in there -- and this is the case, the main case
16 the plaintiffs rely upon your Honor for their wiretap
17 act theory. In that case the court did not decide
18 this timing issues as Mr. Barnes calls it on this --
19 and what I think of as separate communications, they
20 didn't resolve the timing issue. They in fact
21 explicitly reserved the timing issue and said the
22 facts here do not require us to enter the debate over
23 the existence of a real time requirement. And why
24 was that? Because they found a simultaneous
25 communication, which we don't have here, and an

1 identical communication, which we -- I showed on the
2 screen, we don't have here. So "Pharmatrak" really
3 doesn't get them where they need to go. Nor does the
4 "Facebook" case out of the ninth circuit. I mean
5 that case only --

6 THE COURT: Again -- again, Mr. Melodia, I don't
7 see any simultaneous or contemporaneous requirement
8 in the Massachusetts Wiretap Act. I don't see it.
9 Am I missing something? Is it there? Have I just
10 overlooked it?

11 MR. MELODIA: -- well I think it doesn't say the
12 word "simultaneous", your Honor, that is true.
13 However, what it does say is a third party needs to
14 have heard or recorded a communication. And that
15 didn't happen here. As alleged, it didn't happen
16 here. There was no recording, secret or otherwise.
17 And there was no hearing, secret or otherwise by
18 Facebook, or Google, or any third party to
19 communication number one, the get communication, as
20 pled by Mr. Barnes in the complaint and as is
21 obviously found in the Smith affidavit repeatedly.

22 THE COURT: Okay. Let me pause for a moment --

23 MR. MELODIA: So that's my point.

24 THE COURT: -- Mr. Melodia. I'm going to ask you
25 to pause there. I'm going go through these claims

1 | one at a time.

2 | Mr. Barnes, briefly what do you have to say in
3 | response to Mr. Melodia's point that it's not the
4 | same communication?

5 | MR. BARNES: Well, your Honor, if you have Mr.
6 | Smith's declaration -- well, do you have the
7 | complaint in front of you?

8 | THE COURT: I do. The amended complaint, yes.

9 | MR. BARNES: Right. If you go to paragraphs 103
10 | and 104, they are on pages 24 and 25. Mr. Melodia
11 | says --

12 | THE COURT: I have them.

13 | MR. BARNES: -- Mr. Melodia says there are two
14 | separate communications here. And I want to provide
15 | just one example from the complaint to show that
16 | there are not two separate communications. Your
17 | Honor has it right. The Massachusetts law makes no
18 | distinction that the federal law does. But if you
19 | look at paragraph 103 there is the button up there at
20 | the top right screen in the screenshot that says
21 | "enroll or sign in to patient gateway."?

22 | THE COURT: Yes.

23 | MR. BARNES: Okay. When a patient clicks that
24 | button what happens is that's the patient's
25 | communication. That is the patient's sole

1 | communication to Mass General Hospital in that
2 | example. It starts a transmission of data and
3 | exchange of content between Mass General and the
4 | patient's web browser. But immediately upon clicking
5 | that button the source code Mass General puts on its
6 | website redirects the content, the precise content of
7 | that button click to Facebook. And that's shown in
8 | paragraph 104. You see --

9 | THE COURT: I see.

10 | MR. BARNES: -- at the top of the graph where it
11 | says "EV subscribe button click", and then it says
12 | "button text enroll or sign in to patient gateway."
13 | That's not a -- the patient did nothing else to send
14 | that data to Facebook. That's entirely the result of
15 | the source code that Mass General put on its web
16 | property. And the same is true of every other
17 | communication we're talking about in this case. As
18 | it relates to the Facebook tracking pixel, your
19 | Honor, this piece of source code is set up in a way
20 | that Facebook actually gets the content of the
21 | communication in most circumstances before Mass
22 | General even receives it. And the reason for that is
23 | Facebook wants to make sure that it gets it.

24 | I also heard Mr. Melodia say that this is only
25 | because the plaintiff's web browsers are configured

1 -- they had to choose to let this happen. First of
2 all the default setting out of the box, this happens
3 in the default setting out of the box.

4 Second of all, I believe we've alleged in the
5 complaint -- I don't have the particular paragraph,
6 we've alleged the deployment of what's called cookies
7 syncing technology. And what cookie syncing
8 technology means is that even if a user tried to
9 block Facebook's cookies and tracking on a website
10 like MGH, it happened anyway because of this cookie
11 syncing. They've hacked -- they've figured out a way
12 to hack their way around the browser settings that
13 would block this tracking behavior.

14 So there is no separate communication of the
15 patient. And the Massachusetts Wiretap Act is set up
16 to protect the communications of people, not of the
17 redirections caused by intercepting devices.

18 What Mr. Melodia is essentially asking this Court
19 to do is repeal the wiretap act. Because if you
20 think even in the context of a traditional wiretap
21 act, right, where there's a bug on a telephone, a bug
22 on a telephone results in the content of that
23 communication being delivered to the recording
24 interceptor along a separate path from the
25 communication between the victim's phone and the

1 | person they're speaking with's phone. The bug sends
2 | it this way. And that's exactly what this Facebook
3 | source code does. That's why they're called web
4 | bugs, your Honor.

5 | THE COURT: Got it. All right, I think I've got
6 | it Mr. Barnes. Thank you, sir.

7 | So Mr. Melodia, I think I've got this one, sir.
8 | I -- this is a motion to dismiss. I'm going to deny
9 | the motion to dismiss with respect to the wiretap
10 | claim. Again, a different matter whether that claim
11 | ultimately succeeds, but on a motion to dismiss I've
12 | got to -- I have to deny the motion with respect to
13 | -- that's Count One.

14 | We talked briefly about the invasion of privacy
15 | claim. That's statutory as well. "Has to be an
16 | unreasonable, substantial or serious interference
17 | with privacy, and whether the intrusion is
18 | unreasonable, substantial or serious presents a
19 | question of fact." That's the "Polay" case from the
20 | SJC back in 2014. And again when I look at the
21 | allegations of a complaint of what the plaintiff
22 | allege is that the defendants are disclosing
23 | confidential patient medical information to third
24 | parties, including information about their medical
25 | condition. Here's what -- okay, you can -- I'll

1 | listen to you in a moment Mr. Melodia, but here's
2 | what I saw in the complaint. And if I'm misreading
3 | it you can point it out to me. But what I see in the
4 | complaint is plaintiffs allege that the defendants
5 | are disclosing confidential patient medical
6 | information to third parties, like Facebook and
7 | Google, that the information includes information
8 | about the patient's medical condition and diagnoses,
9 | and interest in particular specialists. For example
10 | what we just discussed, the perhaps a patient's
11 | interest in a breast cancer specialist. And that
12 | they're doing it in a way that allows the third
13 | parties like Facebook to correlate that information
14 | and identify the particular user.

15 | So again, you say that's not an unreasonable, or
16 | substantial or serious invasion of the privacy of
17 | those people. I am not sure I see it that way.

18 | MR. MELODIA: Well, your Honor, I would never say
19 | that the disclosure of an individual's personally
20 | identifiable health information was not serious and
21 | substantial. The hospitals completely understand
22 | that. I understand that. Nobody is disputing that.
23 | But that's not what's happening. Not because --

24 | THE COURT: But pause one moment. What's
25 | happening is a different animal.

1 MR. MELODIA: Okay.

2 THE COURT: So that's the point I'm trying to get
3 across here --

4 MR. MELODIA: I get it.

5 THE COURT: -- is there's a huge dispute between
6 these parties with respect to how this technology
7 actually works and what's being transmitted. I got
8 that. I understand that. But my point is simply
9 I've got a motion to dismiss. So what I have to do
10 is I have to accept plaintiff's version which is no,
11 it is happening, it is happening. That's what
12 plaintiffs allege. And in those circumstances if it
13 is happening isn't that an invasion of privacy?

14 MR. MELODIA: Well if a true medical condition of
15 an identified individual were being transmitted to
16 Facebook and Google from our website that would be
17 actionable, that would be an invasion of privacy,
18 that would be substantial and serious. But that's
19 not what really is alleged. They use the word
20 medical conditions, but what they're talking about is
21 searches, and URLs and search terms on a public
22 website like these hospitals. And that is not
23 actionable. That is not PHI. That is not covered by
24 HIPAA. That is no way protected health information.
25 PHI is defined by the law. It's also not even

1 | personal information as defined by Massachusetts law.

2 | THE COURT: If a patient has --

3 | MR. MELODIA: And --

4 | THE COURT: -- has breast cancer for example.

5 | Again, obviously something that can be deeply
6 | disturbing to that patient for good reason --

7 | MR. MELODIA: -- certainly.

8 | THE COURT: -- there's something that they do not
9 | wish to disclose publicly. They get on the MGH
10 | website and start cruising the MGH website for
11 | information about breast cancer and about breast
12 | cancer specialists. Maybe they're looking at Dana-
13 | Farber. I don't know. But they're looking on your
14 | defendant's websites for information that will help
15 | inform them about, you know, their diagnosis, about
16 | what alternative treatment alternatives exist, who
17 | their treatment, you know, provider should be. All
18 | of that information seems to me that can be, very
19 | possibly is, confidential information, confidential
20 | patient information. That patient doesn't want other
21 | people to know that the looking for information about
22 | breast cancer diagnosis, and treatment and potential
23 | providers. But that's the kind of information that
24 | plaintiff say is shared with Facebook and that
25 | Facebook can then trace back and say we know that

1 | this particular Facebook user is looking for a breast
2 | cancer specialist. That's what they allege. And I
3 | don't -- again, I don't think I've got the
4 | allegations wrong. That's -- whether again that's
5 | true in the real world is not a matter for me to
6 | resolve today. But that's what they allege. Isn't
7 | that enough to support a claim for invasion of
8 | privacy under Mass law?

9 | MR. MELODIA: Not to an unidentified individual,
10 | your Honor. They may be a patient in the same way
11 | again that somebody may be a client going onto a law
12 | firm website, but they are not a patient on a public
13 | website with disclosures telling them that cookies
14 | are being used and tracking is happening. Not to
15 | mention the disclosures that they agreed to which
16 | Facebook and Google when they became users of those
17 | products to begin with. So no, your Honor, somebody
18 | -- whether they're a patient or not, that visits a
19 | general website -- they could be on Google.com, they
20 | could be on WebMD, they could be anywhere doing that
21 | search, and if their information went to Facebook and
22 | Google from any of those websites, it is not the
23 | website operator's business whether that operator is
24 | a hospital or anybody else; Google, or WebMD, or
25 | anybody else, to know that that person's a patient.

1 In fact, the hospitals don't know. And they don't
2 try to know in any way who a device ID represents,
3 because as I mentioned at the outset, a device ID
4 could represent -- I'm sorry, not a device ID, an IP
5 address, can represent any number of people, any
6 number of devices. And it doesn't tell us that that
7 person is a patient doing a search on their
8 condition. That is not what personal health
9 information is, protected health information is. It
10 has to be identifiable to an individual. And that's
11 not, because all you're doing is a search on a public
12 website from a certain IP address that can change
13 over time, can change that day. And it could be you,
14 it could be somebody doing medical research for a
15 friend or a family member, it could be somebody doing
16 a term paper in eighth grade or in medical school.
17 It could be a competing research facility that wants
18 to know what's going on at Dana-Farber because they
19 just won, you know, a Nobel Prize in that particular
20 area, and so let's find out more about the research.
21 That does not signify patient status.

22 And importantly, this idea -- I want to go back
23 to paragraph one of three that Mr. Barnes was
24 highlighting. That's a really important paragraph in
25 the complaint because that shows us the page from

1 | which the Court seems concerned that there could be a
2 | direct portal into actual patient records and the
3 | types of HIPAA protected information that does
4 | deserve full protection and is subject to HIPAA, and
5 | is subject to the notice of privacy practice; NPP
6 | that is prominently displayed as it is required to be
7 | by federal law on the website. Not because there's
8 | PHI on the website, but because that notice has to be
9 | disclosed on a website in the same way for example
10 | that you put a notice of a federal employment law
11 | like a parental leave policy. You put that on the
12 | bulletin board of the employer. That doesn't mean
13 | that everybody who walks by the parental leave policy
14 | becomes a parent and has a right to all of a sudden
15 | get leave and get paid for leave. It doesn't create
16 | a new right, nor does the NPP create rights or
17 | signify that there's PHI or patient activity going on
18 | on these websites. Instead these websites are about
19 | the services being offered in the appropriate places,
20 | in the protected places. These hospitals know how to
21 | handle HIPAA. And as your Honor pointed out in his
22 | paragraph 146 of the amended complaint makes really
23 | clear this is not about the patient gateway. This is
24 | not about what's behind a firewall. Where you get if
25 | you log in with a user name, and credentials and a

1 password, that's where you can make an appointment
2 with a doctor. That's where you can communicate with
3 a doctor. That's where your PHR or your pharmacy
4 records are. None of this that is going on on a
5 public website is protectable. And it's certainly
6 not a substantial and serious privacy concern. If it
7 is, then websites across the world -- not just for
8 hospitals, because this basic principle would flow
9 through to virtually every profession, every website
10 dealing with any sort of information that if it were
11 linked truly to an individual, an identifiable
12 individual could be of concern. But it's not.
13 That's the entire reason to have a general website,
14 and then a separate distinct URL which is the patient
15 gateway. Which I'm not sure whether that's become
16 clear enough yet that that is a separate URL --

17 THE COURT: No, it's clear.

18 MR. MELODIA: Okay. I --

19 THE COURT: I promise you it's clear. And also
20 -- I'll also tell you I think at a macro level I
21 agree with you I think that HIPAA is a bit of a red
22 herring in this proceeding and in these arguments,
23 okay? I'm not persuaded that HIPAA really has much
24 of a role to play in the analysis that I have to
25 undertake. But I'm taking it --

1 MR. MELODIA: Well --

2 THE COURT: -- in a much more maybe mundane
3 pragmatic level, which is I've got a complaint that
4 alleges that take aside, ignore the patient portals,
5 that patients who use the defendant's website for
6 other purposes, their own personal medical purposes,
7 that that information is in fact being shared with
8 third parties through the website. And that -- we'll
9 get to -- at some point in time again I want -- we
10 need to re-circle, circle back on the question of
11 disclosure and consent, we're going to get there.
12 But I -- and that's what I've got is alleged here.

13 So Mr. Melodia I'm going to ask you to pause for
14 a second.

15 MR. MELODIA: Mm-hm.

16 THE COURT: Mr. Barnes, two minutes, anything you
17 want to say on this -- we're talking about invasion
18 of privacy.

19 MR. BARNES: Right, your Honor. I think I want
20 to answer that I think there is a question there in
21 HIPAA's role and the analysis. We would agree that
22 the Court doesn't have to ultimately reach any HIPAA
23 question here. But HIPAA does play some role in the
24 analysis. And let me explain why. And the first
25 place I think to start is paragraph one where Mass

1 General's chief marketing officer says the trust and
2 confidence that you have in your --

3 THE COURT: This is the sacred language, the
4 sacred language that if I -- I wish I could search
5 your complaint for sacred, I think it would pop up a
6 number of times. Certainly plaintiff's made good use
7 of that language. I got it.

8 MR. BARNES: -- right. And those are their
9 words.

10 THE COURT: Yes, I understand.

11 MR. BARNES: And part of that is patients to a
12 person understand -- they might not know the line and
13 detail of the HIPAA statute and HIPAA regs, but
14 they've got this idea that HIPAA protects their
15 personally identifiable information from disclosure
16 from their healthcare provider. And that idea is
17 furthered when they show up for their first
18 appointment and it's required by law that the HIPAA
19 notice is provided to them. And as you noted in the
20 previous hearing, that HIPAA notice says we never
21 share your personal information for marketing
22 purposes without your written authorization. And
23 "never" is in italics. And so any time that a
24 patient goes to these web properties they go to --
25 they go there with the -- they're bringing with them

1 | this baggage so to speak, this trust and confidence
2 | that their healthcare provider is not like
3 | Zappos.com. They're not buying shoes here, Judge,
4 | they're talking to their healthcare provider. Okay?
5 | And so that colors every other disclosure that there
6 | may or may not have. And I want to -- we can get
7 | further into those disclosures later but that colors
8 | everything.

9 | In addition to that Mr. Melodia keeps talking
10 | about public websites, oh, and basically making the
11 | argument I think that there is no privacy on public
12 | websites on the internet. Well, your Honor, the
13 | "Pharmatrak" case called that argument frivolous.
14 | Not my words. That's the first circuit's words to
15 | the argument that hey if you go on the internet you
16 | need to be wary.

17 | The second thing is that didn't prevent the court
18 | in "Medstar" -- "Doe versus Medstar" from finding a
19 | claim, or "Doe versus Virginia Mason", or the "Google
20 | Cookie" case that I happened to argue, or the
21 | "Nickelodeon" case that I happened to be counsel for
22 | the plaintiffs on, or "Weld versus -- well, "Weld
23 | versus CVS" was not an internet privacy case, or the
24 | Facebook" internet case that the ninth circuit said
25 | was actionable on which I represented the plaintiffs.

1 This is squarely in the line of those cases. If
2 anything, the conduct of the defendants here are
3 worse.

4 THE COURT: Thank you.

5 MR. MELODIA: Your Honor, may I respond?

6 THE COURT: Mr. Melodia, one minute, I'll give
7 you one minute to respond. But then we're going to
8 keep moving.

9 MR. MELODIA: It's absurd to say that the conduct
10 here was worse. The whole idea of the "Google" case
11 in the third circuit, the "Nickelodeon" case in the
12 third circuit, and the "Pharmatrak" decision is
13 outright deception by the plaintiff -- by the
14 defendants against the plaintiffs, the active
15 hoarding of their efforts to protect their privacy
16 and active deception; saying one thing and doing
17 another. The only thing that plaintiffs can come up
18 with to try to create the impression of that here is
19 by tying us to a promise in the NPP which only
20 applies, according to OCR, when you have PHI. So if
21 your Honor is true to his words --

22 THE COURT: Believe me -- pause for a moment Mr.
23 Melodia. I've got it. There's always a certain
24 level of hyperbole in these arguments. Okay? And so
25 I've got it. I heard what Mr. Barnes had to say.

1 Here's what we're going to do. I'm denying the
2 motion to dismiss with respect to the invasion of
3 privacy claim. Folks, that's a very ambiguous right
4 in Massachusetts, but it seems to extend to
5 confidential medical information. And the
6 allegations of the complaint are that patient's
7 confidential medical information is being shared
8 probably without their knowledge or understanding
9 with third parties. That it seems to me that at
10 least states a viable claim for invasion of right of
11 privacy under Massachusetts law. So I'm going to
12 deny it.

13 We've got a breach of fiduciary duty claim.
14 Here's the -- I think we can deal with this one
15 pretty quickly.

16 Mr. Melodia, I read the arguments. Not a lot of
17 ink was spilled on either side on this one. But I
18 did. So I was interested to see actually the SJC has
19 recognized a fiduciary obligation on the part of
20 physicians not to disclose medical information. They
21 did that in the "Alberts versus Devine" case. And
22 the appeals court has picked up on that as well in
23 the "Corper versus Weinstein" case. So --

24 MR. BARNES: Yes.

25 THE COURT: -- those cases seem to recognize yes

1 | in Mass a physician could have a fiduciary obligation
2 | not to disclose -- or the opposite side, flip side of
3 | the coin is to maintain the confidentiality of a
4 | patient's medical information.

5 | So basically what we've got alleged here, it
6 | seems to me that it's potentially -- potentially it's
7 | a breach of fiduciary duty. And it seems a little
8 | bit of an odd fit. But those cases recognize a
9 | fiduciary obligation.

10 | MR. MELODIA: But we're being -- no, that would
11 | be I think clear error to find that in this case.
12 | Because --

13 | THE COURT: It wouldn't be the first time, but go
14 | ahead.

15 | MR. MELODIA: -- no. But this one -- clearer
16 | than most, your Honor, because of this reason. Look,
17 | the -- if you take as a given that a physician can
18 | have such a personal fiduciary relationship with a
19 | patient in the same way that for example a priest
20 | might have with a parishioner like the "Petrelvy
21 | Reposi" (phonetic) case we've cited, case nine of our
22 | brief. That's fair enough, those are personal
23 | relationships. I'm not contesting that. I don't
24 | think we ever contested that. The point here is
25 | nobody has sued a physician. We've sued hospital

1 | systems and hospitals. Fundamentally what the
2 | "Petrelvy Reposi" case stands for is that the church
3 | as an organization and the diocese is not the priest.
4 | Nor is the physician, the hospital or the hospital
5 | system. There's fundamentally a difference in a
6 | fiduciary --

7 | THE COURT: So you're argument essentially that
8 | an organization can't owe a fiduciary obligation? It
9 | has to be an individual obligation? Am I
10 | characterizing --

11 | MR. MELODIA: -- it has to --

12 | THE COURT: -- correctly?

13 | MR. MELODIA: -- but I think there are times when
14 | you could have a sole proprietorship or something,
15 | your Honor, where there's an organization technically
16 | speaking, but there is a personal relationship. I'm
17 | not suggesting that it only has to do with how many
18 | people or the corporate form. I'm having -- I'm
19 | talking about where the reality of the relationship
20 | rests, where the duty rests. And the duty rests not
21 | with the hospital in terms of an individualized
22 | personal relationship with the plaintiff here, with
23 | the patient. Rather it rests with the physician. In
24 | the same way that --

25 | THE COURT: Well pause, Mr. Melodia. You're

1 | confusing me. So are you saying for example that MGH
2 | doesn't have any duty or obligation to its patients?

3 | MR. MELODIA: -- well --

4 | THE COURT: You have MGH -- let me finish the
5 | question. Does MGH, or Dana-Farber, or Brigham, have
6 | any duty as organizations not to disclose their
7 | patient's confidential information? Do they have a
8 | duty?

9 | MR. MELODIA: Yes, under HIPAA, absolutely, your
10 | Honor. They have a --

11 | THE COURT: You don't think they have any common
12 | law duty? So when the SJC talks about a physician's
13 | obligation not to disclose confidential medical
14 | information of a patient again you don't think that
15 | there's a comparable duty on the part of the
16 | organizations as well?

17 | MR. MELODIA: -- I don't think there's a
18 | fiduciary duty, your Honor. I think you could have a
19 | negligence claim, your Honor. There could be a duty
20 | in the negligence sense. So you could have a breach
21 | of a duty in the negligence claim potential. But I
22 | can't see -- I mean and of course if an institution
23 | says one thing and does another, you know, there's a
24 | problem there. But that's not what we have here.
25 | We're trying to impose a fiduciary duty. And that is

1 | different in the law than other types of duties,
2 | including duty in the negligence sense. So I'm not
3 | suggesting in any way that any of these hospitals
4 | don't fully understand and meet their obligations for
5 | privacy. But these are highly regulated
6 | institutions. And HIPAA does (inaudible --
7 | indecipherable at 2:57:51) how they approach these
8 | issues. So to sort of suggest that HIPAA defines the
9 | expectation as Mr. Barnes would have it, of everybody
10 | walking in the door, and yet HIPAA doesn't really
11 | technically have to apply and we don't really have to
12 | find that PHI is present (inaudible -- indecipherable
13 | at 2:58:10). That's disingenuous. So I think here
14 | there is no case law that extends anything in terms
15 | of a fiduciary duty to institutions in the (inaudible
16 | -- indecipherable at 2:58:23) of hospitals here.

17 | THE COURT: Got it. All right.

18 | MR. MELODIA: And I think it would be a mistake.

19 | THE COURT: Mr. Barnes, he says institutions,
20 | that the duty that's been recognized by the Supreme
21 | Judicial Court and the Mass Appeals Court doesn't
22 | extend to the institutions, it's personal to the
23 | physicians. What do you say?

24 | MR. BARNES: Can you hear me, your Honor?

25 | THE COURT: I can hear you, sir.

1 MR. BARNES: Okay. Sorry. I got -- the
2 technology got mixed up here. Well we disagree, your
3 Honor. I don't think that should surprise you, for a
4 number of reasons. First, the case "Doe versus
5 Harbor Schools", the Massachusetts -- the Supreme
6 Judicial Court outlined that a fiduciary duty exists
7 quote, "When one reposes faith, confidence and trust
8 in another."

9 Paragraph one -- to go back to it, the quote from
10 Mass General's own chief marketing officer was "The
11 trust and confidence you place in your existing or
12 potential healthcare provider is sacred."

13 That fits the Massachusetts test and we're there.

14 The "CVS" case found a breach of fiduciary duty
15 of the first go-around. That's a corporate entity.
16 And I think the "Alberts versus Devine", which you
17 mentioned your Honor, that court -- the court clearly
18 said just because a certain fact pattern hasn't come
19 before us before doesn't mean the common law doesn't
20 recognize a cause of action in that fact pattern.
21 And it's not a far stretch. And it's interesting
22 because the remedy for a dismissal for failure to
23 name the corporate entity is to bring in every doctor
24 at all of these hospitals as defendants in this case,
25 which would be somewhat unwieldy and we don't really

1 think that's the thing to do because the corporate
2 entities were the ones making the decision to put
3 this source code on these web pages.

4 And your Honor, there's one thing I'd like to --
5 Mr. Melodia said -- seemed to suggest we were making
6 the argument that HIPPA defines the expectations. I
7 think that's the opposite of the argument I made.
8 It's that HIPAA colors the expectations. And I'd
9 like to give you an example as it relates to this
10 breach of fiduciary claim.

11 THE COURT: Yes.

12 MR. BARNES: Okay? If an oncologist clinic took
13 down the phone numbers of everyone who called the
14 public phone line for that clinic and some basic
15 notes on the topics of what the caller discussed, and
16 at the end of the day they bundled all of that up and
17 they sent it off to a third-party marketing firm and
18 said hey, we want to advertise to these people to
19 potentially come in for treatment at our clinic,
20 would that be a breach of fiduciary duty for that
21 subset of callers who were patients? I think there
22 is no doubt that it would be. But we also know that
23 there would likely be some pharmaceutical drug reps
24 who had called. There may be some random advertising
25 people who had called. There may be other doctors

1 | who had called, who would have been in that batch of
2 | phone numbers that was sent to the third-party
3 | marketing company. But the fact that those positives
4 | might exist in the data does not negate the
5 | hospital's duty to its patients. It can't just give
6 | patient information away. And the other thing, your
7 | Honor that's relating to this is it's not just the
8 | enroll or sign in to the patient portal click that
9 | attaches patient status to a person at the primary
10 | website, it's also all kinds of other things, like
11 | when they look up to request an appointment, when
12 | they look up at Dana-Farber to get a second opinion.
13 | Those examples are in our complaint. And we
14 | specifically pled that our clients -- and you stated
15 | this earlier, we specifically pled that our clients
16 | used that sign in button to get where they were
17 | going, which attaches patient status to them. It's
18 | as if they called the phone line and the phone number
19 | said hey, press one if you're a patient --

20 | THE COURT: I'm not sure I --

21 | MR. BARNES: -- and you press one.

22 | THE COURT: -- I agree with you on that point Mr.
23 | Barnes. But okay, I think I've got it.

24 | So here's what I'm going to do with respect to
25 | this claim. Folks, I want to reserve -- I want to

1 take a look. I want to take closer look at the point
2 that Mr. Melodia raised. Certainly again I agree
3 with the Mass law definitely recognizes some sort of
4 fiduciary obligation. And it's kind of interesting.
5 You read -- I read the "Alberts" case earlier. You
6 can see sort of the SJC wrestling with the notion of
7 there is this obligation and how they're going to
8 characterize it. Ultimately they say it's a
9 fiduciary obligation. I can't say they look like
10 they're entirely comfortable with that. But I -- but
11 that's what they hold. I need to go back and take a
12 look, and see whether that would extend to the
13 organization as well. So I'm going to defer on that
14 one.

15 That leaves the 93A claim. Let me jump on that
16 one.

17 So Mr. Barnes, front and center, you have on that
18 one, 93A. So the SJC has held -- let me pull it up,
19 they held in the "Linkage Corp versus Trustees of
20 Boston" case, "That in most circumstances a
21 charitable institution will not be engaged in trade
22 or commerce when it undertakes activities in
23 furtherance of its core mission."

24 So you have to agree with me Mr. Barnes that
25 these websites definitely are part of the core

1 mission of these institutions.

2 MR. BARNES: Well I -- accept that the reason for
3 the -- for the use of these marketing tools is to
4 increase revenue, gain more patients --

5 THE COURT: I saw that.

6 MR. BARNES: -- your Honor.

7 THE COURT: But that's not what we're talking
8 about here. We're talking about the relationship,
9 the interaction between these organizations and the
10 patients, your clients. So your patients, they're
11 going to this website, they're going to these
12 websites because they're looking for healthcare
13 information. Part of what these defendants provide.
14 That's their core mission is to provide healthcare to
15 people who need it. And so it's a little difficult
16 to say that really anything that goes on at these
17 websites is trade or commerce when it's part of the
18 core. It's the core mission of these not-for-profit
19 healthcare institutions. And I'll hear you, but I'm
20 wrestling with it. I don't see how you can see it
21 any other way.

22 MR. BARNES: Well, thank you for that warning,
23 your Honor. And I --

24 THE COURT: Laughing. Go for it. Go for it.
25 You know, it's never caused people to hold back in

1 the past. Go for it.

2 MR. BARNES: -- okay. So your Honor, I think
3 that the Massachusetts Consumer Protection Act is out
4 there to -- it's not just to protect consumers, it's
5 to protect businesses engaged in commerce from unfair
6 methods or practice in their business.

7 There is no doubt that these hospitals compete
8 against other institutions that are not nonprofit
9 institutions; that are for-profit institutions. And
10 that --

11 THE COURT: But you're not pursuing a claim on
12 behalf of other institutions against these hospitals.
13 You've got individuals. So if anything, this is a
14 Section 9 claim, 93A, Section 9. It's not business
15 to business.

16 MR. BARNES: -- correct. And I want to connect
17 the dots to why it involves commerce. It's because
18 it involves competition for the dollars that are
19 attached to those consumer patients that it involves
20 commerce. And in -- first of all we have alleged it,
21 but in addition to that I think the opposition papers
22 on the motion for preliminary injunction it's
23 conceded that this was to increase patient volume to
24 -- it's a marketing effort. That's what these tools
25 are, they're marketing efforts. Maybe it would be

1 | more appropriate to -- do you want me to talk about
2 | -- we've got a couple documents in discovery that
3 | we're going to provide for the Court relating to the
4 | motion for preliminary injunction that I guess can
5 | wait, or if you want me to speak about them now, your
6 | Honor, I can.

7 | THE COURT: No, well actually, let's stay on --
8 | if you don't mind just stay on this point for the
9 | moment, which again is what we're talking about are
10 | the websites. That's the core.

11 | MR. BARNES: Yes. That --

12 | THE COURT: That's the core of the complaint, is
13 | what happens on the websites. And again it seemed --
14 | I don't think you actually -- with all due respect, I
15 | don't think you answered the question which is the
16 | website --

17 | MR. BARNES: -- well, I wanted --

18 | THE COURT: -- the websites --

19 | MR. BARNES: -- what --

20 | THE COURT: -- seem to be again to be front and
21 | center even these days. There are probably more
22 | people interact with these institutions via their
23 | websites than in person I'm guessing. But in any
24 | event, that the websites are part and parcel of what
25 | these folks deliver which is healthcare, healthcare

1 | advice and it's part of -- when you look at it that
2 | way you can't characterize it I don't think fairly as
3 | anything other than part of the core mission.

4 | So Mr. Barnes, you want to take another crack at
5 | it?

6 | MR. BARNES: Yes. I think the Court should
7 | narrow in a little bit further. It is about the
8 | websites. It's also about the deployment of these
9 | specific invisible marketing tools on those websites,
10 | and how those marketing tools are used by the
11 | defendant to increase revenues by bringing more
12 | patients to their facilities to increase revenues.
13 | That's the purpose of this, is to increase revenue.
14 | And our argument is look, when you have an entity
15 | engaged in commerce -- and they are engaged in
16 | commerce and they're taking -- making an effort to
17 | increase their revenue that falls under the Chapter
18 | 93A, Section 9.

19 | THE COURT: It seems to me -- I hear you Mr.
20 | Barnes. What I think you're saying though is you're
21 | focusing on what you allege are the unfair or
22 | deceptive acts or practices. But again, the context
23 | in which those purportedly arise is in the websites.

24 | Mr. Melodia, do you want to say something on this
25 | point?

1 MR. MELODIA: Just a little bit, your Honor. You
2 know the case your Honor cited, the "Linkage" case
3 from the Supreme Judicial Court was actually the case
4 the plaintiffs cited. There are two other cases; the
5 "All Seasons Services" case against the "Boston" --
6 then called "Boston City Hospital" and the "Melrose
7 Wakefield Hospital" case, both cited in our briefs.
8 Those are cases that show where hospitals;
9 nonprofits, were engaged in conduct that if a for-
10 profit were doing it could be something that makes
11 money. But that doesn't mean, according to the
12 Supreme Judicial Court, that automatically because
13 one markets, or advertises or amplifies the message
14 of these public charitable institutions that
15 automatically that converts it to trade or commerce.
16 So if there is no message that get out there, if
17 there is ultimately no margin to the services
18 offered, there is no mission, there is no public
19 charity to be had because the organizations won't
20 exist very long.

21 So I think in addition to the point your Honor
22 made even taking Mr. Barnes' representations as, you
23 know, part of what he's after in this case, focusing
24 on the advertising tool, that isn't enough to convert
25 this to trade or commerce under the case law from the

1 Supreme Judicial Court.

2 THE COURT: Okay. All right, Counsel.

3 Mr. Barnes --

4 MR. BARNES: Your Honor?

5 THE COURT: -- yes, very briefly, sir. Yes?

6 MR. BARNES: Very briefly. So I'd like to point
7 out the defendant's memorandum on page 13
8 characterized what it's doing here as quote, "routine
9 commercial behavior." And the precise quote from
10 Linkage Corp -- and it cites to a Planned Parenthood
11 case is "That where an institution has inserted
12 itself into the marketplace in a way that makes it
13 only proper that it be subject to the rules of
14 ethical behavior and fair play."

15 And I think that language from the case lends
16 itself to what I was speaking about earlier that the
17 CPA is designed not just to protect consumers, but
18 one of its purposes is to make sure there is ethical
19 behavior and fair play in the marketplace. And that
20 means making sure that even nonprofit corporations
21 when they're engaged in revenue enhancing activities
22 in the marketplace they're subject to the CPA.

23 THE COURT: That would be true for all sorts of
24 activities it seems to me that not-for-profits would
25 be engaged in.

1 I'm going to dismiss Count Four. Again, SJC has
2 indicated that as a general matter 93A doesn't apply
3 when a charitable institution undertakes activities
4 in furtherance of its core mission. Again, I can't
5 describe these websites as anything other than part
6 of these defendants' core mission. So maybe this is
7 another instance of my clear error. I don't think
8 so, but I'm going to run with it.

9 All right, let me address the motion for
10 preliminary injunction. Folks, I'm denying that
11 motion. And here's why. I read everything that was
12 supplied to me in the aftermath of our last hearing
13 of the various submissions; the written submissions,
14 the affidavits, the further letters. A preliminary
15 injunction is prospective in nature. And anyone who
16 was alive and listened to or participated in our last
17 hearing on this matter understood that I had very
18 significant concerns that really revolve primarily
19 around issues of notice and consent on the part of
20 users of these websites. And consent seems to me, if
21 it exists, effectively moots all of the plaintiff's
22 claims. So a lot of your fight here is going to be
23 about consent, whether there is in fact consent. By
24 plaintiff's own admission defendants already have
25 gone a long way to solving the problem. I know

1 that's the same -- that's the equivalent of the
2 sacred language that you're probably going to hear a
3 lot about Mr. Barnes, but by including those cookie
4 banners and other changes in their websites. I mean
5 I got on folks. I looked at the cookie banners. And
6 I -- they're also recited in the papers. And I don't
7 -- I'm not required to say I think in the preliminary
8 injunction context whether those changes are
9 sufficient to eliminate all liability. In fact it
10 seems to me the cookie banners might make some
11 reference to the fact that actually the institutions
12 share some of the data that's collected with third
13 parties. That could be referenced it seems to me in
14 the cookie banners as well. But I'm not -- it's not
15 up to me to dictate the language of the cookie
16 banners. But it does cause me to conclude that in
17 light of those changes and in light of the
18 prospective nature of a preliminary injunction that
19 the defendants -- that the plaintiffs have not
20 demonstrated a likelihood of success going forward.

21 And I'll also mention that I think the changes
22 that have been made significantly undermine
23 plaintiff's irreparable harm arguments because if the
24 nondisclosure -- if nondisclosure of confidential
25 information is of great importance to a user of those

1 | websites then I suspect that they'll click on those
2 | privacy notices that are presented to them in the
3 | cookie banner and that they will get a fairly good
4 | understanding of what is actually happening with
5 | their data and how it can be used.

6 | And so it seems to me in those circumstances they
7 | have a means themselves, it's available to them, to
8 | address any potential irreparable harm.

9 | So I'm going to -- it seems that this is not a
10 | case right now that calls for a preliminary
11 | injunction. I'm denying the motion for preliminary
12 | injunction for the reasons that I've stated.

13 | Counsel, some of this case is going to survive.
14 | I have to get back to you with respect to the count
15 | for breach of fiduciary duty. I'm going to do that
16 | quickly. It's not going to take me very long. I'm
17 | going to do that research. You should get my
18 | decision on that by next week.

19 | We need to give you a next date in this case.
20 | All right. It's going to take -- regardless of how I
21 | rule with respect to the breach of fiduciary duty
22 | claim, some of the claims survive, which means that
23 | defendant's going to need to respond and then I need
24 | to answer the amended complaint in this case.

25 | Mr. Melodia, how long do you think it's going to

1 take for your client's to do that?

2 MR. MELODIA: I'd ask if 30 days from your
3 Honor's ruling on the fiduciary duty?

4 THE COURT: Yes, I'm going to give that to you
5 next week. So let's just pick a date that works.

6 Mr. Barnes, 30 days, that sounds reasonable in
7 the circumstances, do you agree?

8 MR. BARNES: More than reasonable, your Honor.

9 THE COURT: So let's just say -- well, I'll give
10 you until the end of December. That works. So
11 December 31st, Mr. Melodia, you need to get your --
12 please if you would, get the answers on file, get
13 those served.

14 Then let me give you -- see if I can set you up
15 for a Rule 16 conference in this case say maybe later
16 in January? Does that work?

17 MR. MELODIA: It does.

18 MR. BARNES: Yes, your Honor.

19 THE COURT: How's the 26th look, or the 27th look
20 Ms. Brooks?

21 MR. MELODIA: We will make either work, your
22 Honor.

23 THE COURT: Are they problematic Mr. Barnes? If
24 those are problematic I can give you other dates.
25 There's no urgency to those dates?

1 MR. BARNES: I don't believe so at this point in
2 time.

3 THE COURT: Maybe move it to the first week of
4 February, is that better? I want to give --

5 MR. BARNES: I've pulled up --

6 THE COURT: -- the parties are going to need to
7 get together. You're going to get a Rule 16 order in
8 this case which is going to require you to confer,
9 come up with some -- a proposed agenda for Rule 16.
10 I just want to leave you enough time in this case to
11 do that.

12 MR. MELODIA: The first week in February would
13 work for me, your Honor if it works for Mr. Barnes.

14 THE COURT: Mr. Barnes, you get to choose --

15 MR. BARNES: I'm sorry. As soon as you give me
16 -- it will -- tell me, I can look at my calendar,
17 your Honor. I'm -- it's -- my computer is locking up
18 a little bit here.

19 THE COURT: All right.

20 MR. BARNES: Hold on.

21 THE COURT: That's okay.

22 MR. BARNES: Okay. The --

23 THE COURT: Yes, this is going to be on Zoom, so
24 no travel required.

25 MR. BARNES: -- yes. Okay. Earlier in the week

1 | is better for me, your Honor.

2 | THE COURT: All right. How about the 2nd of
3 | February?

4 | MR. MELODIA: Groundhog Day, works, your Honor.

5 | THE COURT: Mr. Barnes, February 2nd, is that
6 | early enough?

7 | MR. BARNES: Yes, your Honor.

8 | THE COURT: All right. Let's do it 2:00 p.m.
9 | please on February 2nd is going to be your Rule 16
10 | conference. Again, it will almost certainly be a
11 | Zoom folks, unless those vaccines are available in
12 | vending machines in the next eight weeks.

13 | So with that, we'll do it via Zoom on the 2nd.
14 | Again, you're going to get a notice and an order from
15 | the court that tells you what needs to be done in
16 | advance of the Rule 16. Please come with an agenda.
17 | And actually if you get that to the Court in advance
18 | that would be appreciated.

19 | Also, we'll invite you -- you're going to need to
20 | work out some tracking order dates in this case,
21 | meaning discovery deadlines; things of that nature.
22 | I ask you in this first instance to confer. We try
23 | to be pragmatic about that in this session which
24 | means we're interested in your input and what you
25 | think works in this case. So again I will give you

1 | the dates that you propose but we're very interested
2 | in what you think is reasonable in the circumstances.
3 | So please --

4 | MR. MELODIA: Your Honor, we've been cooperating
5 | already on discovery, notwithstanding the pending
6 | motions. So I suspect we'll have no problem doing
7 | that.

8 | THE COURT: Good. Okay. So I'll give you a new
9 | date for a next date for a Rule 16 conference on the
10 | 2nd of February. I will get you a decision on that
11 | one remaining count, which I think is Count Three;
12 | the breach of fiduciary duty count. I want to take a
13 | look at the case law on that. So you'll get that by
14 | next week. I'm not expecting to do anything
15 | elaborate folks, but I will give you an answer by
16 | next week.

17 | Is there anything else that we can accomplish on
18 | this case today, Counsel? No?

19 | MR. MELODIA: No, your Honor. Thank you your
20 | Honor.

21 | THE COURT: Thank you.

22 | MR. BARNES: Thank you, your Honor.

23 | THE COURT: Stay well everyone.

24 | MR. MELODIA: Thank you. You too. Have a good
25 | weekend.

1 | (Hearing ends at 3:18 p.m.)

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

C E R T I F I C A T E

I, Raymond F. Catuogno, Jr., do hereby certify that the foregoing is a true and accurate transcript, prepared to the best of my ability, of an audio recording provided to me in the matter of John Doe vs. Partners Healthcare System, Inc.

I, Raymond F. Catuogno, Jr., further certify that the foregoing is in compliance with the Administrative Office of the Trial Court Directive on Transcript Format.

I, Raymond F. Catuogno, Jr., further certify that I neither am counsel for, related to, nor employed by any of the parties to the action in which this hearing was taken, and further that I am not financially nor otherwise interested in the outcome of the action.



Raymond F. Catuogno, Jr.
November 25, 2020
9 Hammond Street
Worcester, MA 01610
raycatuogno@realtimereorting.net



The Commonwealth of Massachusetts
OFFICE OF COURT MANAGEMENT, Transcription Services

AUDIO ASSESSMENT FORM

For court transcribers: Complete this assessment form for each volume of transcript produced, and include it at the back of every original and copy transcript with the certificate page, word index, and CD PDF transcript.

TODAY'S DATE: 11/25/2020 **TRANSCRIBER NAME:** Raymond F. Catuogno, Jr.

CASE NAME: Doe v Partners Healthcare System **DOCKET NUMBER:** 1984CV01651

RECORDING DATE: 11/20/2020 **TRANSCRIPT VOLUME:** I OF I

(circle one) TYPE: **CD** TAPE QUALITY: EXCELLENT GOOD **FAIR** POOR

(circle all that apply) **ISSUES** (include time stamp):

background noise time stamp: _____

low audio _____

low audio at sidebar _____

simultaneous speech _____

cannot understand 2:05:10, 2:06:54, 2:08:38, 2:13:15, 2:13:20, 2:22:43, 2:25:30, 2:57:51, 2:58:10, 2:58:23.

other: _____ **time stamp:** _____

COMMENTS:

0

0 ----- 1
01 ----- 3
01610 ----- 67
04/15/2019 ----- 68
05 ----- 6, 68
06 ----- 8, 68
08 ----- 9, 68

1

1 ----- 1, 68
10 --- 2, 6, 48, 68
100 ----- 2
1001CR006761 --- 68
103 ----- 29
104 ----- 29, 30
11 ----- 68
11/13/2018 ----- 68
11/2 ----- 68
11/20 ----- 68
111 ----- 13, 14
12 ----- 1, 3
13 -- 1, 12, 58, 68
1323CR0284 -- 1, 68
146 ----- 38
15 ----- 12, 68
1523CR001679 --- 68
1523CR1679 ----- 1
16 - 62, 63, 64, 65
18 ----- 66
1984CV1651 ----- 3

2

2 -- 1, 3, 6, 8, 9,
12, 20, 23, 48,
64, 68
20 -- 1, 12, 23, 68
2001 ----- 23
2013 ----- 68
2014 ----- 32
2015 ----- 68
2016 ----- 68
2018 ----- 68
2019 ----- 68
2020 ---- 1, 67, 68

22-----20, 68
23-----48, 68
24-----29
25--1, 23, 29, 67,
68
26th-----62
272-----15
27th-----62
2nd-----64, 65

3

3-----66, 68
30-----23, 62, 68
327-----14, 22
38-----9, 68
31st-----62

4

40-----20
400-----13
43-----20, 68

5

5-----68
5/2-----68
5/20-----68
51-----48, 68
54-----8, 68
57-----48, 68
58-----48, 68

6

6-----68
67-----1, 13

7

74-----14

9

9-----54, 56, 67
99-----15

A

a 3, 4, 5, 7, 8, 9,
10, 11, 12, 13,
14, 15, 16, 17,
18, 19, 20, 21,
22, 23, 24, 25,
26, 27, 28, 29,
30, 31, 32, 33,
34, 35, 36, 37,
39, 40, 41, 42,
43, 44, 45, 46,
47, 48, 49, 50,
52, 53, 54, 56,
57, 58, 59, 60,
61, 62, 63, 64,
65, 67
A ----- 1, 59, 67
abet ----- 20, 21
abetting ----- 19
ability ---- 19, 67
about 7, 8, 9, 10,
11, 12, 13, 14,
15, 19, 22, 25,
30, 32, 34, 35,
37, 38, 40, 42,
46, 47, 53, 55,
56, 58, 59, 64
absolutely 13, 27,
47
absurd ----- 43
ac - 6, 21, 26, 34,
39
accept - 7, 12, 20,
22, 23, 34, 53
access ----- 9, 19
accessed ----- 13
accomplish ----- 65
according 8, 43, 57
accurate ----- 67
acknowledged --- 23
across - 6, 21, 26,
34, 39
Act 5, 16, 27, 28,
31, 54
action ----- 49, 67
actionable - 34, 42
active ----- 43
activities 26, 52,
58, 59

activity --- 25, 38
 acts ----- 56
 actual 14, 20, 25, 38
 actually -- 14, 24, 27, 30, 34, 44, 55, 57, 60, 61, 64
 Actually ----- 13
 added ----- 22
 addition 3, 23, 42, 54, 57
 address -- 5, 6, 7, 14, 16, 27, 37, 59, 61
 addresses ----- 24
 Administrative - 67
 admission ----- 59
 advance ---- 10, 64
 advertise ----- 50
 advertises ----- 57
 advertising 50, 57
 advice ----- 56
 affidavit - 20, 21, 28
 affidavits ----- 59
 after ----- 57
 aftermath ----- 59
 afternoon ---- 3, 4
 again 5, 6, 12, 19, 21, 22, 25, 28, 32, 33, 36, 40, 47, 52, 55, 56, 64
 Again -- 3, 15, 28, 32, 35, 59, 64
 against 43, 54, 57
 agenda ----- 63, 64
 ago ----- 17
 agree - 26, 39, 40, 51, 52, 62
 agreed ----- 36
 ahead --- 8, 13, 45
 aid 16, 17, 20, 21
 aiding 14, 15, 16, 17, 19, 22
 alive ----- 59
 all -- 4, 5, 6, 21, 24, 26, 31, 37, 38, 49, 50, 54, 55, 58, 59, 61, 63, 64
 All --- 4, 5, 6, 17, 32, 35, 48, 57, 58, 59, 61, 63, 64
 allegation-10, 16, 17, 22, 25, 26
 allegations-7, 12, 15, 22, 26, 32, 36, 44
 allege-11, 23, 32, 34, 36, 56
 alleged 10, 11, 14, 16, 22, 28, 31, 34, 40, 45, 54
 alleges ----- 16, 40
 allow-8, 9, 17, 18
 allowing ----- 10
 allows ----- 18, 33
 almost ----- 15, 64
 along ----- 22, 31
 already-9, 17, 23, 59, 65
 also 6, 25, 30, 34, 39, 50, 56, 60
 Also ----- 64
 alternative ----- 35
 alternatives ---- 35
 Alton ----- 2
 always ----- 7, 43
 am ----- 6, 33, 67
 Am ----- 28, 46
 ambiguous ----- 44
 amended 6, 7, 8, 9, 14, 15, 22, 29, 38, 61
 among ----- 15, 22
 amplifies ----- 57
 an 6, 7, 9, 12, 14, 15, 16, 19, 25, 27, 32, 33, 34, 36, 39, 42, 45, 46, 47, 50, 56, 58, 64, 65, 67
 An ----- 19
 analogy ----- 21, 24
 analysis ---- 39, 40
 and-3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 55, 56, 57, 58, 59, 61, 64, 67
 And 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 28, 29, 30, 31, 32, 34, 35, 36, 37, 39, 40, 41, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 58, 59, 60, 61, 64
 animal ----- 33
 anonymous ----- 27
 another 15, 19, 22, 43, 47, 49, 56, 59
 answer - 40, 61, 65
 answered ----- 55
 answers ----- 62
 any 8, 17, 21, 28, 36, 39, 40, 41, 47, 48, 53, 55, 61, 67
 anybody - 6, 9, 26, 36
 anyone ----- 59
 anything 6, 13, 17, 18, 40, 43, 48, 53, 54, 56, 59, 65
 anyway ----- 31
 anywhere ---- 9, 36
 apologize ----- 10
 app ----- 20
 appeals ----- 44
 appearance ----- 3
 APPEARANCE ----- 1

APPEARANCES -- 1, 2
 applied ----- 20
 applies ---- 27, 43
 apply - 26, 27, 48, 59, 68
 appointment 39, 41, 51
 appreciate ----- 5
 appreciated ---- 64
 approach --- 20, 48
 appropriate 38, 55
 April ----- 9
 are 4, 6, 7, 8, 9, 12, 13, 15, 17, 18, 20, 22, 23, 24, 25, 26, 27, 29, 30, 32, 36, 38, 41, 43, 44, 45, 46, 47, 48, 51, 52, 54, 55, 56, 57, 60, 61, 62, 63, 64
 Are ----- 62
 area ----- 37
 argue ----- 42
 arguing ----- 3, 4
 argument 4, 14, 22, 25, 42, 46, 50, 56
 arguments 4, 6, 15, 16, 39, 43, 44, 60
 arise ----- 56
 around 10, 20, 23, 24, 31, 59
 as - 2, 6, 7, 8, 9, 11, 13, 14, 15, 16, 19, 20, 21, 22, 23, 26, 28, 32, 35, 37, 38, 41, 44, 45, 47, 48, 49, 50, 51, 52, 56, 57, 58, 59, 60, 63
 As ----- 28, 30, 63
 aside ----- 16, 40
 ask 5, 28, 40, 62, 64
 aske ----- 5
 asked ----- 5
 asking-----31
 aspects-----7
 assessment-----68
 ASSESSMENT-----68
 assume---7, 17, 24
 assuming-----17
 attached-----54
 attaches-----51
 attachments-----5
 attendance-----4
 attending-----4
 attention-----10
 attorney/client-24
 audibly-----20
 audio-----67, 68
 Audio-----1
 authorization---41
 automatically---57
 available--25, 61, 64
 Avenue-----2
 away-----51
 45, 46, 47, 48, 49, 50, 52, 54, 55, 57, 58, 59, 61, 63, 64
 became ----- 36
 because -- 7, 8, 9, 12, 13, 14, 16, 22, 24, 30, 31, 33, 37, 45, 49, 53, 54, 57, 60
 Because 22, 27, 31, 45
 become ----- 23, 39
 becomes ----- 38
 been -- 20, 23, 24, 48, 51, 60, 65
 before - 3, 13, 14, 30, 49
 BEFORE ----- 1
 begin ----- 36
 beginning ----- 3
 behalf 3, 4, 24, 54
 behavior --- 31, 58
 behind ----- 38
 being - 23, 27, 31, 34, 36, 38, 40, 44, 45
 believe 19, 31, 63
 Believe ----- 43
 best ----- 67
 better ----- 63, 64
 between 10, 16, 18, 21, 30, 31, 34, 53
 beyond ----- 18
 bios ----- 24
 bit 39, 45, 56, 57, 63
 block ----- 13, 31
 bone ----- 14
 Boston 1, 2, 52, 57
 both - 5, 7, 18, 57
 bouncing ----- 24
 bound ----- 22, 26
 Box ----- 2
 Braintree ----- 2
 breach - 6, 24, 44, 45, 47, 49, 50, 61, 65
 breast - 11, 33, 35

B

brief ----- 45
 briefly 22, 29, 32, 58
 briefs ----- 57
 Brigham ----- 2, 47
 bring ----- 49
 bringing --- 41, 56
 broad ----- 22
 Brooks ----- 62
 browser 8, 13, 18, 30, 31
 browsers ----- 30
 bug ----- 31
 bugs ----- 32
 bulletin ----- 38
 bundled ----- 50
 business --- 36, 54
 businesses ----- 54
 but 4, 7, 8, 9, 10, 11, 12, 15, 19, 20, 23, 24, 25, 26, 27, 32, 33, 34, 36, 38, 41, 44, 45, 46, 52, 53, 54, 58, 59, 60, 65
 But -- 3, 4, 6, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 25, 26, 27, 29, 30, 33, 34, 35, 39, 40, 43, 44, 45, 47, 50, 51, 52, 53, 54, 55, 56, 57, 60
 button - 29, 30, 51
 buy ----- 22
 buying ----- 42
 By ----- 2, 59

C

C ----- 2, 67, 68
 calendar ----- 63
 call ----- 3, 10
 called 18, 21, 31, 32, 42, 50, 57
 caller ----- 50
 callers ----- 50
 Calling ----- 3

calls ----- 27, 61
 cameras ----- 4
 can 3, 7, 8, 9, 10, 11, 12, 14, 15, 17, 20, 21, 23, 24, 25, 27, 32, 35, 37, 39, 42, 43, 44, 45, 46, 47, 48, 51, 52, 53, 55, 56, 59, 61, 62, 63, 65
 Can ----- 48
 cancer -- 11, 33, 35
 cannot ----- 21, 68
 capability ----- 17
 case 3, 4, 6, 7, 8, 9, 13, 14, 16, 18, 23, 27, 30, 32, 42, 43, 44, 45, 48, 49, 52, 57, 58, 61, 62, 63, 64, 65
 CASE ----- 68
 cases 7, 8, 15, 43, 44, 45, 57
 Catuogno - 1, 67, 68
 cause ----- 49, 60
 caused ----- 31, 53
 CD ----- 68
 Center ----- 2
 certain - 37, 43, 49
 certainly -- 13, 35, 39, 64
 Certainly --- 41, 52
 certificate ----- 68
 certify ----- 67
 change ----- 37
 changes ----- 8, 60
 Chapter ----- 15, 56
 characterize 52, 56
 characterized --- 58
 characterizing -- 46
 charged ----- 26
 charges ----- 26
 charitable - 52, 57, 59
 charity ----- 57
 Chelsea ----- 4
 chief ----- 41, 49
 choice ----- 10

choose - 24, 31, 63
 Chris ----- 4
 church ----- 46
 circle -- 5, 40, 68
 circuit 8, 28, 42, 43
 circumstances - 25, 30, 34, 52, 61, 62, 65
 cite ----- 8
 cited - 15, 22, 45, 57
 cites ----- 58
 claim -- 5, 11, 14, 15, 24, 26, 32, 36, 42, 44, 47, 50, 51, 52, 54, 61
 claims -- 6, 7, 14, 15, 25, 28, 59, 61
 class ----- 14
 clear - 38, 39, 45, 59
 clearer ----- 45
 clearly ----- 49
 click -- 30, 51, 61
 clicking 23, 24, 30
 clicks ----- 24, 29
 client 23, 24, 36, 62
 clients ---- 51, 53
 clinic ----- 50
 closer ----- 52
 Clovitz ----- 4
 co ----- 21
 code 20, 30, 32, 50
 coin ----- 45
 colleague ----- 4
 colleagues ----- 4
 collected -- 27, 60
 colors ----- 42, 50
 com ----- 36, 42
 come -- 16, 43, 49, 50, 63, 64
 comfort ----- 52
 comfortable ---- 52
 COMMENTS ----- 68
 commerce -- 52, 53, 54, 56, 57

commercial ----- 58
 common ----- 47, 49
 Commonwealth 25, 68
 COMMONWEALTH ---- 1
 communicate ---- 39
 communicated --- 20
 communication - 16,
 17, 18, 19, 20,
 21, 25, 27, 28,
 29, 30, 31
 communications 14,
 16, 18, 20, 22,
 27, 29, 31
 companies ----- 21
 company ----- 51
 comparable ----- 47
 compete ----- 54
 competing ----- 37
 competition ---- 54
 complaint 6, 7, 8,
 9, 10, 13, 14,
 15, 18, 22, 26,
 28, 29, 31, 32,
 37, 40, 41, 44,
 51, 55, 61
 complaints ----- 15
 complete --- 19, 21
 Complete ----- 68
 completely - 26, 33
 completion ----- 21
 compliance ----- 67
 computer ----- 63
 conceded ----- 54
 concern ---- 12, 39
 concerned ----- 38
 concerns ----- 59
 conclude --- 11, 60
 conclusion ----- 23
 condition -- 8, 32,
 34, 37
 conditions - 27, 34
 conduct ---- 43, 57
 confer ----- 63, 64
 conference 62, 64,
 65
 confidence 41, 42,
 49
 confidential -- 12,
 25, 32, 35, 44,
 47, 60
 confidentiality-45
 configured-16, 18,
 30
 confuses -----10
 confusing-----47
 Conley-----1, 2, 3
 connect-----54
 connection-----9
 Conroy-----2
 consent-----40, 59
 consider-----18
 considered-----9
 constitute-----26
 consumer-----54
 consumers---54, 58
 contacting-----24
 contemporaneous 17,
 28
 content-21, 30, 31
 contents-----14
 contested-----45
 contesting-----45
 context 26, 27, 31,
 56, 60
 continue-----14
 continues-----21
 contract-----24
 convert-----57
 converts-----57
 conveyed---11, 12
 cookie--31, 60, 61
 cookies-9, 13, 18,
 19, 23, 31, 36
 coop-----65
 cooperating----65
 Coppola-----68
 copy-----68
 core 8, 52, 53, 55,
 56, 59
 Corp-----52, 58
 corporate---46, 49
 corporations---58
 correct-----5, 54
 Correct-----6, 11
 correctly-----46
 correlate-----33
 could--11, 36, 38,
 41, 45, 46, 47,
 57, 60
 Counsel--3, 5, 58,
 61, 65
 count --- 5, 61, 65
 Count - 14, 32, 59,
 65
 counts ----- 5, 6
 couple ----- 17, 55
 course 3, 4, 19, 47
 Court - 2, 3, 8, 9,
 13, 18, 23, 26,
 31, 38, 40, 48,
 49, 55, 56, 57,
 58, 64, 67
 COURT - 1, 3, 4, 6,
 10, 11, 13, 14,
 15, 16, 17, 18,
 19, 20, 22, 23,
 24, 26, 28, 29,
 30, 32, 33, 34,
 35, 39, 40, 41,
 43, 44, 45, 46,
 47, 48, 50, 51,
 53, 54, 55, 56,
 58, 62, 63, 64,
 65, 68
 Courtney ----- 4
 covered ---- 15, 34
 CPA ----- 58
 crack ----- 56
 create ----- 38, 43
 credentials ---- 38
 crime ----- 25
 cruising --- 11, 35
 cut ----- 6
 CVS ----- 42, 49

D

Dana 2, 35, 37, 47,
 51
 danger ----- 26
 data 30, 51, 60, 61
 date --- 61, 62, 65
 DATE ----- 68
 dates ----- 62, 64
 day ----- 37, 50
 Day ----- 64
 days --- 17, 55, 62
 deadlines ----- 64
 deal ----- 26, 44
 dealing 15, 22, 39

G

gain ---- 7, 19, 53
game ----- 7
gender ----- 27
general 24, 25, 36,
39, 59
General 2, 30, 41,
49
generalized ---- 15
get 10, 14, 17, 18,
28, 34, 35, 38,
40, 42, 51, 57,
61, 62, 63, 64,
65
gets 11, 12, 21, 30
getting ---- 6, 25
give 6, 43, 50, 51,
61, 62, 63, 64,
65
given ---- 8, 9, 45
go 10, 11, 13, 14,
18, 28, 29, 37,
41, 42, 45, 49,
52
Go ----- 53
goes --- 24, 41, 53
going 5, 6, 9, 16,
17, 22, 23, 28,
32, 36, 38, 40,
43, 44, 51, 53,
55, 59, 61, 62,
63, 64
gone ----- 5, 59
good 35, 41, 61, 65
Good ---- 3, 4, 65
Google - 8, 13, 14,
16, 21, 22, 23,
28, 33, 34, 36,
42, 43
got 5, 10, 12, 22,
25, 32, 34, 36,
40, 41, 43, 44,
45, 49, 51, 54,
55, 60
Got - 4, 19, 32, 48
grade ----- 37
graph ----- 30
grave ----- 26
great ----- 60

Groundhog ----- 64
guess ----- 55
guessing ----- 55
guilty ----- 13

H

h ----- 32, 42, 50
hack ----- 31
hacked ----- 31
had - 8, 13, 31, 43,
50, 57, 59
Hammond ----- 67
HAMPDEN ----- 1
handle ----- 38
happen ----- 28, 31
happened 15, 31, 42
happening -- 27, 33,
34, 36, 61
happens - 29, 31, 55
happy ----- 6
harm ----- 60, 61
has -- 3, 8, 11, 17,
18, 20, 21, 23,
25, 29, 35, 37,
38, 39, 44, 45,
46, 52, 58, 59
Has ----- 32
hat ----- 23, 39
have 5, 6, 7, 8, 9,
10, 11, 12, 14,
15, 16, 17, 22,
23, 24, 25, 26,
27, 28, 29, 31,
32, 34, 39, 40,
42, 43, 45, 46,
47, 51, 52, 54,
56, 59, 60, 61,
65
Have ----- 28, 65
having ----- 46
he - 21, 37, 38, 48,
57, 67, 68
head ----- 24
health -- 9, 13, 33,
34, 37
healthcare - 21, 41,
49, 53, 55
hear 3, 15, 19, 20,
48, 53, 56, 60

heard - 20, 21, 28,
30, 43
hearing 3, 16, 17,
19, 20, 28, 41,
59, 67
Hearing ----- 66
HEARING BEFORE -- 1
held ----- 8, 52
help ----- 22, 35
here 3, 4, 5, 7, 9,
10, 15, 18, 20,
21, 22, 23, 24,
26, 28, 29, 33,
34, 40, 42, 43,
45, 46, 47, 49,
51, 53, 58, 59,
63
Here ----- 32, 44
hereby ----- 67
herring ----- 39
hey ---- 32, 42, 50
highlight ----- 6
highlighting --- 37
highly ----- 48
him ----- 4
himself ----- 4
HIPAA - 13, 34, 38,
39, 40, 41, 47,
48, 50
HIPPA ----- 48, 50
his ---- 3, 38, 43
hoarding ----- 43
hold ----- 52, 53
Hold ----- 63
Holland ----- 2, 4
Hollywood ----- 4
Honor - 3, 4, 6, 7,
9, 12, 13, 15,
16, 17, 18, 20,
21, 22, 23, 26,
27, 28, 29, 30,
32, 33, 36, 38,
40, 42, 43, 45,
46, 47, 48, 49,
50, 51, 53, 54,
55, 57, 58, 62,
63, 64, 65
HONORABLE ----- 1
hospital 9, 17, 18,
21, 23, 36, 45,

46, 51
Hospital 2, 30, 57
hospitals - 33, 34,
37, 38, 46, 48,
49, 54, 57
how 12, 26, 34, 38,
46, 48, 52, 53,
56, 61
How ----- 62, 64
However - 5, 13, 28
huge ----- 34
hyperbole ----- 43

I

I 1, 3, 4, 5, 6, 7,
8, 9, 10, 11,
12, 13, 14, 15,
16, 17, 19, 20,
21, 22, 24, 25,
26, 27, 28, 29,
30, 31, 32, 33,
34, 35, 37, 39,
40, 41, 42, 43,
44, 45, 46, 47,
48, 49, 50, 51,
53, 54, 55, 56,
57, 58, 59, 60,
61, 62, 63, 64,
65, 67, 68
I know ----- 59
Iaquito ----- 4
ID ----- 8, 37
idea 14, 37, 41, 43
identical ----- 28
identifiable 7, 8,
12, 15, 33, 37,
39, 41
identified ----- 34
identifier ----- 11
identifies -- 8, 14
identify ---- 8, 33
identity ----- 25
if -- 6, 8, 10, 12,
13, 17, 18, 19,
21, 22, 23, 24,
29, 31, 33, 34,
36, 38, 41, 42,
43, 45, 47, 51,
54, 55, 57, 59,
60, 62, 63, 64
If-13, 23, 29, 35,
39, 43, 50, 62
ignore-----40
Illinois-----2
immediately----30
importance-----60
important----9, 37
importantly----37
impose-----47
impression-----43
improper-----27
in--3, 4, 6, 8, 9,
10, 11, 12, 13,
14, 15, 16, 17,
18, 19, 20, 21,
22, 23, 24, 25,
26, 27, 28, 29,
30, 31, 32, 34,
36, 37, 39, 40,
41, 42, 43, 44,
45, 46, 47, 49,
50, 52, 53, 54,
55, 56, 57, 58,
59, 61, 62, 63,
64, 67
In--3, 21, 23, 27,
37, 42, 46, 60
inapplicable----13
inaudible-6, 7, 9,
12, 20, 23, 48
Inc-----2, 67
include-----19, 68
includes-----33
including--14, 21,
23, 32, 48, 60
incorrect-----9
increase 53, 54, 56
increasing-----26
indecipherable--6,
8, 9, 12, 20,
23, 48
index-----68
indicated-----59
individual-11, 12,
14, 15, 21, 33,
34, 36, 39, 46
individualized--46
individuals-----54
inference-----12
inform ----- 35
information - 6, 8,
10, 11, 12, 13,
25, 26, 32, 33,
34, 35, 36, 38,
40, 41, 44, 45,
47, 51, 53, 60
informational - 10,
11
injunction -- 5, 9,
10, 18, 54, 59,
61
ink ----- 44
input ----- 64
inserted ----- 58
inserting ----- 15
instance --- 59, 64
Instead ----- 9, 38
institution 47, 52,
58, 59
institutions -- 48,
53, 54, 55, 57,
60
insurance ----- 27
intend ----- 5
inter ----- 33
interact ----- 55
interaction ---- 53
intercept ----- 17
intercepting 21, 31
interception -- 14,
15, 16, 17, 19,
20
interest ----- 33
interested - 4, 44,
64, 67
interesting 24, 49,
52
interference --- 32
internet 9, 15, 21,
23, 26, 42
into 6, 24, 38, 42,
58
introduce ----- 4
intruded ----- 9
intrusion ----- 32
invasion 5, 32, 33,
34, 36, 40, 44
invisible ----- 56
invite ----- 64

involve ----- 27
 involves ----- 54
 IP ----- 14, 37
 irreparable 60, 61
 is - 3, 5, 6, 7, 8,
 9, 10, 11, 12,
 13, 14, 15, 16,
 17, 18, 19, 20,
 21, 22, 23, 24,
 25, 26, 28, 29,
 30, 31, 32, 33,
 34, 35, 36, 38,
 39, 40, 41, 42,
 43, 44, 45, 46,
 47, 49, 50, 52,
 53, 54, 55, 56,
 57, 58, 59, 60,
 61, 63, 64, 65,
 67
 Is ----- 6, 28, 65
 isn 6, 11, 14, 19,
 34, 57
 issue - 10, 16, 25,
 27
 issues - 7, 27, 48,
 59
 it 4, 7, 8, 9, 10,
 11, 12, 13, 15,
 16, 17, 18, 19,
 20, 21, 22, 24,
 25, 26, 27, 28,
 29, 30, 31, 32,
 33, 34, 36, 38,
 39, 41, 43, 44,
 45, 46, 48, 49,
 50, 51, 52, 53,
 54, 55, 56, 57,
 58, 59, 61, 63,
 64, 68
 It - 4, 13, 14, 17,
 21, 23, 25, 30,
 34, 37, 38, 43,
 45, 46, 50, 51,
 53, 54, 56, 61,
 62
 italics ----- 41
 its 6, 11, 16, 19,
 30, 47, 51, 52,
 58, 59
 itself ----- 18, 58

J

J-----1, 2
 James-----2
 Jane-----2
 January-----62
 Jason-----1, 2
 Jay-----3, 4
 John-----2, 3, 67
 Johnson-----3
 Judge-----42
 judicial-----7
 jump-----6, 22, 52
 jurisdictions---22
 jus---4, 7, 8, 15,
 16, 18, 20, 22,
 26, 28, 29, 33,
 37, 39, 49, 51,
 54, 55, 58, 62,
 63
 just--4, 7, 8, 15,
 16, 18, 20, 22,
 26, 28, 29, 33,
 37, 39, 49, 51,
 54, 55, 58, 62,
 63
 Just-----57

K

keeps-----42
 kind-----4, 35, 52
 kinds-----51
 Knight-----2, 4
 know4, 11, 12, 14,
 20, 21, 26, 35,
 36, 38, 41, 47,
 50, 53, 57
 knowing-----26
 knowledge-----44
 knows-----8, 14

L

label-----22
 Lahoy-----4
 language---22, 25,
 41, 58, 60
 last-----59

later ----- 42, 62
 law 7, 21, 23, 24,
 26, 29, 34, 36,
 38, 41, 44, 47,
 48, 49, 52, 57,
 65
 lead ----- 12
 least - 15, 16, 19,
 22, 25, 44
 leave ----- 38, 63
 leaves ----- 52
 legal --- 7, 22, 25
 legally ----- 7, 8
 lends ----- 58
 let -- 4, 6, 7, 14,
 17, 20, 22, 25,
 31, 37, 40, 47,
 52, 55, 59, 62
 Let 15, 25, 28, 52,
 64
 letters - 5, 15, 59
 level -- 39, 40, 43
 liability ----- 60
 light ----- 60
 like 5, 8, 10, 11,
 13, 15, 17, 25,
 31, 33, 34, 38,
 42, 45, 50, 51,
 52, 58
 likelihood ----- 60
 likely ----- 50
 lim ----- 24
 limitations ---- 24
 line --- 41, 43, 50
 Linkage 52, 57, 58
 linked ----- 39
 list ----- 1
 listen ----- 33
 listened ----- 59
 listening ----- 16
 literally --- 9, 13
 little 45, 53, 56,
 57, 63
 ll -- 4, 6, 15, 17,
 22, 25, 32, 39,
 40, 43, 53, 60,
 62, 64, 65
 LLP ----- 2
 locking ----- 63
 log ----- 38

long --- 57, 59, 61	MASSACHUSETTS --- 1	middle ----- 17
look -- 11, 12, 14,	match --- 11, 12, 25	might - 41, 45, 51,
15, 29, 32, 51,	materials --- 5, 25	60
52, 56, 62, 63,	matter -- 3, 23, 26,	Mike ----- 3
65	32, 36, 59, 67	mind --- 11, 22, 55
Look ----- 45	may 17, 27, 36, 42,	minute ----- 43
looked 13, 22, 24,	43, 50	minutes ----- 40
60	maybe --- 40, 59, 62	misreading ----- 33
looking 11, 23, 25,	Maybe --- 35, 54, 63	missed ----- 24
35, 53	me -- 3, 4, 5, 6, 7,	missing ----- 28
looks ----- 15, 24	10, 12, 14, 15,	mistake ----- 48
lot ----- 44, 59	17, 20, 22, 25,	Mitchell ----- 3
low ----- 68	26, 28, 33, 35,	mixed ----- 49
luddite ----- 20	40, 43, 44, 45,	Mm ----- 4, 40
	47, 48, 52, 55,	modulate ----- 10
	56, 58, 59, 61,	moment - 8, 10, 16,
	62, 63, 64, 67	17, 19, 24, 28,
	mean -- 12, 20, 21,	33, 43, 55
	27, 38, 47, 49,	money ----- 57
	57, 60	months ----- 8
	meaning ----- 64	moots ----- 59
	means -- 31, 58, 61,	more -- 10, 25, 37,
	64	40, 53, 55, 56
	measures ----- 13	More ----- 62
	meat ----- 14	most 7, 30, 45, 52
	medical 11, 27, 32,	mostly ----- 15
	34, 37, 40, 44,	motions ---- 18, 65
	45, 47	move ----- 15, 63
	medications ---- 27	moving ----- 6, 43
	meet ----- 48	Mr 1, 3, 4, 6, 10,
	Melodia 1, 2, 4, 6,	14, 17, 18, 19,
	10, 14, 17, 18,	22, 24, 27, 28,
	19, 22, 24, 28,	29, 30, 31, 32,
	29, 30, 31, 32,	33, 37, 40, 42,
	33, 40, 42, 43,	43, 44, 46, 48,
	44, 46, 50, 52,	50, 51, 52, 56,
	56, 61, 62	57, 58, 60, 61,
	Melrose ----- 57	62, 63, 64
	member ----- 14, 37	MR 3, 4, 6, 7, 10,
	memorandum ----- 58	11, 12, 13, 14,
	mention - 25, 36, 60	15, 16, 17, 18,
	mentioned 9, 37, 49	19, 20, 22, 23,
	merely ----- 23	26, 28, 29, 30,
	merits ----- 7	33, 34, 35, 36,
	message ----- 57	39, 40, 41, 43,
	methods ----- 54	44, 45, 46, 47,
	MGH 11, 16, 31, 35,	48, 49, 50, 51,
	47	53, 54, 55, 56,
	microphone ----- 68	57, 58, 62, 63,
	microphones ----- 4	64, 65

M

MA ----- 67
machine ----- 8
machines ----- 64
macro ----- 39
made -- 15, 25, 41,
50, 57, 60
main ----- 27
maintain ----- 45
make 7, 13, 24, 27,
30, 39, 58, 60,
62
makes - 25, 29, 38,
57, 58
making 15, 42, 50,
56, 58
malpractice ---- 24
MANAGEMENT ----- 68
many ----- 46
margin ----- 57
Mark ----- 1, 2, 4
marketing - 41, 49,
50, 53, 54, 56
marketplace ---- 58
markets ----- 57
MARONEY ----- 4
Mason ----- 42
Mass 6, 22, 30, 36,
40, 45, 48, 49,
52
Massachusetts 1, 2,
5, 7, 15, 16,
28, 29, 31, 35,
44, 49, 54, 68

Ms -----	62	53, 54, 58, 60,	on - 1, 3, 4, 5, 6,
much ---	14, 39, 40	61, 65, 67	7, 9, 10, 11,
mundane -----	40	Not 10, 33, 36, 38,	14, 15, 16, 18,
mute -----	6, 10	42, 44	21, 23, 24, 25,
N			
NA -----	68	note ---	3, 4, 5, 18
name 3, 27, 38, 49		noted -----	41
NAME -----	68	notes -----	50
named -----	13, 14	nothing -----	14, 30
narrow -----	56	notice --	7, 13, 38,
nature -----	59, 64	41, 59, 64	
necessarily --	4, 5	notices -----	61
need - 5, 7, 9, 12,		notion -----	52
17, 26, 40, 42,		notwithstanding	14,
52, 53, 61, 62,		65	
63, 64		November -----	1, 67
needed -----	4	now -----	17, 55, 61
needs 8, 16, 28, 64		NPP -----	13, 38, 43
negate -----	51	number ---	4, 8, 16,
negligence -----	47	17, 18, 19, 20,	
neither 20, 21, 67		21, 25, 28, 37,	
never -- 33, 41, 53		41, 49, 51	
new -----	38, 65	Number -----	12
next -- 20, 21, 61,		NUMBER -----	68
62, 64, 65		numbers --	8, 24, 50
nine -----	45	O	
ninth -----	28, 42	o ---	12, 33, 55, 67
No 1, 3, 6, 16, 20,		objection -----	17
24, 39, 55, 65		obligation -	44, 45,
Nobel -----	37	46, 47, 52	
nobody -----	45	obligations -----	48
Nobody -----	33	obvious -----	9
noise -----	68	occur -----	18
nondisclosure --	60	occurs -----	21
None -----	39	OCR -----	13, 43
Nonetheless ----	20	odd -----	45
nonprofit -- 54, 58		OF -----	1, 68
nonprofits -----	57	off -----	4, 50
nor ---- 20, 38, 67		Off -----	2, 67
not 3, 4, 6, 7, 8,		offensive -----	10
9, 11, 12, 13,		offered -----	38, 57
15, 16, 17, 18,		Office -----	2, 67
19, 20, 21, 22,		OFFICE -----	68
24, 26, 29, 30,		officer -----	41, 49
31, 33, 34, 35,		officially ---	5, 6
36, 38, 39, 41,		Okay - 3, 6, 14, 22,	
42, 44, 45, 46,		28, 29, 34, 39,	
47, 49, 51, 52,		42, 43, 49, 50,	
		58, 63, 65	
			oncologist ----
			50
			one - 8, 9, 10, 11,
			12, 13, 15, 16,
			17, 18, 20, 21,
			22, 24, 27, 28,
			29, 32, 33, 37,
			40, 43, 44, 45,
			47, 49, 50, 51,
			52, 57, 58, 65,
			68
			One 2, 10, 14, 15,
			17, 18, 32
			ones -----
			50
			ongoing -----
			17
			only -- 10, 13, 28,
			30, 43, 46, 58
			onto -----
			36
			operator -----
			36
			opinion -----
			51
			opportunity ----
			6
			opposed ----
			15, 20
			opposite ---
			45, 50
			opposition ----
			54
			or 6, 8, 9, 11, 12,
			13, 15, 16, 17,
			19, 20, 21, 24,
			26, 27, 28, 29,
			30, 32, 33, 36,
			38, 42, 44, 45,
			46, 47, 49, 51,
			52, 53, 54, 55,
			56, 57, 59, 62,
			64, 67, 68
			order 5, 9, 63, 64
			organization 46, 52
			organizations - 47,
			53, 57
			organized -----
			25

original ----- 68	participated----59	physician - 45, 46,
other - 14, 15, 21,	particular-11, 23,	47
22, 30, 35, 40,	25, 31, 33, 36,	physicians - 44, 48
42, 48, 50, 53,	37	pick ----- 62
54, 56, 57, 59,	particularly----17	picked ----- 14, 44
60, 62, 68	parties32, 34, 40,	piece -- 16, 22, 30
others - 14, 16, 22	44, 60, 63, 67	PII ----- 27
otherwise -- 28, 67	parts-----7	pile ----- 12
ought ----- 26	party--16, 17, 18,	pixel ----- 30
our10, 26, 34, 45,	19, 21, 27, 28,	pixels ----- 23
50, 56, 57, 59	50	place ----- 40, 49
out28, 31, 33, 37,	pass-----8, 21	places ----- 22, 38
38, 54, 57, 58,	passing-----17	plaintiff 3, 5, 6,
64	password-----39	8, 10, 14, 18,
outcome ----- 67	past -----54	21, 22, 26, 30,
outlined ----- 49	path-----31	32, 34, 35, 41,
outright ----- 43	patient-8, 10, 12,	43, 46, 59, 60
outset ----- 37	29, 30, 31, 32,	Plaintiff ----- 1
over5, 13, 21, 27,	35, 36, 38, 40,	plaintiffs - 3, 11,
37	41, 44, 45, 46,	13, 14, 15, 22,
overcome ----- 13	47, 51, 54	23, 27, 33, 34,
overlooked ----- 28	patients---11, 16,	42, 43, 57, 60
owe ----- 46	23, 40, 41, 47,	play --- 39, 40, 58
own 8, 11, 14, 40,	50, 53, 54, 56	plead ----- 13
49, 59	pattern-----49	pleading12, 13, 23
	Pause-----10	pleadings ----- 15
	PDF-----68	please - 3, 62, 64,
	pending-----65	65
	people--8, 13, 14,	Please ----- 64
	15, 23, 26, 31,	pled ---- 7, 28, 51
	33, 35, 37, 46,	point 6, 8, 12, 16,
	50, 53, 55	27, 28, 29, 33,
	perhaps-11, 12, 33	34, 40, 45, 51,
	Perhaps-----6	52, 55, 56, 57,
	permit-----19	58, 63
	person---7, 8, 11,	pointed ----- 38
	14, 16, 24, 32,	points ----- 10
	36, 41, 51, 55	policies ----- 9
	personal---10, 35,	policy ----- 13, 38
	37, 40, 41, 45,	pop ----- 41
	46, 48	portal - 10, 38, 51
	personally-12, 33,	portals ----- 9, 40
	41	positives ----- 51
	persuaded---22, 39	possibility ---- 12
	pharmaceutical--50	possible --- 10, 19
	pharmacy-----39	possibly ----- 35
	phone3, 24, 31, 50	post ----- 18, 19
	phonetic-----45	potential - 35, 47,
	PHR-----39	49, 61
	physical-----8	potentially25, 45,

P

p ----- 3, 64, 66
pa ----- 68
page 9, 11, 13, 14,
37, 58, 68
Page ----- 1
PAGE ----- 2
Pages ----- 1
paid ----- 38
paper ----- 15, 37
papers 5, 6, 7, 14,
16, 54, 60
Paragraph -- 14, 49
paragraphs - 13, 29
parcel ----- 55
parent ----- 38
parental ----- 38
Parenthood ----- 58
parishioner ---- 45
part -- 14, 18, 21,
41, 44, 47, 52,
53, 55, 57, 59
Part ----- 53

50		
practice ---	38, 54	
practices --	13, 56	
pragmatic --	40, 64	
preamble -----	25	
precise ----	30, 58	
preliminary -	5, 9, 10, 17, 54, 59, 61	
prepared ----	1, 67	
presence -----	3	
present ----	3, 48	
presented -----	61	
presents -----	32	
press -----	51	
pretty -----	44	
prevent -----	42	
previous -----	41	
priest -----	45	
primarily -----	59	
primary -----	51	
principle -----	39	
privacy	5, 7, 8, 9, 13, 32, 33, 34, 36, 38, 40, 42, 43, 44, 48, 61	
private -----	9	
privilege -----	24	
probability ----	12	
probable -----	12	
probably	44, 55, 60	
problem	24, 47, 59, 65	
problematic ----	62	
problems -----	26	
produced -----	68	
products -----	36	
profession -----	39	
profit -	53, 54, 57	
profits -----	58	
prohibits -----	16	
prologue -----	25	
prominently ----	38	
promise ----	39, 43	
proper ----	18, 58	
properly ----	7, 9	
properties -----	41	
property -----	30	
propose -----	65	
proposed -----	63	
propriatorship--	46	
prospective-----	59	
protect	31, 43, 54, 58	
protectable-----	39	
protected--	10, 13, 34, 37, 38	
protection-----	38	
protective-----	13	
protects-----	41	
provide-	29, 53, 55	
provided----	41, 67	
provider	35, 41, 49	
providers---	11, 35	
providing-----	9	
public--	9, 23, 26, 34, 36, 39, 42, 50, 57	
publicly-----	35	
pull----	11, 25, 52	
pulled-----	15, 63	
purportedly-----	56	
purpose-----	56	
purposes---	12, 16, 24, 40, 41, 58	
pursuing-----	54	
put-	11, 30, 38, 50	
puts-----	30	
Q		
qualify-----	16, 19	
QUALITY-----	68	
question---	32, 40, 47, 55	
questions-----	7	
quickly-----	44, 61	
quote-----	49, 58	
R		
R-----	67	
ra-----	52	
raised-----	52	
ran-----	24	
random-----	8, 50	
Rather-----	46	
Raymond--	1, 67, 68	
re---	5, 6, 11, 12, 13, 16, 17, 19, 20, 21, 22, 23, 24, 27, 30, 31, 32, 33, 34, 35, 36, 38, 40, 41, 43, 44, 45, 46, 47, 49, 51, 52, 53, 54, 55, 56, 58, 60, 63, 64	
reach -----	40	
read -	5, 6, 7, 14, 16, 20, 25, 44, 52, 59	
real ---	12, 27, 36	
realistically --	26	
reality -----	46	
really	6, 7, 8, 10, 15, 20, 25, 28, 34, 37, 39, 48, 49, 53, 59	
reason	30, 35, 39, 45, 53	
reasonable -	62, 65	
reasons -	6, 7, 49, 61	
rec	16, 17, 20, 22, 28, 31, 67	
recall -----	10	
received -----	5	
receives -----	30	
recited -----	60	
recognize --	6, 10, 11, 26, 44, 45, 49	
recognized -	44, 48	
recognizes -----	52	
recognizing -----	6	
record -	3, 14, 15, 20	
recorded	20, 21, 28	
Recording -----	1	
RECORDING -----	68	
records -----	9, 38	
red -----	39	
redirections ---	31	
redirects -----	30	
reduce -----	4	
ref -----	9, 60	
refer -----	11	
reference ---	9, 60	

40, 45, 52, 56,	68	60, 61
61, 62, 65	That-7, 9, 10, 15,	them --17, 28, 29,
taken ----- 67	17, 22, 24, 29,	35, 36, 41, 51,
takes ----- 25	30, 32, 34, 35,	55, 61
taking 12, 18, 20,	37, 42, 44, 45,	themselves -7, 13,
39, 56, 57	48, 49, 52, 53,	61
talk13, 15, 22, 55	54, 55, 56, 58,	Then ----- 5, 62
talked ----- 32	60, 62, 63	theory -- 8, 21, 27
talking 8, 11, 19,	that I---5, 6, 17,	there 6, 7, 9, 10,
30, 34, 40, 42,	39, 40, 42, 54,	12, 13, 14, 15,
46, 53, 55	59, 60, 61, 67	16, 18, 20, 21,
talks ----- 9, 47	the-1, 2, 3, 4, 5,	22, 25, 26, 28,
TAPE ----- 68	6, 7, 8, 9, 10,	29, 31, 34, 35,
targeted ----- 26	11, 12, 13, 14,	38, 40, 41, 42,
technically 8, 26,	15, 16, 17, 18,	46, 47, 49, 50,
46, 48	19, 20, 21, 22,	52, 54, 57, 58,
technological -- 21	23, 24, 25, 26,	59, 65
technology 31, 34,	28, 29, 30, 31,	There -- 7, 16, 23,
49	32, 33, 34, 35,	27, 28, 43, 46,
telephone ----- 31	36, 37, 39, 40,	47, 50, 54, 55,
tell -- 13, 24, 37,	41, 42, 43, 44,	57, 62
39, 63	45, 46, 47, 48,	therefore --- 9, 12
telling ----- 36	49, 50, 52, 53,	these -- 9, 12, 14,
tells ----- 64	54, 55, 56, 57,	15, 16, 20, 23,
Teresa ----- 4	58, 59, 60, 61,	27, 28, 34, 38,
term ----- 37	62, 63, 64, 65,	39, 41, 43, 48,
terms -- 8, 12, 15,	67, 68	49, 50, 52, 53,
34, 46, 48	The---2, 7, 9, 16,	54, 55, 56, 57,
test ----- 49	17, 21, 22, 23,	59
testing ----- 7	25, 29, 32, 33,	These -- 20, 23, 38
text ----- 30	42, 43, 45, 49,	They -- 11, 13, 18,
than -- 22, 45, 48,	63, 68	21, 23, 24, 27,
55, 59, 62	THE1, 3, 4, 6, 10,	31, 34, 35, 36,
Thank -- 5, 11, 18,	11, 13, 14, 15,	42, 44, 47
32, 43, 65	16, 17, 18, 19,	thing -10, 13, 42,
that 4, 5, 6, 7, 8,	20, 22, 23, 24,	43, 47, 50, 51
9, 10, 11, 12,	26, 28, 29, 30,	things -- 6, 7, 15,
13, 14, 15, 16,	32, 33, 34, 35,	27, 51, 64
17, 18, 19, 20,	39, 40, 41, 43,	think -5, 6, 7, 9,
21, 22, 23, 24,	44, 45, 46, 47,	10, 11, 22, 26,
25, 26, 28, 29,	48, 50, 51, 53,	27, 28, 31, 32,
30, 31, 32, 33,	54, 55, 56, 58,	36, 39, 40, 41,
34, 35, 36, 37,	62, 63, 64, 65	42, 44, 45, 46,
39, 40, 41, 42,	THE CLERK-----3	47, 48, 49, 50,
43, 44, 45, 46,	their7, 8, 13, 14,	51, 54, 55, 56,
47, 48, 49, 50,	15, 16, 18, 19,	57, 58, 59, 60,
51, 52, 53, 54,	25, 27, 31, 32,	61, 64, 65
55, 56, 57, 58,	35, 36, 40, 41,	third -- 8, 16, 17,
59, 60, 61, 62,	43, 44, 47, 48,	18, 21, 28, 32,
63, 64, 65, 67,	53, 54, 55, 56,	40, 43, 44, 50,

60
Third ----- 9
this -- 4, 6, 7, 8,
10, 11, 12, 13,
14, 15, 16, 20,
21, 22, 23, 25,
26, 27, 30, 31,
32, 34, 36, 37,
39, 40, 41, 44,
45, 49, 50, 51,
53, 54, 55, 56,
57, 59, 61, 62,
63, 64, 65, 67,
68
This 3, 11, 20, 26,
38, 41, 43
those - 4, 5, 6, 8,
12, 13, 25, 33,
34, 36, 41, 42,
43, 44, 45, 51,
54, 56, 60, 61,
62, 64
Those -- 24, 51, 57
though ----- 20, 56
three ----- 9, 37
Three ----- 65
through 5, 11, 19,
28, 39, 40
time 6, 8, 10, 12,
15, 24, 26, 29,
37, 40, 41, 45,
63, 68
times ----- 41, 46
timing ----- 27
to - 3, 4, 5, 6, 7,
8, 9, 10, 11,
12, 13, 14, 15,
16, 17, 18, 19,
20, 22, 23, 24,
25, 26, 28, 29,
30, 31, 32, 34,
35, 36, 37, 39,
40, 41, 42, 43,
44, 45, 46, 47,
48, 49, 50, 51,
52, 53, 54, 55,
56, 57, 58, 59,
60, 61, 62, 63,
64, 65, 67
To ----- 18, 20

today 5, 18, 36, 65
together ---- 11, 63
too ----- 65
took ---- 13, 14, 50
tool ----- 57
tools --- 53, 54, 56
top ----- 29, 30
topics ----- 50
towards ----- 26
trace ----- 35
tracking --- 23, 30,
31, 36, 64
trade --- 52, 53, 57
traditional ---- 31
TRANSCRIBER ---- 68
transcribers --- 68
transcript -- 67, 68
TRANSCRIPT ---- 68
Transcription --- 68
transit ----- 16
transmission 21, 30
transmitted ---- 34
travel ----- 63
treatment --- 35, 50
Trial ----- 67
tried ----- 18, 31
true - 7, 8, 12, 13,
21, 22, 23, 26,
28, 30, 34, 36,
43, 58, 67
truly ----- 39
trust -- 24, 41, 42,
49
truth ----- 7
trying -- 13, 34, 47
turn ----- 4
two 13, 14, 15, 16,
18, 19, 21, 29,
40, 57
tying ----- 43
type ----- 25
TYPE ----- 68
types --- 27, 38, 48

U

Ultimately ----- 52
under --- 7, 13, 26,
36, 44, 47, 56,
57

undermine ----- 60
understand 12, 25,
33, 34, 41, 48,
68
understanding - 44,
61
understood ----- 59
Understood ----- 26
undertake ----- 39
undertakes - 52, 59
unfair ----- 54, 56
unfortunately -- 10
unless ----- 10, 64
unreasonable 32, 33
until ----- 62
unusual ----- 11
unwieldy ----- 49
up - 8, 14, 18, 24,
25, 29, 30, 31,
41, 43, 44, 49,
50, 52, 60, 62,
63
upon 9, 12, 18, 27,
30
urgency ----- 62
URL ----- 39
URLs ----- 34
us 13, 27, 37, 43,
49
use 9, 23, 34, 40,
41, 53
used 8, 36, 51, 56,
61
useful ----- 12
user -- 25, 31, 33,
36, 38, 60
users ----- 36, 59
using -- 8, 21, 23,
24, 26

V

v ----- 1, 68
V ----- 1
vaccines ----- 64
various ---- 15, 59
ve 5, 6, 9, 12, 17,
18, 22, 24, 31,
32, 34, 36, 40,
41, 43, 44, 45,

51, 54, 55, 61,
 63, 65
 vending ----- 64
 version ----- 34
 versus - 3, 42, 44,
 49, 52
 very -- 35, 44, 57,
 58, 59, 61, 65
 Very ----- 58
 VI ----- 1
 via ----- 55, 64
 viability ----- 7
 viable -- 7, 26, 44
 victim ----- 31
 violation ----- 25
 Virginia ----- 42
 virtually ----- 39
 virtue ----- 23
 visited ----- 23
 visitor - 8, 18, 21
 visits ----- 36
 Volume ----- 1
 VOLUME ----- 68
 voracity ----- 7
 vs ----- 67

W

w -- 9, 10, 11, 13,
 17, 18, 19, 21,
 23, 24, 27, 30,
 31, 34, 35, 36,
 38, 40, 51, 53,
 55
 wait ----- 55
 waiting ----- 11
 Wakefield ----- 57
 walk ----- 38
 walking ----- 48
 walks ----- 38
 want 3, 6, 13, 22,
 29, 35, 37, 40,
 42, 50, 51, 54,
 56, 63, 65
 wanted ----- 14, 55
 wants ----- 30, 37
 warning ----- 53
 wary ----- 42
 was 14, 15, 22, 24,
 26, 27, 28, 33,
 37, 42, 43, 44,
 49, 51, 54, 57,
 58, 59, 67
 way -- 8, 9, 10, 11,
 12, 16, 17, 18,
 20, 21, 23, 30,
 31, 32, 33, 34,
 36, 38, 45, 46,
 48, 53, 56, 58,
 59
 we - 5, 7, 8, 9, 11,
 13, 14, 15, 17,
 18, 19, 20, 22,
 25, 27, 30, 31,
 33, 35, 40, 41,
 43, 44, 45, 47,
 49, 50, 53, 54,
 55, 64, 65
 We --- 5, 7, 12, 17,
 32, 40, 44, 45,
 47, 53, 61, 62,
 64
 web - 8, 30, 32, 41,
 50
 WebMD ----- 36
 website - 9, 10, 11,
 13, 17, 18, 19,
 21, 23, 24, 27,
 30, 31, 34, 35,
 36, 38, 40, 51,
 53, 55
 websites - 7, 9, 11,
 16, 23, 35, 36,
 38, 42, 52, 53,
 55, 56, 59, 61
 week 61, 62, 63, 65
 weekend ----- 65
 weeks ----- 64
 Welcome ----- 3
 welfare ----- 26
 well - 6, 7, 13, 23,
 28, 29, 32, 42,
 44, 47, 52, 55,
 60, 62, 65
 Well --- 13, 17, 29,
 33, 34, 40, 42,
 46, 49, 53
 went ----- 22, 36
 were - 5, 9, 13, 15,
 22, 34, 39, 50,
 57
 what 5, 7, 10, 11,
 14, 15, 16, 18,
 22, 25, 26, 27,
 28, 29, 31, 32,
 33, 34, 35, 37,
 38, 40, 43, 44,
 45, 46, 47, 50,
 51, 53, 54, 55,
 56, 57, 58, 61,
 64
 What -- 11, 31, 33,
 48, 56
 whatsoever ----- 27
 when -- 26, 32, 36,
 41, 43, 46, 47,
 51, 52, 53, 56,
 58, 59
 When ----- 29, 49
 where - 22, 23, 28,
 30, 31, 39, 40,
 46, 51, 57, 58
 Where ----- 38
 whether 12, 13, 22,
 32, 36, 39, 52,
 59
 Whether ----- 26
 which - 5, 7, 8, 9,
 10, 11, 13, 14,
 15, 20, 22, 23,
 24, 27, 34, 36,
 38, 40, 42, 43,
 49, 51, 55, 56,
 61, 63, 64, 65,
 67
 Which ----- 22, 39
 while ----- 16
 white ----- 15
 who - 3, 4, 11, 13,
 23, 24, 26, 35,
 37, 38, 40, 50,
 53, 59
 whole ----- 21, 43
 will 3, 4, 26, 35,
 52, 61, 62, 63,
 64, 65
 win ----- 22
 wire --- 14, 15, 22
 wiretap 5, 14, 15,
 20, 22, 23, 25,

26, 27, 31, 32
 wish ---- 6, 35, 41
 wit ----- 25
 with 3, 5, 6, 7, 8,
 9, 11, 12, 13,
 14, 15, 17, 22,
 24, 26, 32, 34,
 35, 36, 38, 39,
 40, 41, 43, 44,
 45, 46, 51, 52,
 53, 55, 59, 60,
 61, 63, 64, 67,
 68
 within ----- 25
 without ---- 41, 44
 won ----- 37, 57
 Worcester ----- 67
 word 23, 28, 34, 68
 words - 21, 41, 42,
 43
 work --- 62, 63, 64
 work -- 62, 63, 64
 works - 21, 23, 26,
 34, 62, 63, 64
 world --- 9, 36, 39
 worry ----- 5
 worse ----- 43
 would 4, 6, 8, 12,
 18, 19, 25, 31,
 33, 34, 39, 40,
 41, 45, 48, 49,
 50, 52, 54, 58,
 62, 63, 64
 Would ----- 11
 wrestling -- 52, 53
 written ---- 41, 59
 wrong ----- 36

14, 15, 16, 17,
 18, 20, 21, 22,
 24, 26, 27, 28,
 29, 31, 32, 33,
 35, 37, 38, 39,
 40, 41, 42, 43,
 45, 46, 47, 48,
 49, 50, 51, 52,
 53, 54, 55, 56,
 57, 60, 61, 62,
 63, 64, 65
 You - 3, 12, 17, 19,
 21, 25, 30, 38,
 46, 47, 52, 53,
 54, 57, 61, 63,
 65
 your 3, 4, 6, 7, 9,
 10, 12, 13, 14,
 15, 16, 17, 18,
 20, 21, 22, 23,
 26, 27, 28, 29,
 30, 32, 33, 35,
 36, 38, 40, 41,
 42, 43, 45, 46,
 47, 48, 49, 50,
 51, 53, 54, 55,
 57, 59, 62, 63,
 64, 65
 Your 3, 17, 29, 43,
 58, 65

Y

years ----- 20, 23
 yes 19, 20, 26, 29,
 44, 58, 63
 Yes - 3, 7, 15, 17,
 18, 29, 41, 44,
 47, 50, 55, 56,
 58, 62, 63, 64
 yet ---- 25, 39, 48
 you 3, 4, 5, 6, 8,
 9, 10, 11, 12,

Handwritten signature

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION
NO. 11-2808-BLS1

OFFICE SET
01.17.12
C.G.K.
K.L.B.
R.C.I.
F.R. 2
J.P. 2
J.A.
C.H.P.
H.G.R.
W.S.

DEBRA L. MARQUIS

v.

GOOGLE INC.

MEMORANDUM OF DECISION AND ORDER ON
DEFENDANT GOOGLE INC.'S MOTION TO DISMISS

(145)

This action arises from the alleged monitoring of emails by defendant Google Inc. ("Google") in order to sell advertisements based on keywords that appear in those emails. Google operates Gmail, which is an electronic communications or email service. The plaintiff, Debra L. Marquis, represents a putative class of Massachusetts residents who have non-Gmail email accounts, but who exchange emails with Gmail users. Marquis alleges that Google's monitoring of emails sent from non-Gmail email accounts violates the Massachusetts wiretap statute, G.L. c. 272, § 99.

Google has now moved to dismiss this action on the grounds that the wiretap statute does not apply to email communications or to its conduct. For the reasons discussed below, Google's motion to dismiss is denied.

BACKGROUND

The court takes as true all well-pled factual allegation set forth in Marquis's Complaint, see *Marshall v. Stratus Pharms., Inc.*, 51 Mass. App. Ct. 667, 670-71 (2001). Marquis is a Massachusetts resident who has a non-Gmail email account.

Add. 063

Compl. ¶ 3. Google is a Delaware corporation with its principal place of business in California. Compl. ¶ 4. It operates Gmail, which is an electronic communication service that is free to its users. Compl. ¶¶ 6-8. While Google does not charge Gmail account holders for using its service, Google generates revenue through advertisements that it presents to Gmail users. Compl. ¶ 8. Google intercepts and scans emails sent from non-Gmail users, such as Marquis, in order to find keywords or content in the emails that will enable it to target advertisements specifically at Gmail users. Compl. ¶ 9. Once targeting individual emails, Google now focuses on numerous emails to find keywords. Compl. ¶ 11. This system is known as "interest-based advertising." Compl. ¶ 11.

Marquis has an America-On-Line ("AOL") email account that she has used since the late 1990s. Compl. ¶ 13. While she routinely exchanged emails with Gmail users, Marquis did not consent to Google's secret interception, disclosure, or scanning of her emails. Compl. ¶¶ 12, 14. Marquis seeks to represent a class of Massachusetts residents who have non-Gmail email accounts and who exchange emails with Gmail users, and who have their emails intercepted and/or scanned without their consent. Compl. ¶ 15.

Marquis alleges that Google's conduct violates the Massachusetts Wiretap statute, G.L. c. 272, § 99. The statute "was enacted to give due protection to the privacy of individuals by barring the secret use of electronic surveillance devices for

eavesdropping purpose” *Dillon v. Massachusetts Bay Transp. Auth.*, 49 Mass. App. Ct. 309, 310 (2000). It prohibits any person from intercepting or attempting to intercept “any wire or oral communication.” G. L. c. 272, § 99(C)(1). A wire communication is defined as “any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception.” *Id.* at § 99(B)(1). An intercepting device does not include “any telephone or telegraph instrument, equipment facility, or a component thereof . . . being used by a communications common carrier in the ordinary course of business.” *Id.* at § 99(B)(3).

Google has now moved to dismiss the Complaint. First, it contends that the Massachusetts wiretap statute does not apply to electronic communications, and if it does, then it is preempted by the federal wiretap statute. Second, it argues that Marquis was aware that Google intercepted and scanned her emails, and the statute requires that the interception be done secretly. Third, Google’s alleged interception occurred in the ordinary course of business and is therefore exempted from the statute.

DISCUSSION

In order to withstand a motion to dismiss, a plaintiff’s complaint must contain “allegations plausibly suggesting (not merely consistent with) an entitlement to relief,

in order to reflect [a] threshold requirement . . . that the plain statement possess enough heft to sho[w] that the pleader is entitled to relief." *Iannacchino v. Ford Motor Co.*, 451 Mass. 623, 636 (2008), quoting *Bell Atl. Corp. v. Twombly*, 127 S. Ct. 1955, 1966 (2007) (internal quotations omitted). While a complaint need not set forth detailed factual allegations, the plaintiff is required to present more than labels and conclusions, and must raise a right to relief "above the speculative level . . . [based] on the assumption that all the allegations in the complaint are true (even if doubtful in fact)." *Id.* See also *Harvard Crimson, Inc. v. President & Fellows of Harvard Coll.*, 445 Mass. 745, 749 (2006). The court will examine the Complaint under this standard.

Google's first argument is that the Massachusetts wiretap statute does not include a prohibition against monitoring emails. In essence, it contends that had the Legislature desired to include such electronic communications in the statute, then it would have done so expressly.¹ The Massachusetts wiretap statute was originally intended to mirror its federal counterpart. See *O'Sullivan v. NYNEX Corp.*, 426 Mass. 261, 264 (n.5) (1997). In 1986, the federal statute was "recognized to be hopelessly out of date," and it was amended by the Electronic Communications Privacy Act ("ECPA") in order to cover "electronic communication," which encompasses email. *Dillon*, 49 Mass. App. Ct. at 314-15 (citations omitted); 18

¹ Google presents G.L. c. 276, § 1B, which expressly defines "electronic communication services" and "remote computing services," as one such example. In contrast, the Massachusetts wiretap statute does not define these terms.

U.S.C. § 2510(12). The Massachusetts Legislature did not provide for a similar amendment. However, “the fact that there has been no amendment of the Massachusetts statute comparable to the Congressional action of 1986 does not bar us from reading [an exception] so as to preserve it in its intrinsic intended scope and maintain its viability in the broad run of cases.” *Dillon*, 49 Mass. App. Ct. at 315.

This court declines to accept Google’s contention that the Massachusetts wiretap statute does not prohibit the secret interception of emails. First, the statute’s definition of “wire communications” is sufficiently broad to include electronic communications, as it includes “the aid of wire, cable, or *other like connection* between the point of origin and the point of reception.” G.L. c. 272, § 99(B)(1) (emphasis supplied). Permitting the interception of private emails, while prohibiting the same conduct for oral telephone conversations, is an inconsistency that contravenes the purpose of the statute. Second, a Massachusetts court has recently held that the Massachusetts wiretap statute cover email, and the court finds its reasoning persuasive. See *Rich v. Rich*, 2011 WL 3672059, *5 (Mass. Super. July 8, 2011) (McGuire, J.).

At this stage of the litigation, the court must accept the factual allegations of the Complaint. Marquis alleges that Google intercepts and scans private emails that she sends from her AOL account to Gmail account users, and that she did not consent to Google’s interception. Compl. ¶¶ 9, 13-14. This alleged conduct violates

the Massachusetts wiretap statute.

Google's second argument is that federal law preempts the Massachusetts wiretap statute. Federal law may preempt state law "when it explicitly or by implication defines such an intent, or when a State statute actually conflicts with Federal law or stands as an obstacle to the accomplishment of Federal objectives. Whether a Federal statute preempts State law is ultimately a question of Congress's intent." *City of Boston v. Commonwealth Employment Relations Bd.*, 453 Mass. 389, 396 (2009) (internal citations omitted). A court should be hesitant to find preemption, as "[u]nless Congress's intent to do so is clearly manifested, a court does not presume that Congress intended to displace State law on a particular subject. . . ." *Id.*

Prior to the 1986 amendments to the federal wiretap statute, the Supreme Judicial Court determined that the federal statute did not preempt the Massachusetts wiretap statute. See *Commonwealth v. Vitello*, 367 Mass. 224, 249-53 (1975). Google maintains that the ECPA's comprehensive regulatory scheme indicates Congress's intent to occupy the field. However, this is insufficient to warrant a finding that the federal wiretap statute preempts the Massachusetts wiretap statute. The ECPA does not contain language expressly, or by implication, preempting state law. See 18 U.S.C. §§ 2510-2522. In addition, the ECPA does not occupy the entire field of interception of electronic surveillance, as Google contends. As long as the Massachusetts wiretap statute does not conflict with the federal wiretap statute, then

it is a valid law under principles of federalism. *Vitello*, 367 Mass at 247 (“[A] State statute may adopt standards more stringent than the requirements of Federal law.”). As Google itself notes, the federal wiretap statute prohibits the secret interception of electronic communications, just like the Massachusetts wiretap statute, see *supra*. In the absence of manifest Congressional intent to preempt state law, the ECPA does not preempt the Massachusetts wiretap statute.

Google’s next contention is that while the Massachusetts wiretap statute prohibits “secret” interceptions, its advertisement policy is publicly disclosed and transparent. As a result, Google argues that its conduct does not violate the Massachusetts wiretap statute. Under the statute, an interception “means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication. . . .” G.L. c. 272, § 99(B)(4). Marquis alleges that Google “secretly” intercepts her electronic communications with Gmail users. Compl. ¶¶ 14, 27. To rebut that allegation, Google has submitted an affidavit that includes Google’s Terms of Service and Privacy Center screen. See Burhans Affidavit at Tabs 1 and 2. These documents illustrate that Google’s “interest-based advertising” is fully disclosed.

The Burhans Affidavit does not rebut the Complaint’s allegations. First, Google’s attempt to introduce documents outside the pleadings is improper at the

motion to dismiss stage.² Second, the court accepts as true Marquis's allegation that Google secretly intercepted her electronic communications with Gmail users.

Additionally, Marquis is entitled to the reasonable inference that she, as an AOL account holder, would not be privy to or have notice of Google's Terms of Use and Privacy Center policy for Gmail users. The Complaint alleges sufficient facts that Google secretly intercepted electronic communications between non-Gmail users and Gmail users.

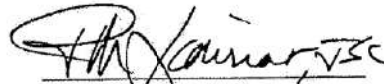
Google's final argument is that it is exempt from liability because it is a communications common carrier, and that it conducted the alleged interceptions "in the ordinary course of its business." G.L. c. 272, § 99(B)(3). In support of this contention, Google presents two cases that involve employers who secretly intercepted communications between their employees and third-parties. Google's reliance on these cases is misplaced, as it does not have an employer-employee relationship with Gmail users. While Gmail is a free service, Google generates revenue through selling advertising. Compl. ¶ 8. It intercepts and scans emails sent to Gmail users by non-Gmail users such as Marquis in order to find keywords so that

² "In evaluating a rule 12(b)(6) motion, we take into consideration the allegations in the complaint, although matters of public record, orders, items appearing in the record of the case, and exhibits attached to the complaint, also may be taken into account." *Schaer v. Brandeis Univ.*, 432 Mass. 474, 477 (2000) (quotation omitted). Google's Terms of Use and Privacy Center policy, external to the Complaint, are not appropriate for consideration at this stage.

it can target Gmail users with relevant advertisements. Compl. ¶¶ 9, 11. At this preliminary stage, the court cannot conclude as a matter of law that intercepting and scanning emails for purposes of "interest-based advertising" is "in the ordinary course of [Google's] business" under the Massachusetts wiretap statute.

ORDER

For the foregoing reasons, Defendant Google Inc.'s Motion to Dismiss is DENIED.


Peter M. Lauriat
Justice of the Superior Court

Dated: January 17, 2012

JANE DOE, <i>on behalf of herself and all others</i> *	IN THE
<i>similarly situated</i>	
Plaintiff *	CIRCUIT COURT
v. *	FOR BALTIMORE CITY
MEDSTAR HEALTH, INC., <i>et al.</i> *	CASE NO.: 24-C-²⁰19-0004⁵⁹¹
Defendants *	

* * * * *

MEMORANDUM OPINION

This matter has come before the Court on Defendants Medstar Health, Inc. and Medstar Good Samaritan’s Motion to Dismiss (Docket Entry #5). The Court has considered the briefs of the parties, oppositions, replies, and the oral argument of counsel, held on July 27, 2020.

I. Background.

Plaintiff, Jane Doe, is a patient of Defendant, medical provider MedStar Health, Inc. (“MedStar”). MedStar is the owner and operator of hospitals and health care facilities, including MedStar Good Samaritan Hospital. MedStar has public websites that any individual can access to obtain information about general medical topics and information about MedStar and its facilities and services. Patients can also use MedStar’s website to log in, access their private medical records, communicate with doctors, and schedule appointments. Plaintiff alleges that MedStar uses computer coding to disclose personally identifiable, private data related to patients’ medical care to at least 23 different third parties, including, but not limited to Facebook, Google, LinkedIn, Twitter, and Pinterest. Plaintiff claims that MedStar disclosed: the URLs that Plaintiff visited; “search queries about specific doctors, medical conditions, treatments”; patients’ clicks to “Search,” “FindADoctor,” “Login,” or “Enroll” in MyMedStar (Medstar’s online patient portal); “summaries of MedStar’s responsive communications, the parties to all

communications at MedStar's web properties, and the existence of communications at MedStar's web properties.”

Plaintiff raises five claims: 1) violation of the Maryland Wiretap Act, 2) intrusion upon seclusion, 3) publication of private facts, 4) breach of confidence, and 5) violation of the Consumer Protection Act. Plaintiff alleges that her data was disclosed without prior authorization, and that the disclosure of her data harms Plaintiff by invading her privacy and harming her property rights to her data. Plaintiff seeks general damages and economic damages for these harms. Additionally, Plaintiff pursues a theory of unjust enrichment for Defendant's profit from Plaintiff's data, as well as statutory damages.

II. Applicable Law.

In deciding a Motion to Dismiss, the Court takes as true all well-pleaded allegations and reviews them in the light most favorable to the plaintiff. *Lloyd v. General Motors Corp.*, 397 Md. 108, 121 (2007). Although a court must assume the truth of all well-pleaded facts, dismissal is proper when the facts alleged, if proven, would fail to afford relief to the plaintiff. Md. Rule 2-322(b)(2); see also *Hogan v. Maryland State Dental Ass'n*, 155 Md. App. 556, 561 (2004). The facts as set forth in the complaint must be pleaded with “sufficient specificity; bald assertions and conclusory statements by the pleader will not suffice.” *Sutton v. FedFirst Financial Corp.*, 226 Md. App. 46, 74 (2015) (quoting *RRC Northeast, LLC v. BAA MD, Inc.*, 413 Md. 638, 643 (2010)). Any ambiguity or uncertainty in the allegations is construed against the pleader. *Shenker v. Laureate Educ., Inc.*, 411 Md. 317, 335 (2009).

III. Analysis.

In Count 1 of the Complaint, Plaintiff alleges that Defendants have violated the Maryland Wiretap Act, Md. Code Ann., Cts. & Jud. Proc. § 10-402. Maryland's appellate courts have not,

to this Court's knowledge, addressed wiretapping in the context of online data being intercepted and disclosed to third parties. This is apparent from the briefs of the parties, which look extensively to other jurisdictions for persuasive authority to assist in interpreting the Maryland statute.¹

Despite the paucity of Maryland precedent, the Court feels that the plain language of the statute itself is straightforward and provides a legal foundation for Count 1 of the Complaint. The Maryland Wiretap Act provides as follows with respect to prohibited conduct:

- (a) Except as otherwise specifically provided in this subtitle it is unlawful for any person to:
- (1) Willfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
 - (2) Willfully disclose, or endeavor to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subtitle; or
 - (3) Willfully use, or endeavor to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subtitle.

Md. Code Ann., Cts. & Jud. Proc. § 10-402. The statute goes on to authorize a civil cause of action for any victim of the unlawful conduct:

¹ The Court finds the analysis in *Doe v. Virginia Mason Medical Center*, 2020 WL 1983046, No. 19-2-26674-1 (Kings County, WS Feb. 12, 2020) to be persuasive. In that matter, MedStar presented nearly identical arguments as Defendant in the instant case. The court rejected MedStar's arguments and distinguished that case from *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943 (N.D. Cal. 2017), noting that the *Smith* Plaintiffs "consented to Facebook tracking . . . and the allegations in this case are broader than sharing URL information only." *Virginia Mason* at 2. Similarly, in the instant matter, Plaintiff alleges to be a patient, that Defendant Medstar's information disclosures were executed without Plaintiff's knowledge, and that the disclosures were made to "at least 23 different third-party marketing firms." The *Virginia Mason* court noted that the case before it, as with the instant case, "involves the allegations of sharing data with more than Facebook and does not hinge on the relationship between the Plaintiff and Facebook." *Id.*

(a) Any person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of this subtitle shall have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use the communications, and be entitled to recover from any person:

- (1) Actual damages but not less than liquidated damages computed at the rate of \$100 a day for each day of violation or \$1,000, whichever is higher;
- (2) Punitive damages; and
- (3) A reasonable attorney's fee and other litigation costs reasonably incurred.

Md. Code Ann., Cts. & Jud. Proc. § 10-410. In the instant case, the Court finds that Plaintiff has sufficiently plead the elements of a Wiretap Act claim and that such a claim can be maintained by Plaintiff under the Act. The Court further finds that there are questions of fact as to whether Defendant's conduct constitutes an "interception," whether the types of data alleged to have been disclosed constitute "communications" and/or "disclosures," and whether Plaintiff consented to disclosure, thus rendering Defendant's conduct lawful under Md. Code Ann., Cts & Jud. Proc. § 10-402(c)(3).

Counts 2 and 3 of Plaintiff's Complaint assert privacy claims: invasion of privacy – intrusion upon seclusion (Count 2), and invasion of privacy – publication of private facts (Count 3). Intrusion upon seclusion is "the intentional intrusion upon the solitude or seclusion of another or his private affairs or concerns that would be highly offensive to a reasonable person." *Pemberton v. Bethlehem Steel Corp.*, 66 Md. App. 133, 163 (1986) (citing Restatement of Torts, 2d, § 652B). The parties disagree about the kinds of data that Defendant disclosed and whether that data is personally identifiable information. At this stage in the proceedings, and pursuant to a motion to dismiss, the Court assumes the truth of Plaintiff's allegations that Defendant provided express promises of privacy to patients, and that Defendant violated those promises by disclosing Plaintiff's data. Under these circumstances, dismissal of this claim is inappropriate as a

reasonable finder of fact could conclude that, if Plaintiff's disclosed data constitutes personally identifiable information, Defendant's disclosures are highly offensive.

Similarly, Defendant has failed to persuade the Court regarding Count 3 alleging disclosure of private facts. To sustain such a claim, Plaintiff must demonstrate that a party has publicized Plaintiff's "private life" and that the matter publicized "is of a kind which (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." *Furman v. Sheppard*, 130 Md. App. 67, 77 (2000). Private medical data is not of legitimate concern to the public, and again, assuming the allegations in the Complaint to be true, the data disclosed constitutes personally identifiable information; a reasonable fact-finder could conclude that Defendant's disclosures are highly offensive.

Count 4 of the Complaint alleges a claim for breach of a confidential relationship. Generally, there is no cause of action in Maryland offering relief for a breach of confidence claim involving a patient-provider relationship. Plaintiff likens her case to precedent that addresses confidentiality in the context of business relationships involving free competition and trade secrets, but the comparison is not persuasive. See *Space Aero Prods. Co. v. R. E. Darling Co.*, 238 Md. 93, 208 A.2d 74 (1965). In *Space Aero Prods. Co.*, the breaching party profited by replicating the non-breaching party's product, and the non-breaching party lost profits as a result. The Court in *Space Aero Prods. Co.* provided that compensatory damages are awarded unless they would be inadequate, in which case the Court will issue an injunction. Even assuming *arguendo* that there is a cause of action for a patient-provider relationship, Plaintiff has not demonstrated a monetary loss tied to the data itself, and the purpose of an injunction for this type of claim is meant to curb further economic loss, again not present here. *Id.* at 124. While

Plaintiff's other privacy tort claims may recognize general damages for the loss of privacy itself, the Court has no method to award her relief under a breach of confidence claim.

Finally, in Count 5, Plaintiff alleges a breach of the Consumer Protection Act. To establish a claim under the Consumer Protection Act, a consumer must state "an identifiable loss, measured by the amount the consumer spent or lost as a result of his or her reliance on the sellers' misrepresentation." *Lloyd v. GMC*, 397 Md. 108, 143 (2007). Although Plaintiff cites to cases from other jurisdictions, there is no basis in Maryland law to suggest that Plaintiff is entitled to claim a "privacy injury" under this cause of action. Any recovery for such an injury should be limited to Plaintiff's privacy tort claims. Additionally, Plaintiff argues that she is entitled to this cause of action because she can claim benefit of the bargain damages and unjust enrichment, but Plaintiff is not raising a breach of contract claim, and these are theories for damages under contract law.

IV. Conclusion.

For the reasons set forth above, the Court will grant the Motion in part, dismissing Counts 4 and 5.

August 5, 2020
Date

Judge's Signature appears on the
original document
Jeffrey M. Geller, Judge
Circuit Court for Baltimore City

SUPERIOR COURT OF CALIFORNIA,
COUNTY OF SACRAMENTO
GORDON D SCHABER COURTHOUSE

MINUTE ORDER

DATE: 06/09/2022 TIME: 01:30:00 PM DEPT: 28

JUDICIAL OFFICER PRESIDING: Lauri A. Damrell

CLERK: V. Aleman

REPORTER/ERM: Shella Pham #13293

BAILIFF/COURT ATTENDANT: T. Gonzalez

CASE NO: 34-2019-00258072-CU-BT-GDS CASE INIT.DATE: 06/10/2019

CASE TITLE: **Doe I vs. Sutter Health**

CASE CATEGORY: Civil - Unlimited

EVENT TYPE: Motion for Judgment on the Pleadings - Civil Law and Motion - Demurrer/JOP

APPEARANCES

Jeffrey A Koncius, counsel, present for Plaintiff(s) remotely via video.

Nicole Ramirez, specially appearing for counsel Mitchell M. Breit, present for Plaintiff(s).

Jay Barnes, counsel, present for Plaintiff(s) remotely via video.

Stephen C Steinberg, counsel, present for Defendant(s) remotely via video.

Michael D. Abraham, counsel, present for Defendant(s) remotely via video.

Nature of Proceedings: Motion for Judgment on the Pleadings

The matter became before the Court his date for a hearing with the above-indicated counsel present.

After hearing from the parties, the Court affirmed the tentative ruling.

Tentative Ruling:

Defendant Sutter Health's ("Sutter") Motion for Judgment on the Pleadings against Plaintiffs' Third Amended Complaint ("3AC") is DENIED as follows.

Background

Facts

In this putative class action, Plaintiffs are patients of Sutter, a health care provider in Sacramento. (3AC, ¶¶ 14-16.) The action arises out of Plaintiffs' use of Sutter's "My Health Online" patient portal ("Portal"). Plaintiffs allege that Sutter represents that the Portal is secure, but when a person uses it, Sutter discloses certain information about such use to Facebook, Google, and other third parties. (*Id.*, ¶¶ 3-5.) For example, Plaintiffs allege that upon signing into the Portal, Sutter discloses the fact of the sign in and each patient's personally identifiable information to Facebook, Google, and Crazy Egg. (*Id.*, ¶¶ 5b, 8.) Once signed-in, if a patient clicks to view allergies, a disclosure of that action is made to Google of the specifics; if a patient clicks "Find-A-Doctor" or set up an appointment, a disclosure of that action is made to Facebook, Google, and others. (*Id.*, ¶5c.) On logoff, Sutter discloses this action to Facebook and Google. (*Id.*, ¶ 5i.) Plaintiffs allege Sutter makes these disclosures by intentionally including source code on its website that commanded Plaintiffs' browser to redirect the contents of HTTPS communications to third parties through invisible tracking pixels that are also code web bugs. (*Id.*, ¶¶ 128-130.)

Plaintiffs' 3AC was filed on December 7, 2021 and contains three causes of action: (1) violation of the

DATE: 06/09/2022

MINUTE ORDER

Page 1

DEPT: 28

Calendar No.

California Invasion of Privacy Act ("CIPA"), specifically Penal Code § 631 ("section 631"), (2) breach of contract, and (3) breach of the implied covenant of good faith and fair dealing. This Court has twice sustained Sutter's demurrer to Plaintiffs' cause of action for violation of section 631. (See ROA 134, 206.) However, on November 16, 2021, the Court overruled Plaintiffs' demurrer to that cause of action as stated in the 2AC. (ROA 301.) Sutter now moves for judgment on the pleadings with respect to the 3AC's cause of action for violation of section 631.

Request for Judicial Notice

Sutter's request for judicial notice in support of this motion is GRANTED as to request Nos. 1 (the Court's 11/16/2021 Minute Order sustaining portions of Sutter's demurrer to Plaintiffs' 2AC); 2 (the Court's 11/16/2021 Minute Order granting parts of Sutter's motion to strike portions of Plaintiffs' 2AC); 3 (the Court's 11/3/2020 Minute Order sustaining Sutter's demurrer to the 1AC); 4 (the Court's 11/3/2020 Minute Order granting parts of Sutter's motion to strike portions of Plaintiffs' 1AC); 5 (the Court's 1/29/2020 Minute Order sustaining Sutter's demurrer to the original complaint); 6 (Plaintiffs' 2AC); 7 (Plaintiffs' 1AC); 8 (Plaintiffs' original complaint); and 10 (the text of AB 860 passed by the Assembly on July 26, 1967 and passed by the California Senate on July 27, 1967). (Evid. Code, § 452(a), (d).)

Sutter's request for judicial notice is DENIED as to request No. 9 (Model Notice of Privacy Practices for health care providers published by the US Department of Health and Human Services' Office for Civil Rights) as this material is irrelevant to the disposition of this motion. (See *State Comp. Ins. Fund v. ReadyLink Healthcare, Inc.* (2020) 50 Cal.App.5th 422, 442.)

Legal Standard

A motion for judgment on the pleadings has the same function as a general demurrer, but may be made after the time for demurrer has expired. (See Code Civ. Proc., § 438.) Like a demurrer, the grounds for a motion for judgment on the pleadings must appear on the face of the complaint, or in documents attached to the pleadings and properly incorporated by reference. (Code Civ. Proc., § 438(d); *Lumbermens Mutual Casualty Company v. Vaughn* (1988) 99 Cal.App.3d 171, 178.) The motion may be based on matters of which the court may take judicial notice. (Code Civ. Proc. § 438(d); see also *Howard Jarvis Taxpayers Assoc. v. Riverside* (1999) 73 Cal.App.4th 679, 685.) However, the motion does not lie on grounds previously raised by demurrer unless there has been a "material change in applicable case law or statute" since the demurrer was overruled. (Code Civ. Proc. § 438(g)(1); see *Yancey v. Superior Court* (1994) 28 Cal.App.4th 558, 562, fn. 1.) The motion should be granted if, taking all of the allegations of the complaint to be true, the defendant is entitled to judgment as a matter of law. (*Consolidated Fire Protection Dis. v. Howard Jarvis Taxpayers' Ass'n* (1998) 63 Cal. App. 4th 211, 219.) A motion for judgment on the pleadings is properly granted without leave to amend when there is no reasonable possibility that the defect can be cured by amendment. (See *Schonfeldt v. State of California* (1998) 61 Cal. App.4th 1462, 1465 ("If there is no liability as a matter of law, leave to amend should not be granted."))

Analysis

Section 631 penalizes various forms of secret monitoring of conversations. (*Ribas v. Clark* (1985) 38 Cal.3d 355, 359 (*Ribas*)). It provides, in pertinent part:

"(a) Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to

communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars (\$2,500), or by imprisonment in the county jail not exceeding one year, or by imprisonment pursuant to subdivision (h) of Section 1170, or by both a fine and imprisonment in the county jail or pursuant to subdivision (h) of Section 1170. . . ." (Emphasis added.)

Sutter advances two arguments with respect to the construction of the following phrases in section 631 emphasized above: "without the consent of all the parties" and "reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable." The Court discusses each argument separately below.

First Argument: "Without the Consent of All the Parties"

The parties do not dispute that section 631 requires the consent of "all parties" to the communication. (See *People v. Conklin* (1974) 12 Cal.3d 259, 270; RJN Ex. J.) Nor do they dispute that section 631 applies only to third parties and not to a participant to the communication. (See *Warden v. Kahn* (1979) 99 Cal.App.3d 805, 811.) However, Sutter contends that (1) section 631 applies only where there are least two participants to the communication, (2) that both of those participants must be natural persons capable of giving consent, and (3) that Plaintiffs do not allege the presence of "another individual as a second participant who could have given consent." (Mov. Mot. P&A, p. 6: 15-16.) While Sutter's argument is creative, the Court finds it ultimately lacks merit.

As Sutter's argument is based on statutory construction, the Court begins by setting forth the fundamental rules governing such construction. When a court interprets a statute, its fundamental task is to determine the Legislature's intent so as to effectuate the law's purpose. (*Smith v. LoanMe, Inc.* (2021) 11 Cal.5th 183, 190.) The court first examines the statutory language, giving it a plain and commonsense meaning. (*Ibid.*) The court does not examine the language in isolation, but in the context of the statutory framework as a whole in order to determine its scope and purpose and to harmonize the various parts of the enactment. (*Ibid.*) If the language is clear, courts must generally follow its plain meaning unless a literal interpretation would result in absurd consequences the Legislature did not intend. (*Ibid.*)

Sutter's statutory argument relies on *Kight v. CashCall, Inc.* (2011) 200 Cal.App.4th 1377 (*Kight*). In *Kight*, the plaintiffs brought claims against a consumer finance company under Penal Code § 632 ("section 632"), which is part of CIPA and prohibits eavesdropping on confidential communications. The plaintiffs alleged that the company monitored their telephone conversations with the company's employees without the plaintiffs' knowledge or consent. (*Id.* at p. 1383.) The trial court determined that eavesdropping under section 632 requires three parties and there were only two parties to the conversations – the corporation and the customer. (*Id.* at p. 1391.) The appellate court reversed, finding this interpretation contrary to the statutory language and intent of section 632. (*Ibid.*) With respect to the statutory language, the court focused on the use of the terms "party" and "person" in the statute. The court noted that section 632 prohibits a "person" from overhearing a confidential communication without the consent of "all parties" and that the term "person" is defined, for purposes of section 632, to include both an individual and a corporation. (*Id.* at p. 1391.) By contrast, as the court explained, the statutory term "parties" is used to identify the "individuals who are the conversation participants from whom consent is required" before a conversation may be overheard. (*Ibid.* (Emphasis added).) The court determined that this difference in terms supported the interpretation that a corporation is not a single unit for purposes of determining who must give consent and that all participants to the conversation must give consent. The court held that each individual listener should be counted as a person as opposed to all corporate employees counting as one corporate person. (*Ibid.*) Sutter argues that, pursuant to *Kight*, the term "party" in section 631 can only mean an individual and, thus, section 631 cannot apply here where the intended recipient of the communication is not a natural person.

The Court is not convinced. First, the Court does not interpret *Kight* to mean that sections 631 and 632 are inapplicable when a communication is between a natural person and an entity or technology created by other natural persons. Second, the particular context of *Kight* alone is distinguishable. *Kight* considered a telephone conversation between a corporate employee and the plaintiff, a conversation to which another corporate employee listened unbeknownst to the plaintiff. Here, the Court does not consider a telephone conversation but rather click communications by Plaintiffs to Sutter's website. "Tautologically, a communication will always consist of at least two parties: the speaker and/or sender, and at least one intended recipient." (*In re Google Inc.* (3d Cir. 2015) 806 F.3d 125, 143.) Courts interpreting section 631 have indicated that a party to a communication, for purposes of section 631, may include an entity or website. In *Revitch v. New Moosejaw* (2019) 2019 U.S. Dist. LEXIS 186955 (*Revitch*), for example, the plaintiff alleged that the defendant, Moosejaw, embedded into its webpages a mechanism that allowed another company, NaviStone, to eavesdrop on the plaintiff's communications. (*Id.* at *2.) The court held that the plaintiff's "interaction with the Moosejaw website was a communication within the meaning of section 631." (*Id.* at *3.) In particular, the court noted that "[a]dmittedly, a customer in [a] brick-and-mortar store does not communicate by searching through the inventory. But the same is not true for off-site shoppers: a customer who calls to inquire about a store's products undoubtedly communicates with the retailer. As does an online patron, [the plaintiff] requested information from Moosejaw by clicking on terms of interest; Moosejaw responded by supplying that information. This series of requests and responses – whether online or over the phone – is communication." (*Ibid.*; see also *Graham v. Noom* (N.D. Cal. 2021) 533 F.Supp.3d 823, 832-833 [concluding that a company was a party to a communication and another company was an extension of that company]; *Flanagan v. Flanagan* (2002) 27 Cal.4th 766, 775 (*Flanagan*) [addressing possibility that an auditor to a conversation can be a person or a mechanical device].) The Court disagrees with Sutter that *Revitch* is inapposite here or deviates from California precedents interpreting CIPA. The only precedent Sutter cites is *Kight*, and the Court is unconvinced that precedent dictates a different result than *Revitch*.

Courts have also reached the same result with respect to the federal Wiretap Act, which prohibits similar conduct as section 631 and involves a similar analysis. (See *In re Google Inc.* (3d Cir. 2015) 806 F.3d 125, 143 [concluding defendant advertising companies were parties to a communication for purposes of the federal wiretapping law because they were the intended recipients of requests that plaintiff's browsers sent to the defendant's servers]; *Calhoun v. Google LLC* (N.D. Cal. 2021) 526 F.Supp. 3d 605, 623.) [discussing website consent under the federal Wiretap Act]; *Chance v. Ave. A, Inc.* (W.D. Wash. 2001) 165 F.Supp.2d 1153, 1162 [finding it implicit that web pages consented to interception under federal wiretapping law]; *In re Doubleclick Privacy Litig.* (S.D.N.Y. 2001) 154 F.Supp.2d 497, 514 [concluding certain websites were parties to the communications from the plaintiffs and gave sufficient consent]; see also *Cline v. Reetz-Laiolo* (N.D. Cal. 2018) 329 F.Supp.3d 1000, 1051 ["The analysis for a violation of CIPA is the same as that under the federal Wiretap Act."] As stated in the Court's ruling on Sutter's demurrer to the 2AC, "California courts are likely to rely on federal decisions interpreting the federal wiretap statute" when interpreting section 631. (ROA 301, p. 21.)

Second, in addition to considering the text of section 631, the court in *Kight* considered the legislative intent and determined that the Legislature enacted section 632 to "ensure an individual's right to control the firsthand dissemination of a confidential communication, and expressed its intent to strongly protect an individual's privacy rights in electronic communications." (*Id.* at p. 1392.) Based on that legislative purpose, the court construed section 632 broadly in favor of the plaintiff, concluding the required third party to the conversation was present. Accordingly, contrary to Sutter's point, *Kight* does not suggest that section 631 or 632 applies only if the parties to the conversation or communication are natural persons. Instead, it suggests that CIPA, including section 631, should be construed broadly to protect an individual's privacy rights. As *Kight* held with respect to section 632, the privacy rights affected under section 631 are the same regardless whether a communication is with a machine or a human being. (*Id.* at p. 1393.) Interpreting section 631 in the way Sutter suggests would undermine both the requirement

of two-party consent and the overall purpose of this section. CIPA was enacted in 1967, "replacing prior laws that permitted the recording of telephone conversations with the consent of one party to the conversation." (*Flanagan, supra*, 27 Cal.4th at p. 768.) "The purpose of the act was to protect the right of privacy by, among other things, requiring that all parties consent to a recording of their conversation." (*Ibid.*) The legislative history is "replete with references to the Legislature's intent to strengthen then existing law by 'prohibiting wiretapping or 'electronic eavesdropping' without the consent of all parties to the communication which is being tapped or overheard." (*Frio v. Superior Court* (1988) 203 Cal.App.3d 1480, 1487.) "The philosophy [of protecting an individual's privacy right] lie[s] at the heart of virtually all the decisions construing the [Act]." (*Flanagan, supra*, 27 Cal.4th at p. 775.) The addition of all-party consent in section 631 was clearly intended to broaden the coverage of section 631; however, Sutter's suggested interpretation here would limit that coverage by effectively removing entities or technological devices as possible parties to a communication. The Court refuses to adopt such an interpretation.

Second Argument: "Reads, or Attempts to Read, or to Learn the Contents or Meaning of any Message, Report, or Communication While the Same Is in Transit or Passing Over any Wire, Line, or Cable"

The California Supreme Court has explained that section 631 contains three operative clauses covering "three distinct and mutually independent patterns of conduct." (*Tavernetti v. Superior Court* (1978) 22 Cal. 3d 187, 192.) Section 631 also includes a fourth clause that establishes liability for anyone "who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the" other three bases for liability. (*Mastel v. Miniclip SA* (E.D.Cal. 2021) 549 F.Supp.3d 1129, 1134 (*Mastel*); see 3AC ¶¶ 367-368 [alleging Sutter aided, agreed with, and conspired with third-party tracking companies in violating section 631].)

The first clause of section 631 has been described as creating "liability for any individual who 'intentionally taps, or makes any unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument.'" (*Matera v. Google Inc.* (N.D.Cal. Aug. 12, 2016, No. 15-CV-04062-LHK) 2016 U.S.Dist.LEXIS 107918, at *56-57 (emphasis added).) Sutter argues that, according to its plain language, this first clause is limited to only *telegraphic or telephonic* communications and that Plaintiffs' allegations do not involve such a communication. On the one hand, Sutter's argument is supported by precedent. (See *Mastel, supra*, 549 F.Supp.3d at pp. 1133-1135, citing *In re Google Assistant Priv. Litig.* (N.D. Cal. 2020) 457 F.Supp.3d 797, 826 [claim under first clause must be dismissed if allegations do not show technology at issue operates using a telegraph or telephone wires]; *In re Google Inc. Gmail Litig.* (N.D. Cal. 2013 No. 13-MD-02430-LHK) 2013 U.S.Dist.LEXIS 172784, at *77 (*Google Gmail*) ["difference in coverage between first and second clauses suggests that the Legislature intended the two clauses to apply to different types of communication"]; see also *Ward General Insurance Services, Inc. v. Employers Fire Ins. Co.* (2003) 114 Cal.App.4th 548, 554 [adjective in series of nouns generally modifies each noun following the phrase].) On the other hand, other federal courts have suggested, without breaking down the different clauses in section 631, that section 631 covers the type of claims at issue here. In *Revitch, supra*, the plaintiff argued that Moosejaw embedded into its webpages a mechanism that allowed a third party to eavesdrop on the plaintiff's communications with the Moosejaw website. (2019 U.S. Dist. LEXIS 186955 at *2.) The code embedded on the website functioned as a wiretap that redirected the plaintiff's communications to the third party. (*Id.* at *3.) The court held that the plaintiff's allegations were sufficient to state a claim under section 631. (*Id.* at *2.)

However, the Court need not resolve the extent of the first clause's coverage as it finds Sutter's argument as to the second clause of section 631 unpersuasive. "The second clause of [section 631] creates liability for any individual who 'reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state.'" (*Matera v. Google Inc.* (N.D.Cal. Aug. 12, 2016, No. 15-CV-04062-LHK) 2016 U.S.Dist.LEXIS 107918, at *56-57.) Sutter's argument relies on the absence of the term "instrument" from this clause (whereas "instrument" is included in the first clause). Sutter argues that Plaintiffs' 3AC allegations are premised on connection to an "instrument"

and, as a result, Plaintiffs' allegations are outside the scope of the second clause. More specifically, Sutter contends the 3AC alleges that Sutter's "source code connected to and 'commandeer[ed]' an instrument – the visitor's computer – which caused the computer's web browser to react to inputted or received web data in the visitor's web browser and/or computer by sharing information about the data in separate transmissions to third parties." (Mov. Mot. P&A, p. 16: 13-16.) Again, the Court finds Sutter's argument lacks merit.

In support of its argument, Sutter's moving papers do not cite any cases interpreting section 631 and instead rely on general cases for rules of statutory construction. Conducting its own research, the Court has located a single case in which a federal court stated that "the second clause applies only to 'wire[s], line[s], or cable[s]' – not 'instrument[s,]' which are included in the first clause." (*Google Gmail, supra*, at *77.) However, in so doing, the federal court intended to highlight the breadth of the statute, not its limitations. Specifically, the court concluded that, by excluding the term "instrument" in the second clause, the Legislature reflected its intent to have the first and second clauses apply to different types of communications, thereby *expanding* its coverage. The court did not interpret "wire," "line" or "cable" narrowly. Rather, the Court found that the second clause is broad enough to encompass email. (*Id.*)

The Court's research further confirms that other courts have not read the second clause, or section 631 in its entirety, as narrowly as Sutter. In its order with respect to Sutter's demurrer to Plaintiffs' 2AC, this Court noted that "[f]ederal courts . . . have concluded that section 631 applies to communications over the internet." (See ROA 301, p. 4, citing *Matera, supra*, at *52; see also (*Yoon v. Lululemon United States* (C.D.Cal. 2021) 549 F. Supp. 3d 1073, 1080 (*Yoon*) "[c]ourts agree . . . that [section 631] applies to communications conducted over the internet").) Such communications by definition involve a computer; thus, Sutter's interpretation would upend the general consensus among federal courts as to Section 631's application to internet-based communications. These cases help illustrate that Sutter's argument with respect to the phrase "wire, line, or cable" is misplaced. That phrase refers to the *device* through which the communication is transmitted. Federal courts have already determined that communications transmitted over the Internet are transmitted over a wire, line, or cable for purposes of section 631. (See *Matera, supra*, at *57.) The parties do not question whether Plaintiffs' communications at issue here were conducted over the Internet – the fact that they involved a computer is part and parcel of the communication occurring over the Internet.

It appears that Sutter's argument also takes issue with the *means* by which the improper interception of the communication over wire, line, or cable is achieved. In this regard, Sutter directs the Court's attention to the structure of section 631. According to Sutter, when broken down into grammatical clauses, the first two clauses of section 631 read as follows:

"Any person:

- (i) who *by means of any machine, instrument, or contrivance, or in any other manner*, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or
- (ii) who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or" (431 (Emphasis added).)

Sutter argues that the italicized phrase specifies the means by which the unlawful activity is achieved but this phrase only appears in the first clause. In Sutter's view, this phrase does not apply to the second clause and, as a result, using an "instrument" to act as described in clause (ii) is not a violation of that clause. However, Sutter's interpretation would make it impossible to violate the second clause of section 631 because any means by which the violation is achieved is not mentioned in that clause. The Court

rejects such an interpretation. With respect to the means by which the interception is achieved, the Ninth Circuit has described section 631 as prohibiting "any person from *using electronic means* to 'learn the contents or meaning' of any 'communication' 'without consent' or in an 'unauthorized manner.'" (*Davis v. Facebook, Inc.* (9th Cir. 2020) 956 F.3d 589, 606-607.) Additionally, the Central District of California read the second clause as prohibiting the unlawful reading or learning "by means of any machine, instrument, or contrivance." (See *Alder v. Cmty.* (C.D.Cal. Aug. 2, 2021, No. 2:21-cv-02416-SB-JPR) 2021 U.S. Dist. LEXIS 201644, at *5 [describing section 631 as imposing "liability on any person who 'by means of any machine, instrument, or contrivance, . . . and without the consent of all parties . . . reads, or attempts to read, or to learn the contents or meaning of any . . . communication while the same is in transit . . . or is being sent from, or received at any place within this state'"]; see also *Yoon, supra*, 549 F.Supp.3d 1073, 1080.) Another court described the second clause as applying to "both communications 'in transit over any wire, line, or cable' and those 'sent from, or received at any place within this state.'" (*Lopez v. Apple, Inc.* (N.D. Cal. 2021) 519 F.Supp. 3d 672, 687; see also *In re Google Assistant Privacy Litig.* (N.D. Cal. 2020) 457 F.Supp.3d 797, 826 [agreeing that second clause could be read in disjunctive].) Under these constructions, the allegation that Sutter used Plaintiffs' computers to enable a third-party's interception of their communications on the Portal does not remove Plaintiffs' claim from section 631.

Lastly, the Court reiterates the California Supreme Court's instruction to interpret CIPA in a manner that "fulfills the legislative purpose of [the Act] by giving greater protection to privacy interests." (*Flanagan, supra*, 27 Cal. 4th at p. 775.) Thus, when faced with two possible interpretations of CIPA, the California Supreme Court has construed the Act in accordance with the interpretation that provides the greatest privacy protection. (See *Ribas, supra*, 38 Cal. 3d at 360-61.) Sutter's interpretation of section 631 would provide less privacy protection and the Court finds it not well supported by case law. Accordingly, the Court rejects Sutter's second argument with respect to the cause of action for violation of section 631.

Disposition

Based on the foregoing, Sutter's Motion for Judgment on the Pleadings is DENIED.

This minute order is effective immediately. No formal order or other notice is required. (Code Civ. Proc., § 1019.5; Cal. Rules of Court, rule 3.1312.)

To request oral argument on this matter, you must call Department 28 at (916) 874-6695 by 4:00 p.m., the court day before this hearing and notification of oral argument must be made to the opposing party/counsel. If no call is made, the tentative ruling becomes the order of the court. (Local Rule 1.06.) Parties requesting services of a court reporter may arrange for private court reporter services at their own expense, pursuant to Government code §68086 and California Rules of Court, Rule 2.956. Requirements for requesting a court reporter are listed in the Policy for Official Reporter Pro Tempore available on the Sacramento Superior Court website at <https://www.saccourt.ca.gov/court-reporters/docs/crtrp-6a.pdf>. The list of Court Approved Official Reporters Pro Tempore is available at <https://www.saccourt.ca.gov/court-reporters/docs/crtrp-13.Pdf>. Please check your tentative ruling prior to the next Court date at www.saccourt.ca.gov prior to the above referenced hearing date.

If oral argument is requested, the matter shall be held via Zoom with the links below:

To join by Zoom link - <https://saccourt-ca-gov.zoomgov.com/my/sscdept28>
To join by phone dial (833) 568-8864 ID 16039062174

Counsel for Plaintiff is directed to notice all parties of this order.

Defendant Sutter Health's ("Sutter") Motion for Judgment on the Pleadings against Plaintiffs' Third Amended Complaint ("3AC") is DENIED as follows.

Background

Facts

In this putative class action, Plaintiffs are patients of Sutter, a health care provider in Sacramento. (3AC, ¶¶ 14-16.) The action arises out of Plaintiffs' use of Sutter's "My Health Online" patient portal ("Portal"). Plaintiffs allege that Sutter represents that the Portal is secure, but when a person uses it, Sutter discloses certain information about such use to Facebook, Google, and other third parties. (*Id.*, ¶¶ 3-5.) For example, Plaintiffs allege that upon signing into the Portal, Sutter discloses the fact of the sign in and each patient's personally identifiable information to Facebook, Google, and Crazy Egg. (*Id.*, ¶¶ 5b, 8.) Once signed-in, if a patient clicks to view allergies, a disclosure of that action is made to Google of the specifics; if a patient clicks "Find-A-Doctor" or set up an appointment, a disclosure of that action is made to Facebook, Google, and others. (*Id.*, ¶5c.) On logoff, Sutter discloses this action to Facebook and Google. (*Id.*, ¶ 5i.) Plaintiffs allege Sutter makes these disclosures by intentionally including source code on its website that commanded Plaintiffs' browser to redirect the contents of HTTPS communications to third parties through invisible tracking pixels that are also code web bugs. (*Id.*, ¶¶ 128-130.)

Plaintiffs' 3AC was filed on December 7, 2021 and contains three causes of action: (1) violation of the California Invasion of Privacy Act ("CIPA"), specifically Penal Code § 631 ("section 631"), (2) breach of contract, and (3) breach of the implied covenant of good faith and fair dealing. This Court has twice sustained Sutter's demurrer to Plaintiffs' cause of action for violation of section 631. (See ROA 134, 206.) However, on November 16, 2021, the Court overruled Plaintiffs' demurrer to that cause of action as stated in the 2AC. (ROA 301.) Sutter now moves for judgment on the pleadings with respect to the 3AC's cause of action for violation of section 631.

Request for Judicial Notice

Sutter's request for judicial notice in support of this motion is GRANTED as to request Nos. 1 (the Court's 11/16/2021 Minute Order sustaining portions of Sutter's demurrer to Plaintiffs' 2AC); 2 (the Court's 11/16/2021 Minute Order granting parts of Sutter's motion to strike portions of Plaintiffs' 2AC); 3 (the Court's 11/3/2020 Minute Order sustaining Sutter's demurrer to the 1AC); 4 (the Court's 11/3/20 Minute Order granting parts of Sutter's motion to strike portions of Plaintiffs' 1AC); 5 (the Court's 1/29/2020 Minute Order sustaining Sutter's demurrer to the original complaint); 6 (Plaintiffs' 2AC); 7 (Plaintiffs' 1AC); 8 (Plaintiffs' original complaint); and 10 (the text of AB 860 passed by the Assembly on July 26, 1967 and passed by the California Senate on July 27, 1967). (Evid. Code, § 452(a), (d).)

Sutter's request for judicial notice is DENIED as to request No. 9 (Model Notice of Privacy Practices for health care providers published by the US Department of Health and Human Services' Office for Civil Rights) as this material is irrelevant to the disposition of this motion. (See *State Comp. Ins. Fund v. ReadyLink Healthcare, Inc.* (2020) 50 Cal.App.5th 422, 442.)

Legal Standard

A motion for judgment on the pleadings has the same function as a general demurrer, but may be made after the time for demurrer has expired. (See Code Civ. Proc., § 438.) Like a demurrer, the grounds for a motion for judgment on the pleadings must appear on the face of the complaint, or in documents attached to the pleadings and properly incorporated by reference. (Code Civ. Proc., § 438(d); *Lumbermens Mutual Casualty Company v. Vaughn* (1988) 99 Cal.App.3d 171, 178.) The motion may be based on matters of which the court may take judicial notice. (Code Civ. Proc. § 438(d); see also *Howard Jarvis Taxpayers Assoc. v. Riverside* (1999) 73 Cal.App.4th 679, 685.) However, the motion does not lie on grounds previously raised by demurrer unless there has been a "material change in applicable case law or statute" since the demurrer was overruled. (Code Civ. Proc. § 438(g)(1); see *Yancey v. Superior Court* (1994) 28 Cal.App.4th 558, 562, fn. 1.) The motion should be granted if, taking

all of the allegations of the complaint to be true, the defendant is entitled to judgment as a matter of law. (*Consolidated Fire Protection Dis. v. Howard Jarvis Taxpayers' Ass'n* (1998) 63 Cal. App. 4th 211, 219.) A motion for judgment on the pleadings is properly granted without leave to amend when there is no reasonable possibility that the defect can be cured by amendment. (See *Schonfeldt v. State of California* (1998) 61 Cal. App.4th 1462, 1465 ("If there is no liability as a matter of law, leave to amend should not be granted."))

Analysis

Section 631 penalizes various forms of secret monitoring of conversations. (*Ribas v. Clark* (1985) 38 Cal.3d 355, 359 (*Ribas*.) It provides, in pertinent part:

"(a) Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars (\$2,500), or by imprisonment in the county jail not exceeding one year, or by imprisonment pursuant to subdivision (h) of Section 1170, or by both a fine and imprisonment in the county jail or pursuant to subdivision (h) of Section 1170. . . ." (Emphasis added.)

Sutter advances two arguments with respect to the construction of the following phrases in section 631 emphasized above: "without the consent of all the parties" and "reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable." The Court discusses each argument separately below.

First Argument: "Without the Consent of All the Parties"

The parties do not dispute that section 631 requires the consent of "all parties" to the communication. (See *People v. Conklin* (1974) 12 Cal.3d 259, 270; RJN Ex. J.) Nor do they dispute that section 631 applies only to third parties and not to a participant to the communication. (See *Warden v. Kahn* (1979) 99 Cal.App.3d 805, 811.) However, Sutter contends that (1) section 631 applies only where there are least two participants to the communication, (2) that both of those participants must be natural persons capable of giving consent, and (3) that Plaintiffs do not allege the presence of "another individual as a second participant who could have given consent." (Mov. Mot. P&A, p. 6: 15-16.) While Sutter's argument is creative, the Court finds it ultimately lacks merit.

As Sutter's argument is based on statutory construction, the Court begins by setting forth the fundamental rules governing such construction. When a court interprets a statute, its fundamental task is to determine the Legislature's intent so as to effectuate the law's purpose. (*Smith v. LoanMe, Inc.* (2021) 11 Cal.5th 183, 190.) The court first examines the statutory language, giving it a plain and commonsense meaning. (*Ibid.*) The court does not examine the language in isolation, but in the context of the statutory framework as a whole in order to determine its scope and purpose and to harmonize the various parts of the enactment. (*Ibid.*) If the language is clear, courts must generally follow its plain meaning unless a literal interpretation would result in absurd consequences the Legislature did not intend. (*Ibid.*)

Sutter's statutory argument relies on *Kight v. CashCall, Inc.* (2011) 200 Cal.App.4th 1377 (*Kight*) . In

Kight, the plaintiffs brought claims against a consumer finance company under Penal Code § 632 ("section 632"), which is part of CIPA and prohibits eavesdropping on confidential communications. The plaintiffs alleged that the company monitored their telephone conversations with the company's employees without the plaintiffs' knowledge or consent. (*Id.* at p. 1383.) The trial court determined that eavesdropping under section 632 requires *three* parties and there were only two parties to the conversations – the corporation and the customer. (*Id.* at p. 1391.) The appellate court reversed, finding this interpretation contrary to the statutory language and intent of section 632. (*Ibid.*) With respect to the statutory language, the court focused on the use of the terms "party" and "person" in the statute. The court noted that section 632 prohibits a "person" from overhearing a confidential communication without the consent of "all parties" and that the term "person" is defined, for purposes of section 632, to include both an individual and a corporation. (*Id.* at p. 1391.) By contrast, as the court explained, the statutory term "parties" is used to identify the "individuals who are the conversation participants from whom consent is required" before a conversation may be overheard. (*Ibid.* (Emphasis added).) The court determined that this difference in terms supported the interpretation that a corporation is not a single unit for purposes of determining who must give consent and that all participants to the conversation must give consent. The court held that each individual listener should be counted as a person as opposed to all corporate employees counting as one corporate person. (*Ibid.*) Sutter argues that, pursuant to *Kight*, the term "party" in section 631 can only mean an individual and, thus, section 631 cannot apply here where the intended recipient of the communication is not a natural person.

The Court is not convinced. First, the Court does not interpret *Kight* to mean that sections 631 and 632 are inapplicable when a communication is between a natural person and an entity or technology created by other natural persons. Second, the particular context of *Kight* alone is distinguishable. *Kight* considered a *telephone* conversation between a corporate employee and the plaintiff, a conversation to which another corporate employee listened unbeknownst to the plaintiff. Here, the Court does not consider a telephone conversation but rather click communications by Plaintiffs to Sutter's website. "Tautologically, a communication will always consist of at least two parties: the speaker and/or sender, and at least one intended recipient." (*In re Google Inc.* (3d Cir. 2015) 806 F.3d 125, 143.) Courts interpreting section 631 have indicated that a party to a communication, for purposes of section 631, may include an entity or website. In *Revitch v. New Moosejaw* (2019) 2019 U.S. Dist. LEXIS 186955 (*Revitch*), for example, the plaintiff alleged that the defendant, Moosejaw, embedded into its webpages a mechanism that allowed another company, NaviStone, to eavesdrop on the plaintiff's communications. (*Id.* at *2.) The court held that the plaintiff's "interaction with the Moosejaw website was a communication within the meaning of section 631." (*Id.* at *3.) In particular, the court noted that "[a]dmittedly, a customer in [a] brick-and-mortar store does not communicate by searching through the inventory. But the same is not true for off-site shoppers: a customer who calls to inquire about a store's products undoubtedly communicates with the retailer. As does an online patron, [the plaintiff] requested information from Moosejaw by clicking on terms of interest; Moosejaw responded by supplying that information. This series of requests and responses – whether online or over the phone – is communication." (*Ibid.*; see also *Graham v. Noom* (N.D. Cal. 2021) 533 F.Supp.3d 823, 832-833 [concluding that a company was a party to a communication and another company was an extension of that company]; *Flanagan v. Flanagan* (2002) 27 Cal.4th 766, 775 (*Flanagan*) [addressing possibility that an auditor to a conversation can be a person or a mechanical device].) The Court disagrees with Sutter that *Revitch* is inapposite here or deviates from California precedents interpreting CIPA. The only precedent Sutter cites is *Kight*, and the Court is unconvinced that precedent dictates a different result than *Revitch*.

Courts have also reached the same result with respect to the federal Wiretap Act, which prohibits similar conduct as section 631 and involves a similar analysis. (See *In re Google Inc.* (3d Cir. 2015) 806 F.3d 125, 143 [concluding defendant advertising companies were parties to a communication for purposes of the federal wiretapping law because they were the intended recipients of requests that plaintiff's browsers sent to the defendant's servers]; *Calhoun v. Google LLC* (N.D. Cal. 2021) 526 F.Supp. 3d 605, 623.) [discussing website consent under the federal Wiretap Act]; *Chance v. Ave. A, Inc.* (W.D. Wash.

2001) 165 F.Supp.2d 1153, 1162 [finding it implicit that web pages consented to interception under federal wiretapping law]; *In re Doubleclick Privacy Litig.* (S.D.N.Y. 2001) 154 F.Supp.2d 497, 514 [concluding certain websites were parties to the communications from the plaintiffs and gave sufficient consent]; see also *Cline v. Reetz-Laiolo* (N.D. Cal. 2018) 329 F.Supp.3d 1000, 1051 ["The analysis for a violation of CIPA is the same as that under the federal Wiretap Act."] As stated in the Court's ruling on Sutter's demurrer to the 2AC, "California courts are likely to rely on federal decisions interpreting the federal wiretap statute" when interpreting section 631. (ROA 301, p. 21.)

Second, in addition to considering the text of section 631, the court in *Kight* considered the legislative intent and determined that the Legislature enacted section 632 to "ensure an individual's right to control the firsthand dissemination of a confidential communication, and expressed its intent to strongly protect an individual's privacy rights in electronic communications." (*Id.* at p. 1392.) Based on that legislative purpose, the court construed section 632 broadly in favor of the plaintiff, concluding the required third party to the conversation was present. Accordingly, contrary to Sutter's point, *Kight* does not suggest that section 631 or 632 applies only if the parties to the conversation or communication are natural persons. Instead, it suggests that CIPA, including section 631, should be construed broadly to protect an individual's privacy rights. As *Kight* held with respect to section 632, the privacy rights affected under section 631 are the same regardless whether a communication is with a machine or a human being. (*Id.* at p. 1393.) Interpreting section 631 in the way Sutter suggests would undermine both the requirement of two-party consent and the overall purpose of this section. CIPA was enacted in 1967, "replacing prior laws that permitted the recording of telephone conversations with the consent of one party to the conversation." (*Flanagan, supra*, 27 Cal.4th at p. 768.) "The purpose of the act was to protect the right of privacy by, among other things, requiring that all parties consent to a recording of their conversation." (*Ibid.*) The legislative history is "replete with references to the Legislature's intent to strengthen then existing law by 'prohibiting wiretapping or 'electronic eavesdropping' without the consent of all parties to the communication which is being tapped or overheard." (*Frio v. Superior Court* (1988) 203 Cal.App.3d 1480, 1487.) "The philosophy [of protecting an individual's privacy right] lie[s] at the heart of virtually all the decisions construing the [Act]." (*Flanagan, supra*, 27 Cal.4th at p. 775.) The addition of all-party consent in section 631 was clearly intended to broaden the coverage of section 631; however, Sutter's suggested interpretation here would limit that coverage by effectively removing entities or technological devices as possible parties to a communication. The Court refuses to adopt such an interpretation.

Second Argument: "Reads, or Attempts to Read, or to Learn the Contents or Meaning of any Message, Report, or Communication While the Same Is in Transit or Passing Over any Wire, Line, or Cable"

The California Supreme Court has explained that section 631 contains three operative clauses covering "three distinct and mutually independent patterns of conduct." (*Tavernetti v. Superior Court* (1978) 22 Cal. 3d 187, 192.) Section 631 also includes a fourth clause that establishes liability for anyone "who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the" other three bases for liability. (*Mastel v. Miniclip SA* (E.D.Cal. 2021) 549 F.Supp.3d 1129, 1134 (*Mastel*); see 3AC ¶¶ 367-368 [alleging Sutter aided, agreed with, and conspired with third-party tracking companies in violating section 631].)

The first clause of section 631 has been described as creating "liability for any individual who 'intentionally taps, or makes any unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument.'" (*Matera v. Google Inc.* (N.D.Cal. Aug. 12, 2016, No. 15-CV-04062-LHK) 2016 U.S.Dist.LEXIS 107918, at *56-57 (emphasis added).) Sutter argues that, according to its plain language, this first clause is limited to only telegraphic or telephonic communications and that Plaintiffs' allegations do not involve such a communication. On the one hand, Sutter's argument is supported by precedent. (See *Mastel, supra*, 549 F.Supp.3d at pp. 1133-1135, citing *In re Google Assistant Priv. Litig.* (N.D. Cal. 2020) 457 F.Supp.3d 797, 826 [claim under first clause must be dismissed if allegations do not show technology at issue operates using a telegraph or telephone wires]; *In re Google Inc. Gmail Litig.* (N.D. Cal. 2013 No. 13-MD-02430-LHK) 2013 U.S.Dist.LEXIS 172784, at *77 (*Google Gmail*)

[“difference in coverage between first and second clauses suggests that the Legislature intended the two clauses to apply to different types of communication”]; see also *Ward General Insurance Services, Inc. v. Employers Fire Ins. Co.* (2003) 114 Cal.App.4th 548, 554 [adjective in series of nouns generally modifies each noun following the phrase.] On the other hand, other federal courts have suggested, without breaking down the different clauses in section 631, that section 631 covers the type of claims at issue here. In *Revitch, supra*, the plaintiff argued that Moosejaw embedded into its webpages a mechanism that allowed a third party to eavesdrop on the plaintiff’s communications with the Moosejaw website. (2019 U.S. Dist. LEXIS 186955 at *2.) The code embedded on the website functioned as a wiretap that redirected the plaintiff’s communications to the third party. (*Id.* at *3.) The court held that the plaintiff’s allegations were sufficient to state a claim under section 631. (*Id.* at *2.)

However, the Court need not resolve the extent of the first clause’s coverage as it finds Sutter’s argument as to the second clause of section 631 unpersuasive. “The second clause of [section 631] creates liability for any individual who ‘reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state.’” (*Matera v. Google Inc.* (N.D.Cal. Aug. 12, 2016, No. 15-CV-04062-LHK) 2016 U.S. Dist. LEXIS 107918, at *56-57.) Sutter’s argument relies on the absence of the term “instrument” from this clause (whereas “instrument” is included in the first clause). Sutter argues that Plaintiffs’ 3AC allegations are premised on connection to an “instrument” and, as a result, Plaintiffs’ allegations are outside the scope of the second clause. More specifically, Sutter contends the 3AC alleges that Sutter’s “source code connected to and ‘commandeer[ed]’ an instrument – the visitor’s computer – which caused the computer’s web browser to react to inputted or received web data in the visitor’s web browser and/or computer by sharing information about the data in separate transmissions to third parties.” (Mov. Mot. P&A, p. 16: 13-16.) Again, the Court finds Sutter’s argument lacks merit.

In support of its argument, Sutter’s moving papers do not cite any cases interpreting section 631 and instead rely on general cases for rules of statutory construction. Conducting its own research, the Court has located a single case in which a federal court stated that “the second clause applies only to ‘wire[s], line[s], or cable[s]’ – not ‘instrument[s],’ which are included in the first clause.” (*Google Gmail, supra*, at *77.) However, in so doing, the federal court intended to highlight the breadth of the statute, not its limitations. Specifically, the court concluded that, by excluding the term “instrument” in the second clause, the Legislature reflected its intent to have the first and second clauses apply to different types of communications, thereby *expanding* its coverage. The court did not interpret “wire,” “line” or “cable” narrowly. Rather, the Court found that the second clause is broad enough to encompass email. (*Id.*)

The Court’s research further confirms that other courts have not read the second clause, or section 631 in its entirety, as narrowly as Sutter. In its order with respect to Sutter’s demurrer to Plaintiffs’ 2AC, this Court noted that “[f]ederal courts . . . have concluded that section 631 applies to communications over the internet.” (See ROA 301, p. 4, citing *Matera, supra*, at *52); see also (*Yoon v. Lululemon United States* (C.D.Cal. 2021) 549 F. Supp. 3d 1073, 1080 (*Yoon*) “[c]ourts agree . . . that [section 631] applies to communications conducted over the internet”).) Such communications by definition involve a computer; thus, Sutter’s interpretation would upend the general consensus among federal courts as to Section 631’s application to internet-based communications. These cases help illustrate that Sutter’s argument with respect to the phrase “wire, line, or cable” is misplaced. That phrase refers to the *device* through which the communication is transmitted. Federal courts have already determined that communications transmitted over the Internet are transmitted over a wire, line, or cable for purposes of section 631. (See *Matera, supra*, at *57.) The parties do not question whether Plaintiffs’ communications at issue here were conducted over the Internet – the fact that they involved a computer is part and parcel of the communication occurring over the Internet.

It appears that Sutter’s argument also takes issue with the *means* by which the improper interception of

the communication over wire, line, or cable is achieved. In this regard, Sutter directs the Court's attention to the structure of section 631. According to Sutter, when broken down into grammatical clauses, the first two clauses of section 631 read as follows:

*Any person:

- (i) who *by means of any machine, instrument, or contrivance, or in any other manner*, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or
- (ii) who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or" (431 (Emphasis added).)

Sutter argues that the italicized phrase specifies the means by which the unlawful activity is achieved but this phrase only appears in the first clause. In Sutter's view, this phrase does not apply to the second clause and, as a result, using an "instrument" to act as described in clause (ii) is not a violation of that clause. However, Sutter's interpretation would make it impossible to violate the second clause of section 631 because any means by which the violation is achieved is not mentioned in that clause. The Court rejects such an interpretation. With respect to the means by which the interception is achieved, the Ninth Circuit has described section 631 as prohibiting "any person from *using electronic means* to 'learn the contents or meaning' of any 'communication' 'without consent' or in an 'unauthorized manner.'" (*Davis v. Facebook, Inc.* (9th Cir. 2020) 956 F.3d 589, 606-607.) Additionally, the Central District of California read the second clause as prohibiting the unlawful reading or learning "by means of any machine, instrument, or contrivance." (See *Alder v. Cmty.* (C.D.Cal. Aug. 2, 2021, No. 2:21-cv-02416-SB-JPR) 2021 U.S.Dist.LEXIS 201644, at *5 [describing section 631 as imposing "liability on any person who 'by means of any machine, instrument, or contrivance, . . . and without the consent of all parties . . . reads, or attempts to read, or to learn the contents or meaning of any . . . communication while the same is in transit . . . or is being sent from, or received at any place within this state'"]; see also *Yoon, supra*, 549 F.Supp.3d 1073, 1080.) Another court described the second clause as applying to "both communications 'in transit over any wire, line, or cable' and those 'sent from, or received at any place within this state.'" (*Lopez v. Apple, Inc.* (N.D. Cal. 2021) 519 F.Supp. 3d 672, 687; see also *In re Google Assistant Privacy Litig.* (N.D. Cal. 2020) 457 F.Supp.3d 797, 826 [agreeing that second clause could be read in disjunctive].) Under these constructions, the allegation that Sutter used Plaintiffs' computers to enable a third-party's interception of their communications on the Portal does not remove Plaintiffs' claim from section 631.

Lastly, the Court reiterates the California Supreme Court's instruction to interpret CIPA in a manner that "fulfills the legislative purpose of [the Act] by giving greater protection to privacy interests." (*Flanagan, supra*, 27 Cal. 4th at p. 775.) Thus, when faced with two possible interpretations of CIPA, the California Supreme Court has construed the Act in accordance with the interpretation that provides the greatest privacy protection. (See *Ribas, supra*, 38 Cal. 3d at 360-61.) Sutter's interpretation of section 631 would provide less privacy protection and the Court finds it not well supported by case law. Accordingly, the Court rejects Sutter's second argument with respect to the cause of action for violation of section 631.

Disposition

Based on the foregoing, Sutter's Motion for Judgment on the Pleadings is DENIED.

This minute order is effective immediately. No formal order or other notice is required. (Code Civ. Proc., § 1019.5; Cal. Rules of Court, rule 3.1312.)

To request oral argument on this matter, you must call Department 28 at (916) 874-6695 by 4:00 p.m., the court day before this hearing and notification of oral argument must be made to the opposing party/counsel. If no call is made, the tentative ruling becomes the order of the court. (Local Rule 1.06.) Parties requesting services of a court reporter may arrange for private court reporter services at their own expense, pursuant to Government code §68086 and California Rules of Court, Rule 2.956. Requirements for requesting a court reporter are listed in the Policy for Official Reporter Pro Tempore available on the Sacramento Superior Court website at <https://www.saccourt.ca.gov/court-reporters/docs/crtp-6a.pdf>. The list of Court Approved Official Reporters Pro Tempore is available at <https://www.saccourt.ca.gov/court-reporters/docs/crtp-13.Pdf>. Please check your tentative ruling prior to the next Court date at www.saccourt.ca.gov prior to the above referenced hearing date.

If oral argument is requested, the matter shall be held via Zoom with the links below:

*To join by Zoom link - <https://saccourt-ca-gov.zoomgov.com/my/sscdep28>
To join by phone dial (833) 568-8864 ID 16039062174*

Counsel for Plaintiff is directed to notice all parties of this order.

SUPERIOR COURT OF CALIFORNIA, COUNTY OF SACRAMENTO Gordon D Schaber Courthouse 720 Ninth STREET Sacramento, CA 95814-1311	
SHORT TITLE: Doe I vs. Sutter Health	
CLERK'S CERTIFICATE OF SERVICE BY MAIL (Minute Order)	CASE NUMBER: 34-2019-00258072-CU-BT-GDS

I certify that I am not a party to this cause. I certify that a true copy of the Minute Order was mailed following standard court practices in a sealed envelope with postage fully prepaid, addressed as indicated below. The mailing and this certification occurred at Sacramento, California, on 06/14/2022.

Clerk of the Court, by: /s/ V. Aleman, Deputy

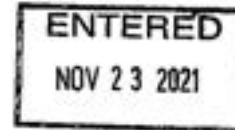
PAUL R KIESEL
KIESEL LAW LLP
8648 WILSHIRE BOULEVARD
BEVERLY HILLS, CA 90211-2910

CLERK'S CERTIFICATE OF SERVICE BY MAIL



D133503521

IN THE COURT OF COMMON PLEAS
HAMILTON COUNTY, OHIO



John Doe, on behalf of himself and all others similarly situated,	:	Case No.: A2002633
	:	
	:	
Plaintiff,	:	Judge Christian A. Jenkins
	:	
v.	:	
	:	Decision And Entry Granting In Part And
Bon Secours Mercy Health,	:	Denying In Part Defendant's Motion To
	:	Dismiss
Defendant.	:	

I. Procedural Background

Plaintiff filed a complaint on July 24, 2020. On August 28, 2020, defendant moved to dismiss for failure to state a claim pursuant to Civ.R. 12(B)(6). Defendant's motion was fully briefed on December 2, 2020 when plaintiff filed a motion for leave to file an amended complaint. Defendant opposed plaintiff's motion for leave to amend.

By entry docketed on February 12, 2021, the Court granted plaintiff's motion for leave to file an amended complaint. The Court deemed plaintiff's amended complaint filed as of said date.

Defendant filed a motion to dismiss plaintiff's amended complaint pursuant to Civ.R. 12(B)(6) on March 9, 2021. That motion is now fully briefed and ripe for decision.

II. Standard of Review

A motion to dismiss for failure to state a claim tests the sufficiency of the complaint. *Assn. for the Defense of the Washington Local School Dist. v. Kiger*, 42 Ohio St.3d 116, 117, 537 N.E.2d 1292 (1989). The material allegations in the complaint are taken as admitted, and all reasonable inferences must be drawn in favor of the nonmoving party. *Mitchell v. Lawson Milk Co.*, 40 Ohio St.3d 190, 192, 532 N.E.2d 753 (1988). Before the Court may dismiss the complaint, it must appear beyond doubt from the complaint that the plaintiff can prove no set of facts entitling



to recovery. *O'Brien v. University Community Tenants Union*, 42 Ohio St.2d 242, 327 N.E.2d 753 (1975).

III. Plaintiff's Allegations

The Court accepts the well-pleaded allegations set forth in the amended complaint to consider defendant's motion to dismiss. Plaintiff is a patient of defendant, a health care provider. (Amended Complaint ¶¶ 1-2). Defendant operates a website (i.e., www.mercy.com) that it encourages its patients to utilize. (*Id.* ¶¶ 4, 42). Defendant's website includes a "patient portal" through which patients can access medical records and test results and make appointments. *Id.* Plaintiff has visited and used www.mercy.com. (*Id.* ¶¶ 11, 154-159).

Plaintiff's Amended Complaint explains at length how a website can be designed to cause information about visitors to the website and their activity on the website to be provided to third parties such as Facebook and Google, and that defendant's site employs such tactics. (*Id.* ¶¶ 44-63). Plaintiff alleges that the information provided to third parties includes among other things: (1) information from which individual users can be identified by matching them to their Facebook accounts (*Id.* ¶¶ 64-73); (2) individual users' IP address and thereby their physical location (*Id.* ¶¶ 89-97); (3) the substance of individual users' searches on [mercy.com](http://www.mercy.com) (*Id.* ¶ 140); (4) whether a user logged into the mychart portal (*Id.* ¶ 149); (5) whether a user attempted to schedule a virtual visit (*Id.* ¶¶ 143-145); and (6) the pages visited on [mercy.com](http://www.mercy.com) by a user (*Id.* ¶ 142). The net effect according to plaintiff is that defendant discloses to Google, Facebook and others the identity of patients who visit [mercy](http://www.mercy.com) and the substance of their search and other activity on [mercy.com](http://www.mercy.com) (*Id.* ¶ 159).

Plaintiff alleges that the disclosure of such information is not necessary for the operation of [mercy.com](http://www.mercy.com), but rather that it enables defendant and others to engage in targeted marketing to

visitors to mercy.com that generates revenue for defendant. (*Id.* ¶¶ 180-181). Plaintiff alleges claims for disclosure of non-public medical information pursuant to *Biddle v. Warren Gen. Hosp.*, 86 Ohio St.3d 395, 715 N.E.2d 518 (1999), breach of confidence, invasion of privacy – intrusion upon seclusion, breach of contract, negligence and breach of fiduciary duty.

IV. Discussion

A. The Complaint Adequately Alleges A Claim Under *Biddle v. Warren General Hospital*.

In *Biddle*, the Ohio Supreme Court established a common law tort under Ohio law “for the unauthorized, unprivileged disclosure to a third party of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship.” *Id.* at 401. According to the Ohio Supreme Court, the *Biddle* decision represents an effort to provide a “legal identity” for “an evident wrongdoing” that Ohio courts had “shoehorned” into traditional legal theories. See *Menorah Park Center for Senior Living v. Rolston*, 164 Ohio St.3d 400, 2020-Ohio-6658, 173 N.E.3d 400, ¶ 14. Thus, a *Biddle* claim is properly evaluated in this broad light.

Defendant argues that plaintiff’s *Biddle* claim fails because: (1) no information learned through the physician-patient relationship was disclosed; (2) there was no disclosure of non-public medical information; and (3) public policy interests favoring the digitization of medical records and defendant’s First Amendment right to promote its services on its website outweigh any privacy interest of plaintiff implicated by the conduct alleged in this case. Defendant’s first two arguments fail based on the factual allegations in the Amended Complaint. Defendant’s third argument cannot be properly assessed on a motion to dismiss on the facts alleged in this case.

Defendant first notes that its website is available to anyone, not just its patients. (Defendant’s Memorandum in Support of Motion to Dismiss p. 2). No doubt this is true, but plaintiff is a patient. Plaintiff alleges he and other patients are encouraged by defendant to use its

website to obtain information about medical conditions, access medical records through the mychart portal and schedule appointments. While a non-patient may visit defendant's website to view some of the information thereon, in the absence of a physician-patient relationship with defendant, plaintiff and others would be unlikely to visit defendant's website to access their medical records or schedule appointments, actions that are allegedly disclosed to third parties. Plaintiff alleges that the information disclosed to third parties includes the fact that a visitor to defendant's website is a patient of defendant. (Amended Complaint ¶ 148).

Defendant also argues that visitors to its website are anonymous. (Defendant's Memorandum in Support of Motion to Dismiss p. 4). But this is contradicted by the Amended Complaint. Plaintiff alleges defendant's website deploys Facebook cookies to identify individual patients by matching them to their Facebook accounts. (Amended Complaint ¶¶ 70-71). Coupled with the other information allegedly disclosed such as IP address, user agent and browser fingerprint (*Id.* 89), the clear implication is that third parties are able to identify plaintiff and other patients of defendant and associate their identities with the data about their activity on defendant's website. (*Id.* 99-116). Plaintiff also alleges that defendant's website does not utilize available "anonymization" tools to protect the identities of visitors to its website. (*Id.* 126). One of the authorities relied on by defendant aptly summed up the net effect of these allegations by noting that by "[u]sing these techniques, Facebook can identify individual users and watch as they browse third-party websites . . ." *Smith v. Facebook*, 262 F.Supp.3d 943, 948 (N.D.Ca.2017).

The real question before the Court at this juncture is whether the aggregated information allegedly disclosed to third parties could conceivably constitute information learned within the physician-patient relationship so as to state a claim at this stage of the proceedings. In *Biddle*, the hospital's law firm requested four pieces of information to assess patients for social security

disability eligibility – name, telephone number, age and medical condition. *Biddle*, 86 Ohio St.3d at 396. The information allegedly disclosed in this case appears to be potentially more extensive when considered collectively. (Amended Complaint ¶¶ 134-153). Plaintiff has used defendant's website to research his and his wife's medical conditions, make appointments and access his medical records. (*Id.* 155-156). These actions were purportedly disclosed to third parties. (*Id.* 78-80). According to the allegations of the Amended Complaint, this means that searches for plaintiff's conditions and/or visits to pages containing information about such conditions have been disclosed to third parties and associated with identifying information about plaintiff. The sum and substance of such disclosures appears at least equivalent to the information at issue in *Biddle*. None of this information would be publicly available if not for defendant's disclosure thereof. (*Id.* 164-167). Thus, the Court cannot say from the face of the Amended Complaint at this juncture that plaintiff can prove no set of facts that would support a *Biddle* claim.¹

With respect to defendant's disclaimer declaring that use of the website does not establish a physician-patient relationship, defendant seemingly misses the point of plaintiff's allegations. Plaintiff does not allege that he became a patient by accessing the website; he is an actual patient of defendant who, at defendant's suggestion, has used defendant's website. If in fact defendant caused the disclosure of nonpublic medical information about one of its patients through the

¹ Defendant's reliance on *Jenkins v. Metro Life Ins. Co.*, 171 Ohio St. 557, 173 N.E.2d 122 (1961) and *Evans v. Toledo Neurological Assocs.*, 2014-Ohio-4336, 20 N.E.3d 333 (6th Dist.) is misplaced. *Jenkins* involved application of the statutory testimonial privilege in a case involving a life insurance claim. The Ohio Supreme Court held that, under the privilege statute and in the context of a dispute about whether the decedent lied on a life insurance application, there was no privilege to prevent a physician from testifying about the fact that the decedent had seen the physician. *Jenkins* predates *Biddle* by 38 years and arises in a completely different context. It does not inform application of *Biddle* in this case. Likewise, *Evans* was a medical malpractice claim in which defense counsel provided a physician with medical records obtained in discovery for his review. The physician being consulted by defense counsel happened to be employed by the same hospital system where plaintiff received care and that he was suing for medical malpractice. There is no allegation in this case that the information allegedly disclosed was provided to third parties other than as a result of the actions of defendant that caused such disclosures. Accordingly, *Evans* is unhelpful.

operation of its website, its self-serving proclamation that use of the website is not part of the physician-patient relationship does not in this Court's view make it otherwise. Thus, the existence of a physician-patient relationship is established for purposes of the current analysis.

Finally, defendant argues that its alleged disclosures are permitted because public policy interests advanced by such disclosures outweigh plaintiff's interest in confidentiality. Defendant relies primarily on the Ohio Supreme Court's decision in *Menorah Park* holding that disclosure of the minimum information necessary to pursue a collection action against a patient is permissible. The *Menorah Park* court based its holding on language in the *Biddle* decision recognizing that "special situations may exist where the interest of the public, the patient, the physician, or a third person are of sufficient importance to justify the creation of a conditional or qualified privilege to disclose in the absence of any statutory mandate or common-law duty." *Biddle*, 86 Ohio St.3d at 402.

In the absence of a statutory mandate or common law duty requiring disclosure, the *Menorah Park* court looked "to HIPAA for guidance in determining how those competing interests should be weighed." *Menorah Park*, 2020-Ohio-6658 at ¶ 32. Federal regulations promulgated pursuant to HIPAA expressly permit disclosure of protected health information "for treatment, payment, or health care operations." 45 C.F.R. 164.502(a)(1)(ii). The *Menorah Park* court went on to find public policy support for a payment-related exception in R.C. 3798.04, which prohibits unauthorized disclosure "except when the use or disclosure is required or permitted without such authorization [under HIPAA regulations]." *Menorah Park* at ¶ 33. Based on these clear recognitions of public policy under which disclosure may be proper, the *Menorah Park* court recognized a qualified privilege under which physicians and hospitals may disclose the minimum amount of patient information necessary to pursue a collection action. *Id.* at ¶ 35.

Looking to HIPAA regulations for guidance as in *Menorah Park* does not yield the same result in this case. HIPAA permits limited disclosures for treatment, payment or health care operations. The alleged disclosures in this case clearly do not facilitate treatment or payment, and review of the regulation defining “health care operations” is equally unavailing. See 45 C.F.R. § 164.501.

Without a statute or regulation expressly recognizing that plaintiff’s privacy interests are outweighed by a policy interest advanced by the disclosures at issue, defendant argues that federal policy favoring the digitization of medical records and defendant’s First Amendment commercial speech rights supply countervailing policy interests. Perhaps they do, but unlike *Menorah Park*, the connection between defendant’s asserted policy interests and the disclosures in this case are far from clear. See e.g. *Turk v. Oiler*, 732 F.Supp.2d 758, 776 (N.D. Ohio 2010) (declining to grant judgment on the pleadings where defendant asked court to “extend the countervailing interests doctrine”).

To be sure there is a public policy interest in making the delivery of healthcare more effective, efficient and less costly through widespread adoption of electronic medical records. But defendant has failed to sufficiently articulate how that interest is advanced by the disclosure of information about plaintiff’s and others’ activity on defendant’s website to third parties to warrant dismissal as a matter of law. Likewise for defendant’s First Amendment argument, unlike the *Menorah Park* court that could look to an unambiguous federal regulation recognizing that the policy interest in allowing providers to pursue payment outweighs patient confidentiality, defendant’s claimed commercial speech interests are simply too nebulous and undeveloped at this stage of the proceedings for this Court to hold as a matter of law that plaintiff cannot establish any facts that might entitle him to relief. This is in accord with the decision of the Cuyahoga County

Court of Common Pleas in an analogous case. *See Jane Doe v. University Hospital Health System, Inc.*, Cuyahoga C.P. No. CV-20-933357 (June 25, 2021).

Plaintiff has adequately alleged a claim under *Biddle v. Warren General Hospital*. Defendant's motion to dismiss is denied with respect to Count I of the Amended Complaint.

B. Breach of Confidence

Count II of the Amended Complaint alleges a claim for "breach of confidence." This count appears to be a verbatim restatement of the *Biddle* claim stated in Count I. Subsequent to *Biddle* it is unnecessary to "shoehorn a breach-of-confidence theory of recovery into many traditional legal theories . . ." *Menorah Park*, 2020-Ohio-6658, ¶ 14. This claim is duplicative of Count I and is therefore subsumed within it and unnecessary. Defendant's motion to dismiss is granted with respect to Count II of the Amended Complaint.

C. Invasion of Privacy – Intrusion Upon Seclusion

Ohio law recognizes the common law tort of invasion of privacy by intrusion upon seclusion where the defendant intentionally intrudes upon the solitude or seclusion or the private affairs or concerns of another, and if such an intrusion would be highly offensive to a reasonable person. *See Housh v. Peth*, 165 Ohio St. 35, 133 N.E.2d 340 (1956), syllabus. Defendant cites *Moran v. Lewis*, 2018-Ohio-4423, 114 N.E.3d 1254, ¶ 5 (8th Dist.) ("In order to properly plead an invasion of privacy claim, there must be allegations that the tracking invaded the seclusion or private affairs of another."). Defendant argues that there was no intrusion in this case, especially not into any secluded or private place.

Moran v. Lewis involved a GPS tracker placed on the plaintiff's car that tracked his movement on public roads. The Eighth District Court of Appeals cited authorities noting that the tracking at issue had not "led to the disclosure of private facts" and there was "no evidence that the vehicle was driven into a private or secluded location where one would have a reasonable

expectation of privacy.” *Id.* at ¶ 10, citing *Troeckler v. Zelser*, S.D.Ill. No. 14-cv-40-SMY-PMF, 2015 WL 1042187, *3 (March 5, 2015) and *Villanova v. Innovative Investigations, Inc.*, 21 A.3d 650, 652, 420 N.J.Super. 353 (2011). The *Moran* court held that “[t]he mere act of monitoring another’s public movements through the attachment of a GPS tracking device is not, in and of itself, sufficient to state an invasion of privacy claim.” *Id.* at ¶ 11.

Moran is not analogous to this case. Plaintiff’s public movements were not tracked, rather his online engagement with his healthcare provider was allegedly disclosed to third parties. As discussed above, this included the substance of searches for medical conditions that plaintiff submitted on defendant’s website, plaintiff’s access of his medical records and scheduling of medical appointments.²

Indeed, intrusion upon seclusion is a heavily fact-dependent claim. An evidentiary record will likely reveal the substantive details of these disclosures for closer scrutiny, but for purposes of a motion to dismiss the allegations are sufficient. *See e.g. Demo v. Kirksey*, D.Md. No. 8:18-cv-00716-PX, 2018 WL 5994995, *6 (“the trier of fact [must] consider all the circumstances including the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion, as well as the intruder’s motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.”) (citations omitted). Defendant’s motion is denied with respect to Count III of the Amended Complaint.

² Distinguishing decisions like *Moran* involving only tracking in public spaces, courts have noted that other forms of electronic surveillance may be much more intrusive. For example, with respect to cell phone location data, Justice Sotomayor noted in a concurrence that “the time stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations.” *Carpenter v. U.S.*, 138 S.Ct. 2206, 2217, 201 L.Ed.2d 507 (2018), citing *U.S. v. Jones*, 556 U.S. 400, 415, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012). Based on the allegations of the Amended Complaint, which must be accepted as true, the net effect of the aggregated data allegedly disclosed in this case seems more akin to the latter than the former.

D. Breach of Contract

Plaintiff's breach of contract claim is not subsumed because the source of the obligation allegedly breached is a contract rather than the common law duty recognized in *Biddle*. However, the parties disagree about the substance of any alleged contract between patients who utilize defendant's website and defendant. Plaintiff contends that the HIPAA Notice of Privacy Practices contains contractually enforceable promises that defendant made to plaintiff and others, which defendant allegedly breached. (Amended Complaint ¶¶ 270-275). Plaintiff also contends that defendant breached the covenant of good faith and fair dealing implicit in contracts under Ohio law. (*Id.* ¶ 276). Defendant argues that the HIPAA Privacy Notice applies to patients' medical records and information communicated in connection with patients' healthcare but is inapplicable to the information allegedly disclosed in this case. The Court cannot resolve this disagreement in the context of a motion to dismiss on the record presented. Defendant's motion is therefore denied with respect to Count IV.

E. Negligence and Breach of Fiduciary Duty

Plaintiff alleges that defendant negligently breached its duty of confidentiality to plaintiff by disclosing the content of plaintiff's communications to third parties, and that plaintiff suffered damages. (Amended Complaint ¶¶ 289-294). Plaintiff also alleges that defendant has a fiduciary duty to its patients, including plaintiff, and that defendant breached that duty by engaging in the conduct alleged in the amended complaint. (*Id.* ¶¶ 295-303). Defendant argues that these claims are duplicative and are subsumed by plaintiff's *Biddle* claim.

To determine whether these claims are subsumed within plaintiff's *Biddle* claim, this Court questions whether a *Biddle* claim includes a claim for unintentional disclosure. If so, they are

subsumed within plaintiff's *Biddle* claim because these theories do not present distinct theories of recovery for plaintiff.

In *Scott v. Ohio Dept. of Rehab. & Corr.*, 2013-Ohio-4383, 999 N.E.2d 231, ¶ 29 (10th Dist.), the Tenth District Court of Appeals indicated in dicta that a *Biddle* claim could include a claim for negligent disclosure. In *Sheldon v. Kettering Health Network*, 2015-Ohio-3268, 40 N.E.3d 661, the Second District Court of Appeals considered whether a *Biddle* claim could be maintained against a health care provider where an employee allegedly abused his position to disclose his ex-spouse's medical information. Plaintiff did not specifically state a *Biddle* claim and alleged that the medical provider was negligent in failing to detect and prevent the disclosure. The court analyzed plaintiff's claims under *Biddle* and concluded that "an inadvertent disclosure might, under different facts, fulfill the elements of *Biddle*, [but] the present case does not." *Id.* at ¶¶ 32-33.

In *Herman v. Kratche*, 8th Dist. Cuyahoga No. 86697, 2006-Ohio-5938, the Court of Appeals analyzed a *Biddle* claim based on a "mistaken" disclosure as a breach of fiduciary duty relying on *Hammonds v. Aetna Cas. & Sur. Co.*, 243 F. Supp. 793 (N.D. Ohio 1965). The Eighth District held that a medical provider owes a patient a fiduciary duty and reasoned that "a claim for breach of fiduciary duty is basically a claim of negligence, albeit involving a higher standard of care." *Herman* at ¶ 18 (citations omitted). On this basis the Court of Appeals reversed summary judgment in favor of the medical provider. *Id.* at ¶ 39.

The result is a continuing lack of clarity with respect to whether and under what circumstances an unintentional disclosure can support a *Biddle* claim. It is the opinion of this Court that *Biddle* does not require intentional disclosure to support a claim. *Biddle* does not expressly require intentional conduct. The *Scott* court held that an unintentional disclosure claim

can be theoretically maintained under *Biddle*, but not on the facts presented in *Scott*. And no court seems to have clearly held that a disclosure must be intentional to support a *Biddle* claim. Accordingly, defendant's motion to dismiss is granted with respect to Counts V and VI of the Amended Complaint, with the caveat that plaintiff's *Biddle* claim can proceed based on intentional and/or negligent conduct if supported by the evidentiary record to be developed as this matter proceeds.

V. Conclusion

For all the foregoing reasons, defendant's motion to dismiss is granted with respect to Count II, V and VI of the Amended Complaint and denied with respect to Counts I, III and IV of the Amended Complaint.

So ordered.

Date: 8/22/21



Judge Christian A. Jenkins



COURT OF COMMON PLEAS
CUYAHOGA COUNTY

JANE DOE,)	Case No. CV-20-933357
)	
Plaintiff,)	JUDGE J. PHILIP CALABRESE
)	
v.)	
)	
UNIVERSITY HOSPITALS HEALTH)	
SYSTEM, INC.,)	
)	
Defendant.)	

FILED
NOV 16 2020
Clerk of Courts
Cuyahoga County, Ohio

OPINION AND ORDER

Plaintiff Jane Doe, proceeding anonymously at this point in the proceedings by agreement of the parties due to the confidential health information underlying the allegations in the complaint, claims that Defendant University Hospitals Health System, Inc. disclosed her confidential health information to Facebook, Google, Microsoft, and other technology and data companies when she used the hospital’s website. Defendant moves to dismiss, arguing that Jane Doe lacks standing and that Plaintiff’s complaint fails to state claims under *Biddle v. Warren General Hospital*, 86 Ohio St.3d 395, 1999-Ohio-115, 715 N.E.2d 518, or for intrusion upon seclusion. For the reasons that follow, the Court concludes that Plaintiff has standing and so DENIES Defendant’s motion to dismiss on that ground. Pending the Ohio Supreme Court’s forthcoming decision in *Menorah Park Center for Senior Living v. Rolston*, 159 Ohio St.3d 1405, 2020-Ohio-3206, 146 N.E.3d 582, the Court defers ruling on the balance of Defendant’s motion to dismiss.

PLAINTIFF’S ALLEGATIONS

Plaintiff’s complaint contains lengthy and detailed allegations about claimed information-sharing between Defendant’s website and various technology and data companies through the use of certain source code, cookies, and browser fingerprints. According to the complaint, various

information shared with or available to the technology and data companies through these means contains or transmits personally identifiable health and similar information. This information allegedly allows technology and data companies to market to those who use Defendant's website or engage in other data mining.

In her complaint, Jane Doe alleges that she is a patient receiving treatment for an unspecified illness at University Hospitals and uses the patient portal on Defendant's website. (Complaint at ¶ 12.) Plaintiff avers that the specific communications she exchanged with University Hospitals through its website include "communications about specific appointments, providers, conditions and treatments." (Complaint at ¶ 173.) She also alleges that she "registered for, used, and exchanged communications with UH inside the MyUHCare patient portal." (Complaint at ¶ 172.) Further, the complaint alleges that the source code of a different domain that hosts the patient portal for University Hospitals causes "data transmissions from patient computers to Google connected to personally identifiable information about patients." (Complaint at ¶ 165.) This information, according to the complaint, constitutes confidential information entitled to privacy protections under State and federal law. Beyond these facts, the complaint scarcely contains any additional information regarding the information Jane Doe claims Defendant improperly disclosed.

Plaintiff's complaint asserts three causes of action. Count I alleges disclosure of non-public medical information under *Biddle*. Count II asserts a claim for breach of confidence, and Count III alleges intrusion on seclusion. Additionally, Plaintiff seeks to maintain this action on behalf of a class of "Ohio residents who are, or were, patients of UH or any of its affiliates, and who used UH's web properties, including but not limited to, [*sic*] www.uhhospitals.org and the Patient Portal at MyUHCare." (Complaint at ¶ 224.)

ANALYSIS

The Eighth District set forth the governing standard under which this Court considers a motion to dismiss pursuant to Rule 12(B)(6) as follows:

Under the notice pleading requirements of Civ.R. 8(A)(1), the plaintiff need only plead sufficient, operative facts to support recovery under his claims. *Doe v. Robinson*, 6th Dist. Lucas No. 1-07-1051, 2007-Ohio-5746, ¶ 17. Nevertheless, to constitute fair notice, the complaint must still allege sufficient underlying facts that relate to and support the alleged claim, and may not simply state legal conclusions. See *DeVore v. Mut. of Omaha Ins. Co.*, 32 Ohio App.2d 36, 38, 288 N.E.2d 202 (7th Dist.1972).

Henderson v. State, 8th Dist. Cuyahoga No. 101862, 2015-Ohio-1742, ¶ 10. “[W]hen a party files a motion to dismiss for failure to state a claim, all the factual allegations of the complaint must be taken as true and all reasonable inferences must be drawn in favor of the nonmoving party.”

Kennedy v. Dottore, 8th Dist. Cuyahoga No. 108562, 2020-Ohio-3451, ¶ 30.

I. Standing

“The Ohio Constitution expressly requires standing for cases filed in common pleas courts.” *ProgressOhio.org, Inc. v. JobsOhio*, 139 Ohio St.3d 520, 2014-Ohio-2382, 13 N.E.3d 1101, ¶ 11. A court of common pleas may only exercise jurisdiction over “justiciable matters.” Ohio Constitution, Article IV, Section 4(B). To present a justiciable controversy, a plaintiff must have standing to sue. *Federal Home Loan Mtge. Corp. v. Schwartzwald*, 134 Ohio St.3d 13, 2012-Ohio-5017, 979 N.E.2d 1214, ¶ 41.

To have standing, a plaintiff must show that she has suffered an injury fairly traceable to the defendant’s allegedly unlawful conduct that is likely to be redressed through the relief requested. *Estate of Mikulski v. Centerior Energy Corp.*, 2019-Ohio-983, 133 N.E.3d 899, ¶ 59 (8th Dist.), citations omitted. “Perhaps the most basic requirement to bringing a lawsuit is that the plaintiff suffer some injury. Apart from a showing of wrongful conduct and causation, proof of

actual harm to the plaintiff has been an indispensable part of civil actions.” *Felix v. Ganley Chevrolet, Inc.*, 145 Ohio St.3d 329, 2015-Ohio-3430, 49 N.E.3d 1224, ¶ 36. Injury results from “an invasion of a legally protected interest that is concrete and particularized, as well as actual or imminent, not hypothetical or conjectural.” *City of Athens v. Testa*, 2019-Ohio-277, 119 N.E.3d 469, ¶ 60 (10th Dist.), quotations omitted. Plaintiff’s attempt to proceed on behalf of a class does not change this threshold standing requirement. *Estate of Mikulski* at ¶ 60, quotation omitted. Indeed, “[i]ndividual standing is a threshold to all actions, including class actions.” *Id.*

Defendant makes two separate arguments that Plaintiff lacks standing. The Court addresses each in turn.

I.A. The Allegations of the Complaint

Defendant maintains that Plaintiff fails to allege concrete and particularized injury in fact. Instead, according to this argument, the complaint details the operation of the website of University Hospitals and its alleged disclosure of protected health information to third parties. In this way, Defendant contends that the complaint presents circumstances involving hypothetical patients or visitors to the website or patient portal. In light of the complaint’s voluminous allegations about the technology at issue and the comparatively few facts alleged about Jane Doe herself, Defendant makes an understandable, though misplaced, argument.

Plaintiff pleads that she is a patient of University Hospitals who communicated with the hospital through its website about specific conditions, appointments, and providers. (Complaint at ¶ 12, 173.) Similarly, she alleges that she exchanged communications with the hospital through the patient portal. (Complaint at ¶ 172.) Although she fails to identify specific protected information or data allegedly disclosed to third parties, one may fairly infer from the allegations of the complaint that transmission of Jane Doe’s private data is at least plausible. Construing these

allegations in Plaintiff's favor, as the Court must at this stage of the proceedings, the complaint pleads sufficient operative facts under Ohio's notice pleading requirements that Jane Doe has allegedly suffered an injury in fact.

I.B. Economic Harm

Defendant also argues that Plaintiff cannot establish standing based on generic allegations that the personal data and information at issue may have value in the marketplace. University Hospitals pins this argument on the absence of any allegation that Jane Doe has lost value in her data. Defendant's position misunderstands Plaintiff's claims. The complaint does not allege unjust enrichment, loss of value of her data, or another sort of claim rooted in pecuniary value. Instead, Plaintiff asserts privacy claims. Valuing such an injury, if proved, may present challenges, but any such difficulties do not warrant dismissal at the pleading stage.

II. Motion to Dismiss the Three Counts of the Complaint

In *Menorah Park Center for Senior Living v. Rolston*, 159 Ohio St.3d 1405, 2020-Ohio-3206, 146 N.E.3d 582, the Ohio Supreme Court *sua sponte* ordered post-argument briefing on whether to overturn or modify *Biddle* in light of the enactment of certain provisions of the Health Insurance Portability and Accountability Act of 1996, Pub.L. No. 104-191, 110 Stat. 1936. Because the Ohio Supreme Court's ruling may well bear on each of Plaintiff's claims, the Court defers ruling on Defendant's motion to dismiss the three counts of the complaint at this time. Doing so will not prejudice the parties because the Ohio Supreme Court's ruling will likely come before the end of the year. Once it does, the Court requests the parties to submit supplemental briefs, not to exceed fifteen pages, by January 18, 2021 on how, if at all, the Ohio Supreme Court's ruling affects Plaintiff's claims. Alternatively, the parties may advise that they are standing on their previous briefing on Defendant's motion to dismiss the three counts of the complaint.

CONCLUSION

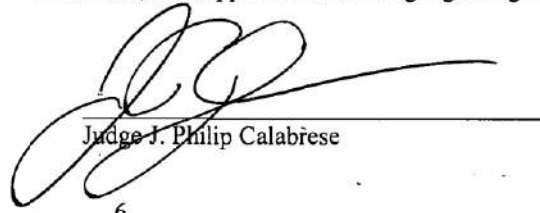
For the foregoing reasons, the Court concludes that the allegations of the complaint establish that Jane Doe has standing. Following the Ohio Supreme Court's forthcoming ruling on whether to overturn or modify *Biddle*, the Court requests supplemental briefing from the parties on how, if at all, the ruling affects the claims in this case.

If Plaintiff's claims survive the Ohio Supreme Court's ruling, it may turn out in discovery that the evidence does not support Jane Doe's factual allegations. Because of the costs and burdens associated with discovery of the technological matters underlying Plaintiff's claims and the likely scope of such discovery Plaintiff will seek, the Court directs the parties to direct their discovery efforts to those matters relating specifically to Jane Doe's use of Defendant's website and the patient portal first. If discovery shows that Defendant has not in fact transmitted Jane Doe's personal health information to any technology or data company as alleged, then an early summary judgment may be appropriate in this case or Plaintiff may lack standing to maintain her claims in whole or in part. On the other hand, if discovery tends to corroborate Jane Doe's factual allegations, then the case may proceed with that assurance. Such an approach is consistent with the proportionality requirement of Rule 26(B)(1) and the mandate of Rule 1(B).

ORDER:

For the foregoing reasons, the Court DENIES Defendant's motion to dismiss for lack of standing and defers ruling on the balance of Defendant's motion to dismiss pending the Ohio Supreme Court's forthcoming ruling in *Menorah Park Center for Senior Living v. Rolston*, 159 Ohio St.3d 1405, 2020-Ohio-3206, 146 N.E.3d 582, and supplemental briefing regarding the same.

Dated: November 16, 2020



Judge J. Philip Calabrese



FILED

**IN THE COURT OF COMMON PLEAS
CUYAHOGA COUNTY, OHIO**

JUN 28 2021

Clerk of Courts
Cuyahoga County, Ohio

JANE DOE, ON BEHALF OF HERSELF AND ALL
OTHERS, ETC
Plaintiff

Case No: CV-20-933357

Judge: WILLIAM F. B. VODREY

UNIVERSITY HOSPITALS HEALTH SYSTEM, INC.
Defendant

JOURNAL ENTRY

THIS CASE IS BEFORE THE COURT ON DEFENDANT'S MOTION TO DISMISS. FOR THE REASONS STATED IN THE ATTACHED DECISION, DEFENDANT'S MOTION TO DISMISS IS HEREBY DENIED.

 6-25-21
Judge Signature Date

06/25/2021

Page 1 of 1

IN THE COURT OF COMMON PLEAS
CUYAHOGA COUNTY, OHIO

JANE DOE, ON BEHALF OF HERSELF)	CASE NO. CV-20-933357
AND ALL OTHERS, ETC)	
)	Judge: WILLIAM F.B. VODREY
Plaintiff,)	
)	
v.)	
)	<u>JOURNAL ENTRY</u>
UNIVERSITY HOSPITAL HEALTH)	
SYSTEM, INC.)	
)	
Defendant.)	


This case is before the court on defendant's motion to dismiss. On Nov. 16, 2020, the court issued an order that denied defendant's motion to dismiss on the grounds that plaintiff lacked standing. At that time, the court deferred ruling on defendant's motion to dismiss the three counts of plaintiff's complaint pending the Supreme Court of Ohio's decision in *Menorah Park Center for Senior Living v. Rolston*, 159 Ohio St.3d 1405, 2020-Ohio-3206, 146 N.E.3d 582. The parties have completed supplemental briefing on the issue, and the remainder defendant's motion to dismiss is now ripe for review.

In *Menorah Park*, the Supreme Court of Ohio, *sua sponte*, ordered post-argument briefing on whether the court should overturn or modify its previous decision in *Biddle v. Warren General Hospital*, 86 Ohio St.3d 395, 1999-Ohio-115, 715 N.E.2d 518, in light of the enactment of certain provisions of the Health Insurance Portability and Accountability Act of 1996, Pub.L. No. 104-191, 110 Stat. 1936. The court held that "*Biddle* remains good law and it continues to permit a cause of action for the unauthorized, unprivileged disclosure to a third party of nonpublic medical information." *Menorah* at ¶40.

A Civ.R. 12(B)(6) motion to dismiss for failure to state a claim upon which relief can be granted tests the legal sufficiency of the complaint. *State ex rel. Hanson v. Guernsey Cty. Bd. of Comms.*, 65 Ohio St.3d 545, 548, 605 N.E.2d 378 (1992). A complaint is subject to dismissal for failure to state a claim upon which relief can be granted when it appears beyond doubt that plaintiff can prove no set of facts in support of his or her claim that would entitle plaintiff to relief. *Doe v. Archdiocese of Cincinnati*, 109 Ohio St.3d 491, 2006-Ohio-2625, 849 N.E.2d 268, ¶11. When considering a Civ.R. 12(B)(6) motion, the court must construe all factual allegations of the complaint as true, and all reasonable inferences shall be drawn in favor of the nonmoving party. *York v. Ohio State Highway Patrol*, 60 Ohio St.3d 143, 144, 573 N.E.2d 1063 (1991).

Here, in accepting plaintiff's allegations as true and acknowledging the Supreme Court of Ohio's ruling in *Menorah Park*, the court finds that plaintiff has adequately stated claims upon which relief can be granted. Defendant's motion to dismiss is hereby denied.

In accordance with this court's prior order on Nov. 16, 2020, the court hereby orders the parties to direct their initial discovery efforts to those matters relating specifically to Jane Doe's use of defendant's website and patient portal. If discovery reveals that defendant did not, in fact, transmit her personal health information to any technology or data company as alleged, an early motion for summary judgment may then be appropriate.

 6-25-21
William F.B. Vodrey, Judge

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT DEPARTMENT
CIVIL ACTION NO. 1984CV01651-BLS1

JOHN DOE AND JANE DOE,
INDIVIDUALLY AND ON BEHALF OF
ALL OTHERS SIMILARLY SITUATED,

Plaintiffs,

v.

PARTNERS HEALTHCARE SYSTEM, INC.,
THE GENERAL HOSPITAL
CORPORATION D/B/A MASSACHUSETTS
GENERAL HOSPITAL, BRIGHAM,
HEALTH INC., AND DANA-FARBER
CANCER INSTITUTE, INC.,

Defendants.

AFFIDAVIT OF JANE MURRAY

I, Jane Murray, state and affirm that the following is true to the best of my knowledge and belief:

1. I am the Vice President of the Data and Analytics Organization at Mass General Brigham Incorporated (“MGB”). I previously served as the Executive Director of the MGB Data and Analytics Organization. I have served in these roles for approximately three years.

2. My job responsibilities in the MGB Data and Analytics Organization include: direct management of the Epic Cogito Analytics Team, Product Management Team, and the Service Operations Team. Together with the teams, I am responsible for engaging with MGB executives to provide data and analytics products to support data driven decision making across clinical, administrative, finance operations, quality, safety and population health management domains. My teams are also responsible for central data and analytic service operations.

3. As part of my oversight responsibilities, I manage and supervise the work of the MGB Data and Analytics Organization, which includes specialists dedicated to support MGB's electronic medical record system, which is licensed from Epic Systems Corporation. I am active in the management of the data and reporting functionality of MGB's electronic medical record platform, although I did not create, program, or support the actual medical record system.

4. The entities owned or operated by MGB include those entities set forth in the Settlement Agreement attached to Plaintiffs' Assented To Motion For Preliminary Class Action Settlement Approval submitted to the Court, reproduced here:

- Brigham and Women's Faulkner Hospital, Inc.
- Brigham and Women's Hospital, Inc.
- Brigham and Women's Physicians Organization, Inc.
- Cooley Dickinson Healthcare Corporation
- Cooley Dickinson Hospital, Inc.
- The General Hospital Corporation, D/B/A Massachusetts General Hospital
- Harbor Medical Associates, Inc.
- Lincoln Physicians
- Martha's Vineyard Hospital, Inc.
- Mass General Brigham Community Physicians, Inc.
- Mass General Brigham Home Care, Inc.
- Mass General Brigham Specialty Pharmacy, Inc.
- Mass General Brigham Urgent Care, LLC
- Massachusetts Eye and Ear Associates, Inc.
- Massachusetts Eye and Ear Infirmary
- Massachusetts General Physicians Organization, Inc.
- The McLean Hospital Corporation
- Middlesex Cardiology
- Mystic Healthcare
- Nantucket Cottage Hospital
- Nantucket Physician Organization, Inc.
- Newton-Wellesley Hospital
- Newton-Wellesley Medical Group, Inc.
- North Shore Medical Center, Inc., D/B/A Salem Hospital
- North Shore Physicians Group, Inc.
- Pentucket Medical
- Spaulding Hospital Cambridge, Inc.
- Spaulding Nursing and Therapy Center Brighton, Inc.
- The Spaulding Rehabilitation Hospital Corporation
- Rehabilitation Hospital of the Cape and Island Corporation
- Spaulding Rehabilitation, Inc.
- Wentworth-Douglass Hospital
- Wentworth-Douglass Physician Corporation
- Westford Internal Medicine
- Windemere Nursing and Rehabilitation Center

5. Within the Epic medical record system, MGB maintains the electronic medical records for each of its owned or operated entities within one general category or classification (the “MGB Owned/Operated Data Set”).

6. The MGB Owned/Operated Data Set is the general category or classification within Epic that contains the scheduling and encounter data for patients of MGB’s owned or operated entities.

7. The MGB Owned/Operated Data Set is used in the normal course of MGB’s business to identify the patients of MGB’s owned or operated entities. This is the central repository for all clinical and revenue cycle enterprise operations within the MGB system, relied upon by MGB in the normal course of its business.

8. The data within the MGB Owned/Operated Data Set contains information from the time each entity became a MGB owned or operated entity, and was enrolled in, and transitioned onto, the Epic electronic medical record platform. The transition of historical data, including the timeframes of such data, onto the Epic electronic medical record platform varied from entity to entity.

9. The MGB Owned/Operated Data Set is the single source relied upon by MGB to identify aggregate patient encounter data.

10. The Settlement Agreement defined the Settlement Class as: “All Persons who, within the Class Period, were Patients of any of the Defendants and visited the Informational Websites, and are either (a) a resident of Massachusetts, and/or (b) received medical care in Massachusetts at any of the Defendants.”

11. The Settlement Agreement defined “Patient” as “any Person who obtained medical care from any of the Defendants.”

12. The Settlement Agreement defined “Person” as “a living natural person who is not an employee of any of the Defendants and who is resident in the United States.”

13. In order to ascertain potential Settlement Class members that were patients of, and had encounters with, any MGB owned or operated entity, I instructed members of my team to extract data from the MGB Owned/Operated Data Set, in which the owned or operated entities’ electronic medical record and scheduling data resides. I provided the logic and am familiar with the coding protocol used to extract the data from the Epic system, and performed quality control checks on the results.

14. To identify those individuals that may be class members, my team applied “filters” to the MGB Owned/Operated Data Set within the Epic system. The resulting list contained 2,813,119 unique individuals (the “Potential Class Member Notice List”). The filters used to create the Potential Class Member Notice List are described further below.

15. My team applied a time frame filter to the MGB Owned/Operated Data set of May 23, 2016 to July 31, 2021, to identify unique patient encounters at any MGB owned or operated entity during that time period.

16. My team set the filters to include patients of all ages of any MGB owned or operated entity, so that individuals were not excluded from the Potential Class Member Notice List based on their age.

17. My team also set the filters to include all visit types at any MGB owned or operated entity, so that individuals were not excluded from the Potential Class Member Notice List based on the type of encounter they had with any MGB owned or operated entity.

18. My team applied filters to exclude deceased individuals and MGB employees, so that those individuals were not included on the Potential Class Member Notice List.

19. On August 26, 2021 my team generated a report from the Epic system, which resulted in the Potential Class Member Notice List.

20. The size of the Potential Class Member Notice List required that my team generate the report in multiple files. My team exported the report into four “.csv” files, in accordance with the settlement administrator’s instruction.

21. The files comprising the Potential Class Member Notice List were ordered alphabetically by patient last name – file A to C identified 583,530 individuals and addresses, file D to H identified 626,232 individuals and addresses, file I to O identified 738,514 individuals and addresses, and file P to Z identified 864,843 individuals and addresses.

22. To facilitate the settlement administrator’s distribution of the settlement notices, the Potential Class Member Notice List included individuals whose address information within the MGB Owned/Operated Data Set on the Epic system was either incomplete, or referred to or included non-United States address information.

23. MGB completed the submission of the Potential Class Member Notice List files to the settlement administration on September 10, 2021, through their secure portal, in accordance with their instruction.

Signed under the pains and penalties of perjury on this 4 day of January, 2022.


Jane Murray

CERTIFICATE OF COMPLIANCE

I, Patrick J. Vallely, hereby certify that the foregoing brief complies with the rules of court that pertain to the filing of briefs, including, but not limited to:

Mass. R. App. Proc. 16(a)(13) (addendum);

Mass. R. App. Proc. 16(e) (references to the record);

Mass. R. App. Proc. 18 (appendix to the briefs);

Mass. R. App. Proc. 20 (form and length of briefs and other documents); and

Mass. R. App. Proc. 21 (redaction).

I further certify that the foregoing brief complies with the applicable length limitation in Mass. R. App. Proc. 20 because it is produced in proportional Times New Roman font at size 14 point and contains 10,976 total words among those parts of the brief specified in Mass. R. App. Proc. 16(a)(5)-(11), as counted using the word count feature of Microsoft Word for Microsoft 365 v.2402 plus a manual counting of words depicted in three website images replicated in the statement of facts.

Dated: March 8, 2024

/s/ Patrick J. Vallely

SHAPIRO HABER & URMY LLP
Patrick J. Vallely (BBO #663866)
One Boston Place, Suite 2600
Boston, MA 02108
(617) 439-3939
pvallely@shulaw.com

CERTIFICATE OF SERVICE

Pursuant to Mass. R. App. Proc. 13(d), I hereby certify, under the penalties of perjury, that on March 8, 2024, I made service of this brief upon the attorney of record for each party, by email and the Electronic Filing System on:

David Quinn Gacioch
MCDERMOTT WILL & EMERY LLP
200 Clarendon Street, Floor 58
Boston, MA 02116
(617) 535-4000
dgacioch@mwe.com

Dated: March 8, 2024

/s/ Patrick J. Vallely

SHAPIRO HABER & URMY LLP
Patrick J. Vallely (BBO #663866)
One Boston Place, Suite 2600
Boston, MA 02108
(617) 439-3939
pvallely@shulaw.com