No. 22-2110

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

COURTHOUSE NEWS SERVICE,

Plaintiff-Appellant,

v.

JACQUELINE C. SMITH, in her official capacity as the Clerk of the Circuit Court for Prince William County, Virgina, and THE COMMONWEALTH OF VIRGINIA

Defendants-Appellees.

On Appeal from the United States District Court
for the Eastern District of Virginia

RESPONSE BRIEF OF THE COMMONWEALTH OF VIRGINIA

JASON S. MIYARES
Attorney General
STEVEN G. POPPS
Deputy Attorney General
ROBERT B. MCENTEE, III
Assistant Attorney General
ERIN R. MCNEILL
Assistant Attorney General

Office of the Attorney General
202 North Ninth Street
Richmond, Virginia 23219
(804) 786-2071 – Telephone
(804) 786-1991 – Facsimile

ANDREW N. FERGUSON
Solicitor General
ERIKA L. MALEY
Principal Deputy Solicitor General
GRAHAM K. BRYANT
Deputy Solicitor General
M. JORDAN MINOT
Assistant Solicitor General

Counsel for Defendant-Appellee the Commonwealth of Virginia

April 20, 2023

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases

Statutes

Other Authorities

INTRODUCTION

Every circuit court in Virginia provides the public with contemporaneous access to civil court records, including newly filed complaints, at the courthouse. This practice fully complies with the qualified First Amendment right of access to certain judicial proceedings. *Courthouse News Serv. v. Schaefer*, 2 F.4th 318, 328 (4th Cir. 2021).

Courthouse News Service (CNS) contends, however, that Virginia violates the First Amendment because CNS cannot access most court records *online*. But the First Amendment does not guarantee CNS the right to access court records in the manner it deems most convenient and profitable.

That many Virginia circuit courts offer online access to certain government agencies and officers of the court does not create a constitutional requirement to provide online access to the public at large. Virginia designed its Officer of the Court Remote Access system (OCRA) to promote judicial efficiency while also protecting citizens' personal information by limiting the system to a small pool of closely vetted subscribers who work directly with the courts. OCRA was not designed to be a public system; its limits on access and dissemination are the

safeguards Virginia's General Assembly chose to protect the privacy of personal information. The experience of other public online databases in Virginia and elsewhere demonstrates that, without those measures, OCRA would be highly vulnerable to data mining. Data miners use automated computer programs, or "bots," to scan large databases of records quickly and extract personal information to sell. Criminals can then use the extracted information for malicious purposes such as identity theft, fraud, and financial exploitation. In-person access to records at the courthouse, by contrast, is far less vulnerable to such data mining tactics.

CNS argues that Virginia could offer the public online access to court records by adopting different measures to protect personal information, including expanding its redaction requirements, broadening the categories of cases deemed confidential, changing its subscriber agreements, and designing and implementing a variety of "bot management" tactics. But the system CNS proposes is not OCRA. In effect, CNS insists that the First Amendment requires Virginia to abandon its current system and implement a system tailored to CNS's business model. The First Amendment does not require Virginia to do so.

As the district court held, CNS's argument "amounts to advocating for Virginia to change its public policy—not a valid First Amendment violation claim—and the place for this argument is the Virginia General Assembly, not the federal judiciary." JA558. This Court should affirm.

JURISDICTIONAL STATEMENT

The district court had jurisdiction over CNS's constitutional claims via 28 U.S.C. § 1331. This Court has jurisdiction under 28 U.S.C. § 1291.

ISSUES PRESENTED

1. Whether there is a First Amendment right to online access to court records in addition to reasonably contemporaneous in-person access.

2. Whether Virginia's provisions regarding online access to court records satisfy the First Amendment because they are content-neutral and narrowly tailored to serve Virginia's important interests in the efficient functioning of its judiciary and the protection of personal information.

3. Whether the district court correctly dismissed CNS's equal protection claim because Virginia has a rational basis for providing

online access to court records to officers of the court but not the public at large.

STATEMENT

I. Factual Background

All Virginia circuit courts, including the Prince William Circuit Court, provide the public with reasonably contemporaneous access to non-confidential civil filings and other court records at the courthouse during business hours. JA81. For instance, the Prince William Circuit Court has terminals, located in the Civil Division, that the public can use to view and copy court records. JA81–82. These terminals are open to the public Monday through Friday, 8:30 a.m. to 5:00 p.m. JA81–82.

Virginia does not have a centralized system required for electronic filing or access to court records. See JA216–17. Instead, the clerks of each circuit court—who are independently elected constitutional officers, see Va. Const. art. VII, § 4—choose the technology systems for their court, JA216. Virginia's circuit courts vary greatly in size, resources, and technological capacity, ranging from populous urban areas to remote rural districts. JA216. Not all Virginia circuit courts currently have

electronic filing, and of the courts "currently offering e-filing in civil cases, user rates are very low." JA216.

Virginia law leave to the clerks of each circuit court the choice whether to provide online public access to court records. Clerks who choose to do so, however, must ensure that court records posted online do not contain several categories of sensitive personal information, including:

> (i) an actual signature, (ii) a social security number, (iii) a date of birth identified with a particular person, (iv) the maiden name of a person's parent so as to be identified with a particular person, (v) any financial account number or numbers, or (vi) the name and age of any minor child."

Va. Code § 17.1-293(B). At least one Virginia circuit court, the Alexandria Circuit Court, has created a proprietary public online access system. JA80, 166–69, 217–21. Most circuit courts, however, do not have a public online access system because ensuring that all sensitive personal information is properly redacted is time-consuming and costly for the circuit clerks, and can result in errors threatening the privacy of litigants or other third parties. JA137–38.

The Office of the Executive Secretary of the Supreme Court of Virginia (OES) provides administrative support to Virginia courts. JA82–

83. OES created and maintains certain technology systems, which circuit court clerks have discretion to use. JA82–83, 133–34. First, OES maintains a Case Imaging System (CIS), which allows participating circuit courts to create and store electronic images of case documents. JA83. OES also maintains OCRA. Clerks that use CIS can also make images of court documents available on OCRA. JA84.

Each clerk has discretion whether to use OCRA. Some circuit courts use other online court record systems created by private vendors; others do not use online systems at all. JA82, 86. If a clerk decides to use OCRA, "the circuit court clerk determines the scope of the clerk's records that will be made available through the OCRA application." JA134. Each clerk also separately handles subscriptions to OCRA; users must separately subscribe to OCRA, and pay a separate subscription fee, for each participating circuit court they wish to access. JA84. Each subscriber then has access to all of that court's online documents without paying any extra charges (such as a per-page printing fee). JA87. The Prince William Circuit Court currently participates in OCRA. It has a total of 551 subscribers, with 274 paying users. JA209. Any person may, however,

access civil records at the public access terminals at the courthouse more quickly after filing than they are posted to OCRA. JA477.

As its name suggests, OCRA—the Officer of the Court Remote Access system—was designed to provide access only for officers of the court: "members in good standing with the Virginia State Bar and their authorized agents, pro hac vice attorneys authorized by the court for purposes of the practice of law, and such governmental agencies as authorized by the clerk." Va. Code § 17.1-293(E)(7). To prevent an OCRA subscriber from simply downloading the entirety of a court's database and disseminating it online, Va. Code § 17.1-293(H) provides that no "data accessed by secure remote access [may] be sold or posted on any other website or in any way redistributed to any third party." It provides an exception that data accessed this way may be included in products or services provided to a third party of the subscriber as long as "(i) such data is not made available to the general public and (ii) the subscriber maintains administrative, technical, and security safeguards to protect the confidentiality, integrity, and limited availability of the data." *Ibid.* The regulations on dissemination do not apply if the records are obtained at a courthouse terminal.

OES also operates publicly available online records systems, including several Online Case Information Systems (OCIS) and the Virginia Date of Birth Confirmation (VDBC) system. JA128. The circuit court version of OCIS allows users to obtain docket information about cases in participating circuit courts, including listing the pleadings and orders that have been filed. JA128–29; see also *Online Services: Case Status and Information*, OES, https://tinyurl.com/58p34n5t (last visited Apr. 20, 2023). Circuit Court OCIS, however, does not provide online access to images of court records or the records' text. See generally *Circuit Court Case Information*, OES, https://tinyurl.com/4z4nnh2e (last visited Apr. 20, 2023). As with OCRA, the decision to participate in OCIS lies within the discretion of individual circuit clerks.

VDBC allows registered organizations to search OCIS to confirm if an individual is "associated with . . . criminal and traffic cases," provided that the individual consents to the search, for instance as part of an employer's background check. JA129–30. VDBC subscribers must agree not to use data mining, including "automated" searches or "attempting to gather information for purposes other than that for which the system was designed." JA130.

OES's public online systems, including OCIS and VDBC, "have all been, and continue to be, subjected to manual and/or automated data mining from around the world." JA129. "[A]nyone with rudimentary programming knowledge" can convert imaged documents "to searchable text, aggregate that data in a database, and subsequently search through the data for" personally identifiable information, or "PII." JA128. This practice is "known as 'data mining' or 'data harvesting.'" *Ibid.* It is typically done by "bots"—computer programs that can operate without input from a human user once they are activated. JA129; JA539. Bots can perform repetitive tasks much more quickly than a human. JA539. Bots have mined OCIS: "instead of searching for a few cases or names within a single session, the bots would enter searches for every single possible case number within the database, sequentially." JA129. The bots "would additionally make requests, per second, far faster than . . . a human." *Ibid.*

Similarly, even though the subscription agreement specifically prohibits automated searches, VDBC has also "been mined for data." JA130. Although VDBC does not display personal information, "by performing multiple searches based on guessed, partial data," the bots

"can piece together the PII." *Ibid.* For instance, "in order to discover the full date of birth, users and/or bots will enter a name, pick a starting year," and then search sequentially until data appears, allowing them to "discover[] the full birth date by process of elimination." *Ibid.*

OES has taken steps to block data mining, but "determined data miners" have "anticipated and circumvented" its efforts. JA130. For instance, if OES limits the numbers of searches, "[t]he bot will then adapt and search just under our algorithm's limit." *Ibid.* Further, "upon receiving a ban, a determined data harvester can simply reapply for access to the VDBC" using different credentials, which OES has "no real way to vet." JA130–31.

In jurisdictions that offer online public access to court records, court records have become a "major avenue[]" for data mining. JA330–32.[1]

[1] Citing Staff of S. Comm. on Commerce, Science, and Transportation, 113th Cong., A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes 15, 24 (Dec. 18, 2013), https://tinyurl.com/3k5y524f [hereinafter "Data Broker Report"]; Office of the Attorney General Department of Financial Regulation, Report to the Vermont General Assembly of the Data Broker Working Group (Dec. 15, 2017), https://tinyurl.com/2p9dvsev [hereinafter "Vermont Attorney General Report"]. Courts may take judicial notice of public records. *Philips v. Pitt Cnty. Memorial Hosp.*, 572 F3d 176, 180 (4th Cir. 2009).

Personal information from court records, including identifying information of crime victims and police officers, as well individual health information, have been mined and sold. JA331–32 (citing Data Broker Report, *supra*; Vermont Attorney General Report, *supra*). And despite being specifically designed for widespread public access, the federal Public Access to Court Electronic Records (PACER) system has also suffered from data mining. For instance, an "embittered former DEA informant" "min[ed] PACER for data on individuals who had plea-bargained in multiple Federal criminal cases," and published the "identities of . . . helpful informants" on "the website whosarat.com."[2]

On a larger scale, "commercial entities that aggregate and consolidate information from governmental and private sources . . . routinely mine court records for personally identifiable information they then incorporate with other data sources to create detailed dossiers on almost every American." David S. Ardia, *Privacy and Court Records: Online Access and the Loss of Practical Obscurity*, 2017 U. Ill. L. Rev.

[2] *Judicial Transparency and Ethics: Hearing Before the Subcomm. on Courts, Intellectual Property and the Internet of the H. Comm. on the Judiciary*, 115th Cong. 27 (2017) (testimony of Thomas R. Bruce) [hereinafter "House Judiciary Hearing"].

1385, 1388 (2017); see generally State of North Dakota Courts, *Supreme Court Suspends Remote Access to Court Records* (Jan. 23, 2020), https://tinyurl.com/7wenvkwz; April Baumgarten, *Remote Access to North Dakota Court Docs Unlikely to Return*, InForum (Jan. 31, 2021) (noting that North Dakota suspended remote access to court records "after media reports revealed millions of documents potentially contained sensitive information that was supposed to be redacted—like Social Security numbers, birth dates and credit card numbers"), https://tinyurl.com/3p8ph4u7.

Mined personal information is used in the commission of crimes, frauds, and other misconduct. Most notably, data mining enables identity theft, in which criminals use the victims' "personal information or financial information without [their] permission" to commit fraud. Federal Trade Comm'n, *What to Know About Identity Theft*, https://tinyurl.com/ycys97f5 (last visited Apr. 20, 2023). For instance, identity thieves may "buy things with [the victim's] credit cards," open "new credit cards in [the victim's] name," "steal [the victim's] tax refund" or other assets, or "pretend to be [the victim] if they are arrested." *Id.* An "estimated 23 million persons, or about 9% of all United States residents

age 16 or older" are victims of identity theft per year, suffering financial losses of more than $15 billion annually. U.S. Dep't of Justice, Bureau of Justice Statistics, Victims of Identity Theft, 2018 (Apr. 2021), https://tinyurl.com/32wepc2y.

Data mining also enables other types of fraud and exploitation. For example, data miners "sell products that identify financially vulnerable consumers" to "predatory businesses seeking to target" them. Data Broker Report at ii, 7. Data miners compile lists of personal information, with titles such as "Rural and Barely Making It," "Ethnic Second-City Strugglers," and "Young Single Parents," which they provide to predatory businesses that "sell high-cost loans and other financially risky products." *Id.* at ii. Data miners also compile lists of personal information identifying "Suffering Seniors" with dementia, used to "target elderly Americans with fraudulent sales pitches." *Id.* at 8. And they "sell[] lists of addresses and names of consumers suffering from conditions including cancer, diabetes, and depression." *Id.* at 5; see generally, *e.g.*, Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues i, 9–11 (Jan. 2016), https://tinyurl.com/mw2mu7jy (describing how even legal data mining can "[e]xpose sensitive information" and "[a]ssist

in the targeting of vulnerable consumers for fraud," ultimately "harm[ing] consumers, particularly low-income and underserved populations"); Geoffrey Xiao, *Bad Bots: Regulating the Scraping of Public Personal Information*, 34 Harv. J. L. & Tech 701, 711, 718–27 (2021) (discussing how "collection, aggregation, and analysis of public personal information create[s] a wide range of harms").

Because OCRA was not designed for public access, it lacks critical safeguards that a public system would need "to prevent unauthorized access to sensitive information such as social security numbers, dates of birth and financial account numbers." JA226. Filers are required to redact all but the last four digits of social security numbers, as well as certain other personal information such as credit card and bank account numbers. JA88. Some filers, however, "fail[] to protect the information within documents that are filed with the clerk." JA226. In addition, filers are not required to redact other sensitive personal information, including original signatures, dates of birth, parents' maiden names, names and ages of minor children, and certain financial account information. See Va. Code § 17.1-293(B). And again, any subscriber may "download every available nonconfidential court record containing personally identifiable

information" from a circuit court's OCRA system "from anywhere in the world," without paying additional fees. JA128.

OCRA instead safeguards data by tightly circumscribing subscriptions to approved government agencies and members of the Virginia bar. See p. 7, *supra*. Lawyers licensed in Virginia must satisfy a thorough character and fitness review and are also subject to Rules of Professional Conduct prohibiting the misuse of personal information. See Va. Sup. Ct. R. Pro. Conduct 1.6. They are subject to severe sanctions for violating Rules of Professional Conduct, including the loss of their professional license. See Va. Sup. Ct. R. Pro. Conduct 8.5; Va. Sup. Ct. R. Pt. 6, § 4, ¶ 13.

II. Procedural History

CNS is a for-profit news organization "specializing in reporting on civil litigation," including in Virginia. CNS Br. 12. Among other things, CNS charges subscribers for reports that summarize civil complaints. JA78.

CNS sued the Executive Secretary of the Supreme Court of Virginia and the Clerk of the Circuit Court for Prince William County, Virginia, alleging that "Virginia Code § 17.1-293, on its face and as-applied" is

unconstitutional because it "deprives CNS, and by extension its subscribers and the public, of their First Amendment right[s]" to access and disseminate court records. JA33–34. CNS further alleged that "Virginia Code § 17.1-293 . . . deprives CNS, and by extension its subscribers and the public, of their Fourteenth Amendment right to equal protection" because it "provid[es] remote online access to civil, nonconfidential, public court filings and other public court records to Virginia-licensed attorneys and their staff, . . . but depriv[es] that same access to others, including CNS." JA35–36.

The defendants moved to dismiss CNS's complaint. The court dismissed CNS's equal protection claim. Because "[n]on-attorneys are not a suspect class," and CNS "d[id] not argue that there is any fundamental right to access civil court records *remotely*," the court held rational basis review applied. JA73–74. Virginia has a "legitimate interest" in "protecting confidential and private information contained in the civil court records," and "it is, as a minimum, rational to believe that limiting OCRA access to attorneys would protect confidential and private information because attorneys are more easily regulated by the court system." JA74. The court therefore held that the equal protection claim

failed as a matter of law. It permitted, however, the First Amendment claims to proceed.

The parties then stipulated to the dismissal of the Executive Secretary, and Virginia intervened as a defendant. JA92–97. The parties filed cross-motions for summary judgment on the First Amendment claims. JA429, 534. Following a hearing, the district court granted the defendants' motions and denied the plaintiff's motion. JA564. The court found that the "non-attorney access restriction challenged here does not stop Plaintiff from accessing civil court records" because CNS "can freely access the records at the courthouse." JA545. Instead, the regulation "merely controls how and when Plaintiff can access such records." *Ibid.* Therefore, "the restriction resembles a time, place, and manner restriction and relaxed scrutiny applies." *Ibid.*

The court held that the challenged regulation satisfied time, place, and manner scrutiny because it is "'content-neutral, narrowly tailored and necessary' to preserve a significant governmental interest." JA545 (quoting *Schaefer*, 2 F.4th at 328). Virginia's "non-attorney access restriction is content-neutral," because it "applies to all nonconfidential civil court records in the same fashion and does not treat civil court

records about a certain subject or topic differently than others." JA547–48. In addition, Virginia has significant governmental interests, both "in policing sensitive information," and "in ensuring the orderly and efficient administration of justice." JA550.

Next, the court held that the regulation is narrowly tailored because "[t]he undisputed evidence reveals that the regulation materially advances an important interest," and does not "burden substantially more speech than is necessary." JA552–58 (cleaned up). The court concluded that "electronic publication of litigants' personal data is a plausible threat to citizens' privacy and the fair and orderly administration of justice," and there is "evidence to show that the regulation currently prevents the mass collection of PII by bots." JA551–52. Providing "remote access to information, including 'secure remote access,' poses unique privacy concerns in contrast to information available only in person," given the far higher risks of data mining of online databases. JA540. Thus, "allow[ing] the public and press access to all nonconfidential civil court records physically at the courthouse," while "mak[ing] that information unavailable *over the internet*," is "specifically targeted to prevent data mining and keep such information out of the

hands of third parties who could engage in criminal conduct or otherwise misuse that information." JA553–54.

At the same time, attorneys are "officers of the court" and an "essential part of the justice system," and thus "stand on entirely different footing than members of the general public." JA554. To "stop allowing all electronic access to civil court records" would "imped[e] on the efficiency of the judicial system." JA553. OCRA "thus promotes the State's significant interest in a manner 'that would be achieved less effectively absent the regulation.'" JA563 (quoting *Ross v. Early*, 746 F.3d 546, 556 (4th Cir. 2014)).

The court similarly held that the "dissemination restriction" is content neutral and "resembles a time, place, and manner restriction" such that "relaxed scrutiny applie[d]." JA558–60. "Because only" members of the Virginia bar "may electronically access civil court records, this regulation only prevents such attorneys . . . from selling, posting, or redistributing data" obtained from OCRA to third parties. JA558–59. Because the provision "does not prevent Plaintiff from selling, posting, or redistributing data obtained from records located at the courthouse," it resembles a time, place, and manner regulation. JA559. The court held

that the provision satisfied intermediate scrutiny because unfettered dissemination of records obtained from OCRA "could jeopardize citizens' privacy and security." JA562.

Finally, the court rejected CNS's argument that the provisions were not narrowly tailored because Virginia could use a combination of expanded redaction and sealing requirements, modified subscriber agreements, and "bot safeguards" to secure personal information. JA556. The court held that CNS's proposal "would be a dramatic policy change for the State, riddled with labor- and resource-intensive repercussions, and it would be less effective than the State's current regulation." JA557.

CNS then appealed. JA566.

STANDARD OF REVIEW

This Court "review[s] de novo a district court's disposition of cross-motions for summary judgment." *Fusaro v. Howard*, 19 F.4th 357, 366 (4th Cir. 2021). This Court "also review[s] de novo a district court's rulings on the constitutionality of a statute." *Ibid.*

SUMMARY OF THE ARGUMENT

CNS and the public have "reasonably contemporaneous" access to court records at Virginia's courthouses. See *Schaefer*, 2 F.4th at 328. The

First Amendment requires no more. CNS contends that if court records are made remotely accessible to anyone, then the First Amendment requires that they also be made remotely accessible to the general public—but no such right exists.

Even if the challenged provisions implicated First Amendment rights, the district court correctly applied intermediate scrutiny because the provisions resemble lawful time, place, and manner regulations. They do not prohibit access to the court records, but rather govern how and where the public may access them: at the courthouse, rather than over the internet.

The district court also correctly held that the challenged provisions satisfy the time, place, and manner test: they are "content-neutral, [and] narrowly tailored" to serve an "important interest." *Schaefer*, 2 F.4th at 328. The provisions are content-neutral because their application does not turn on the expressive message or subject matter of the court records, and their purpose is unrelated to governmental disagreement with any expressive message. The provisions serve important interests in protecting citizens' personal information, and in promoting the orderly and efficient functioning of Virginia's judiciary.

The provisions are also narrowly tailored. Online public access to court records would lead to data mining of sensitive personal information, which can be used to steal people's identities or commit other frauds. Remote access by vetted court officers promotes the efficient functioning of the judicial system without endangering the public. And regulating the dissemination of data obtained from OCRA likewise protects sensitive personal information by preventing an OCRA subscriber from downloading the entire database and then selling it to data miners.

CNS proposes alternative ways to design a court record system to allow public access while diminishing the threat of data mining. But the system CNS proposes is not OCRA; CNS's concept would require Virginia to design a markedly different, and far more resource-intensive, system. CNS may have a policy preference for such a system, but the First Amendment does not require it.

The district court properly rejected CNS's equal protection claim for similar reasons. Non-attorneys are not a suspect class. And claims challenging access provisions that resemble time, place, and manner regulations are not subject to strict scrutiny. CNS cannot bootstrap a

failed First Amendment claim into a higher tier of scrutiny by re-packaging it as an equal-protection claim. The OCRA regulations are subject to rational basis review, which they easily satisfy.

ARGUMENT

I. There is no First Amendment right to online access of court records that are already available at courthouses, so strict scrutiny does not apply

A. Strict scrutiny does not apply to CNS's First Amendment claims because Virginia Code § 17.1-293 does not restrict a First Amendment right

The challenged provisions do not impede the public's access to court records and therefore do not implicate CNS's First Amendment rights.

"[T]here is no general First Amendment right to access a government record." *Fusaro v. Cogan*, 930 F.3d 241, 249 (4th Cir. 2019). Rather, the general rule is that the First Amendment does not "guarantee the public a right of access to information generated or controlled by government." *Ibid.* (quoting *Houchins v. KQED, Inc.*, 438 U.S. 1, 16 (1978) (Stewart, J., concurring in the judgment)). In other words, "the 'Constitution itself' is not a 'Freedom of Information Act.'" *Id.* at 250 n. 6 (quoting *Houchins*, 438 U.S. at 14 (plurality opinion)).

There is a qualified exception to this rule for certain court proceedings. See *Press-Enterprise Co. v. Superior Court of Cal., Cnty. of*

Riverside, 478 U.S. 1, 8 (1986). Although "[t]he Supreme Court never has found a First Amendment right of access to civil proceedings," *Webster Groves Sch. Dist. v. Pulitzer Pub. Co.*, 898 F.2d 1371, 1377 (8th Cir. 1990), several circuits have held that some qualified right of access also applies in the civil context, see *IDT Corp. v. eBay*, 709 F.3d 1220, 1222 (8th Cir. 2013) (collecting cases). Most recently, this Court held that "the press and public enjoy a First Amendment right of access to newly filed civil complaints." *Schaefer*, 2 F.4th at 328. That access must be "reasonably contemporaneous" with the filing of a complaint. *Ibid.* "The media's rights of access are 'co-extensive with and do not exceed those rights of members of the public in general.'" *Id.* at 326 n.5.[3]

The limited First Amendment right to access court records does not encompass CNS's claims. As CNS acknowledges, it already has contemporaneous access to civil complaints, as well as other civil court records, at courthouses. See CNS Br. 34. The First Amendment requires nothing more. See *Schaefer*, 2 F.4th at 328 (discussing the right of access

[3] This Court has never held that a First Amendment right of access exists for *all* civil court records, as CNS appears to assume. Compare CNS Br. 2 with *Schaefer*, 2 F.4th at 327–28 (limiting First Amendment analysis to "newly filed civil complaints").

exclusively in the context of physical access at a courthouse). Indeed, CNS conceded below that "[n]o court has ever held that remote access is . . . a constitutional right." JA431; see JA437–38 ("[W]e do not contend . . . that the First Amendment requires a per se right to remote access").

CNS now appears to argue that "in person access" does not satisfy the First Amendment because it is "not nearly as expeditious as . . . online access." CNS Br. 34. But to the extent CNS now contends that the First Amendment encompasses a right to online access of civil court records, it waived that argument. See JA359 ("CNS is not seeking a *per se* right of remote access."); *Muth v. United States*, 1 F.3d 246, 250 (4th Cir. 1993) ("As this court has repeatedly held, issues raised for the first time on appeal generally will not be considered."); *Singleton v. Wulff*, 428 U.S. 106, 120 (1976) ("[A] federal appellate court does not consider an issue not passed upon below.").

Further, any argument that state courts must provide online access is not consistent with *Schaefer*'s "flexible standard." *Shaefer*, 2 F.4th at 328. *Shaefer* held that the "qualified" right to "reasonably contemporaneous" access "provides courts with some leeway," and "does not require perfect *or instantaneous* access." *Ibid.* It held that

"reasonably contemporaneous" access typically "means the same day on which the complaint is filed, insofar as is practicable." *Ibid.* (internal quotation marks omitted).

CNS contends that in-person access is not "reasonably contemporaneous," *Shaefer*, 2 F.4th at 328, because the "time and expense of traveling from courthouse to courthouse to access civil case records in a vain effort to report on them in a 'contemporaneous' manner" is "insurmountable," CNS Br. 27. But *Schaefer* recognized only a qualified right to access *at the courthouse*, not access in whatever form is most convenient for CNS. See pp. 24–25, *supra*. CNS also does not explain why its only option is to have a single CNS reporter drive between courthouses, rather than, for instance, asking couriers already present in each circuit to obtain the desired records.[4]

CNS suggests that *Courthouse News Service v. Quinlan*, 32 F.4th 15, 17, 21 (1st Cir. 2022), held that the First Amendment creates a right to online access to court records that are available in-person. That is

[4] In addition, CNS's statistics regarding how long it allegedly took one of its reporters to drive to various courthouses is not part of the record and is not entitled to judicial notice because CNS simply cites its own press release. See ECF No. 31, at 3–4.

incorrect. *Quinlan* held only that the plaintiffs had stated a First Amendment claim where the state court ceased providing any access at the courthouse and routinely delayed online access to newly filed complaints for several days. *Ibid.*; see also *Courthouse News Serv. v. Cozine*, 2022 WL 593603, *2, 6 (D. Or. Feb. 14, 2002) (similar). As CNS conceded below, no court has held that the First Amendment creates a right to online access. JA431.

CNS also contends that Virginia violates the First Amendment by creating a "two-tier access system" that gives "preferential" access to Virginia attorneys. CNS Br. 6–7. In other words, CNS argues that "*if* Defendants provide Virginia attorneys remote access to civil court records, *then* the First Amendment also requires them to provide the public with remote access." JA544. But the First Amendment does not require the government to provide unfettered public access to documents merely because it provides access to anyone.

To the contrary, courts have long recognized that the government may protect citizens' privacy by limiting the dissemination of government records. As the Supreme Court explained in *The Florida Star v. B.J.F.*, 491 U.S. 524 (1989), where "sensitive information is in the government's

custody, it has . . . power to forestall or mitigate the injury caused by its release" and to "guard[] against the dissemination of private facts." *Id.* at 534; see also, *e.g.*, *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469, 496 (1975) ("If there are privacy interests to be protected in judicial proceedings, the States must respond by means which avoid public documentation or other exposure of private information"). The government may "restrict[] access" to government documents to "protect[] the privacy of personal information." *Fusaro*, 19 F.4th at 369–70.

CNS points to *Fusaro v. Cogan*, 930 F.3d 241 (4th Cir. 2019), see CNS Br. 19–20, but it does not support their argument. *Fusaro* held that "courts rightly should hesitate before intruding into areas—like the disclosure of government information—that depend on policy considerations reserved to the political branches." *Fusaro*, 930 F.3d at 253. Accordingly, "not all conditions on access to government information will provoke constitutional concerns." *Id.* at 255. Rather, conditions on access may create a First Amendment issue only where "speaker-based restrictions combined with content-based restrictions" pose a "risk of viewpoint discrimination." *Id.* at 252, 254–55. In other words, the

government cannot use conditions on access to suppress the viewpoint of a "small disfavored class." *Id.* at 254.

Here, CNS does not argue that Virginia restricts online access to court records in order to suppress any disfavored viewpoint. To the contrary, the challenged provisions are wholly content-neutral. See Part II.A, *infra*. CNS thus has no First Amendment right to online access to court records.

B. Strict scrutiny does not apply because the challenged provisions resemble time, place, and manner regulations

Even if CNS's claims implicated First Amendment rights, the claims would not be subject to strict scrutiny because the challenged provisions resemble time, place, and manner regulations. "[L]imitations on the right of access [to court records] that resemble 'time, place, and manner' restrictions on protected speech [will] not be subjected to such strict scrutiny." *Schaefer*, 2 F.4th at 328 (quoting *Globe Newspaper Co. v. Superior Ct. for Norfolk Cnty.*, 457 U.S. 596, 607 n.17 (1982)). Courts may "impose reasonable limitations on access" to court records, in the same way "a government may impose reasonable time, place, and manner restrictions upon the use of its streets in the interest of such objectives as the free flow of traffic." *Richmond Newspapers, Inc. v.*

Virginia, 448 U.S. 555, 581 n.18 (1980). Thus, where access provisions "resemble time, place, and manner restrictions, [this Court] appl[ies] more relaxed scrutiny." *Ibid.*

The challenged provisions here resemble time, place, or manner regulations. Indeed, they literally regulate the time, place, and manner that the public may access court records. CNS wants to access court records over the internet, at any time and from any place of its choosing. See JA37. But because of the significant risks posed by granting public access to aggregated court records online, Virginia Code § 17.1-293 prohibits public online access to court records containing sensitive personal information. See p. 5, 7, *supra*. The statute "does not stop Plaintiff from accessing civil court records altogether—Plaintiff can freely access the records at the courthouse." JA545. Rather, "the access restriction merely controls how and when Plaintiff can access such records"—through terminals in the courthouse, during normal business hours. JA545; see pp. 4–7, 17, *supra*.

Because the challenged provisions resemble time, place, and manner regulations, the district court correctly held that strict scrutiny was inapplicable and "more relaxed scrutiny" applied. JA544–45; see

Schaefer, 2 F.4th at 328. Access provisions that resemble time, place, and manner regulations are constitutional if they are "content-neutral, [and] narrowly tailored" to serve an "important interest." *Schaefer*, 2 F.4th at 328.

CNS seemingly rejects this Court's decision in *Schaefer* and argues instead that this Court should apply—if not strict scrutiny—then a third, "rigorous" scrutiny that is "stricter than the intermediate scrutiny applied to pure [time, place, and manner] rules." CNS Br. 43. CNS contends that the Ninth Circuit's ruling in *Courthouse News Serv. v. Planet*, 947 F.3d 581, 596 (9th Cir. 2020) (*Planet III*) applies this "rigorous" standard, and that *Shaefer* "misread[ ] . . . *Planet III*." CNS Br. 42, 43 n.16.

But CNS's argument as to the correct interpretation of *Planet III* is irrelevant because this Court decided the standard of scrutiny that applies to access regulations in *Schaefer*. To the extent there is any conflict between *Schaefer* and the Ninth Circuit's opinion in *Planet III*, then *Schaefer* controls. See *Booker v. S.C. Dep't of Corr.*, 855 F.3d 533, 538 (4th Cir. 2017) (describing "cases of controlling authority in [this] jurisdiction," as "decisions of the Supreme Court, [and] *this* court of

appeals" (emphasis added) (internal quotation marks omitted)). Again, *Schaefer* held that where the First Amendment qualified right of access to court records applies, and "limitations on the right of access . . . resemble 'time, place, and manner restrictions," then courts "apply more relaxed scrutiny," not strict scrutiny. *Schaefer*, 2 F.4th at 328. This "more relaxed scrutiny" is a "flexible standard," and is met if the regulations are "content-neutral, narrowly tailored" and serve an "important interest." *Ibid.*

Numerous other circuits agree and apply the same time, place, and manner standard. See, *e.g.*, *United States v. Kerley*, 753 F.2d 617, 620–21 (7th Cir. 1985) (holding "[a] limitation on the public access to a trial is not subject to the same 'strict scrutiny' given a denial of access . . . . The limitation can withstand constitutional scrutiny so long as it is reasonable and neutral, as with time, place, and manner restrictions generally"); *United States v. Yonkers Bd. of Educ.*, 747 F.2d 111, 114 (2d. Cir. 1984) (holding a limitation on access to court proceedings that "is simply a 'time, place, and manner' restriction . . . should not be subjected to strict scrutiny, but should be upheld if reasonable"); *United States v. Hastings*, 695 F.2d 1278, 1282 (11th Cir. 1983) (holding a time, place,

and manner regulation that restricts access in the courtroom is constitutional "if it is reasonable, if it promotes significant governmental interests, and if the restriction does not unwarrantedly abridge . . . the opportunities for the communication of thought").

Further, CNS's argument that *Schaefer* misread *Planet III* is incorrect. *Planet III* likewise held that "limitations on the right of access that resemble 'time, place, and manner' restrictions on protected speech, would not be subjected to such strict scrutiny." *Planet III*, 947 F.3d at 595. Instead, the Ninth Circuit held that the right of access is a "qualified right," which "does not entitle the press to immediate access." *Id.* at 585. And, like *Schaefer*, it held that "reasonable restrictions resembling time, place, and manner regulations that result in incidental delays in access are constitutionally permitted where they are content-neutral, narrowly tailored" and serve an "important interest." *Ibid.*[5]

[5] CNS points to the *Planet III* concurrence, CNS Br. 42, which argued that the majority erred by applying a standard overly akin to strict scrutiny. *Planet III*, 947 F.3d at 603–04 (Smith, J., concurring). The majority, however, disagreed with this characterization, holding that its "concurring colleague misapprehends the level of scrutiny we apply here." *Id.* at 596 n.9.

Therefore, even if the challenged provisions implicate the qualified First Amendment access right, the district court properly applies the time, place, and manner test.

C. The dissemination provision is likewise a time, place, and manner regulation, not a prior restraint on speech

CNS's argument that the dissemination regulation violates the First Amendment because it is a prior restraint on speech is similarly erroneous. CNS Br. 46. Virginia Code § 17.1-293(H) is not a prior restraint because it does not enjoin CNS from publishing any lawfully obtained information. Instead, as the district court correctly held, the provision at most resembles a time, place, and manner regulation because it regulates the manner in which the public and press may lawfully obtain court records: at the courthouse, rather than electronically.

The "classic mold of prior restraint" is an "injunction against publication." *Smith v. Daily Mail Pub. Co.*, 443 U.S. 97, 101 (1979). For instance, *Near v. Minnesota*, 283 U.S. 697 (1931), struck down a statute that allowed the State to enjoin publication of any newspaper it deemed "malicious [and] scandalous." *Id.* at 702, 722–23. Such injunctions violate the First Amendment because "unless the owner or publisher is able . . .

to satisfy the judge that the [matter is] true and . . . published with good motives . . . his newspaper or periodical is suppressed . . . . This is of the essence of censorship." *Id.* at 713; see *In re Charlotte Observer*, 921 F.2d 47, 48, 50 (4th Cir. 1990) (invalidating injunction against two reporters "not to disclose the name of an attorney, who had been identified in open court" as target of investigation). A "penal sanction for publishing lawfully obtained, truthful information"—such as a prohibition on publishing the name of a juvenile charged with a crime without prior court approval—is also subject to "exacting scrutiny." *Smith*, 443 U.S. at 101–02; see *Soderberg v. Carrion*, 999 F.3d 962, 966 (4th Cir. 2021) (law prohibiting "the broadcasting of the official court recordings of criminal proceedings" subject to strict scrutiny).

Virginia Code § 17.1-293(H) is not a prior restraint on speech. "Because only" members of the Virginia bar lawfully "may electronically access civil court records, this regulation only prevents such attorneys . . . from selling, posting, or redistributing data" obtained from OCRA to third parties. JA558–59. Virginia courts have not enjoined CNS from publishing any information. Section 17.1-293(H) also does not prohibit CNS from publishing any lawfully obtained court records: the provision

"*does not* prevent Plaintiff from selling, posting, or redistributing data obtained from records located at the courthouse." JA559.

Rather, Section 17.1-293(H) regulates the manner in which the press and public lawfully obtain access to court records. Because CNS cannot lawfully obtain records from OCRA, it also cannot publicly disseminate records obtained from OCRA; it must obtain the records from the courthouse instead. The fact that OCRA is not open to the public does not restrain CNS from reporting on public court documents, because every document available on OCRA is equally available at the courthouse. See p. 7, *supra*. Thus, the district court correctly held that Section 17.1-293(H) "resembles a time, place, and manner restriction" such that "relaxed scrutiny applies." JA559–60.

As this Court recently stated, when "there are privacy interests to be protected in judicial proceedings, the States must respond by means which avoid . . . exposure of private information." *Soderberg*, 999 F.3d at 968 (quoting *Cox Broadcasting*, 420 U.S. at 496). Thus, the government may limit access to citizens' personal information contained in government records, and frequently does. See pp. 27–29, *supra*; p. 41, *infra*. But such regulations would be meaningless if the government could

not also prohibit those with access to the sensitive personal information from publicly disseminating it: as the district court pointed out, "without the dissemination restriction, any entity could sell, post, or redistribute the information and write an algorithm to harvest such private information from the records and use that information to the detriment of Virginia litigants." JA562–63. Such regulations have never been treated as "prior restraints" subject to strict scrutiny. Rather, the Supreme Court has recognized that such privacy protections are policy questions for the "political institutions," which "must weigh the interests in privacy with the interests of the public to know." *Cox Broadcasting*, 420 U.S. at 496.

Here, again, electronic access to court records poses special privacy concerns due to the risk of data mining. See pp. 9–14, *supra*. The Commonwealth therefore limited who may lawfully obtain court records electronically, rather than from the courthouse. The dissemination provision does not constitute a "prior restraint . . . upon the communication of news and commentary on current events," *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976), because it does not prohibit CNS from reporting on the exact same court records available

"in public court documents open to public inspection" at the courthouse, *Cox Broadcasting*, 420 U.S. at 496. To the extent the dissemination provision implicates the First Amendment, it "resembles a time, place, and manner restriction and relaxed scrutiny applies." JA560; see Part I.B, *supra*.

II. The district court correctly held that Virginia's court records access system satisfies time, place, and manner review

The district court correctly held that the challenged provisions here satisfy the "intermediate standard" applied to time, place, and manner regulations because they are content-neutral, "narrowly tailored to serve a significant governmental interest, and leave[] open ample alternative channels for communication of the information." *Ross*, 746 F.3d at 552 (cleaned up) (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989)); JA545–48.

A. The challenged provisions are content-neutral

First, the challenged provisions are "content-neutral." *Schaefer*, 2 F.4th at 328. They apply alike to all nonconfidential court records, with no "distinctions drawn based on the message a speaker conveys." *Reed v. Town of Gilbert, Ariz.*, 576 U.S. 155, 163–64 (2015).

"The principal inquiry in determining content neutrality, in speech cases generally and in time, place, or manner cases in particular, is whether the government has adopted a regulation of speech because of disagreement with the message it conveys." *Ward*, 491 U.S. at 791. The governmental purpose is "the controlling consideration," and a regulation is content-neutral if it "serves purposes unrelated to the content . . . even if it has an incidental effect on some speakers or messages but not others." *Ibid.* Generally, "laws that confer benefits or impose burdens on speech without reference to the ideas or views expressed are in most instances content neutral," unless those laws are "structured in a manner that raised suspicions that their objective was, in fact, the suppression of certain ideas." *Turner Broad. Sys., Inc. v. F.C.C.*, 512 U.S. 622, 643, 660 (1994). "[T]he fact that a law singles out a certain medium, or even the press as a whole, 'is insufficient by itself to raise First Amendment concerns.'" *Id.* at 660 (quoting *Leathers v. Medlock*, 499 U.S. 439, 452 (1991)).

Here, as the district court held, the challenged provisions are content-neutral because "Virginia's restriction applies to all nonconfidential civil court records in the same fashion and does not treat

civil court records about a certain subject or topic differently than others." JA547. "The regulation does not center around disagreement with the message it conveys, turn upon the communicative contents of the court records, nor change based on viewpoint or subject matter." JA548. Rather than any "disagreement with the message" conveyed, *Ward*, 491 U.S. at 791, the governmental purpose is to protect the privacy of personal information contained in court records, such as social security numbers, dates of birth, original signatures, and financial information, which data miners can use to commit identity theft or for other fraudulent and exploitative purposes, see pp. 42–43, *infra*; pp. 9–14, *supra*. At the same time, the challenged provisions "promote effective advocacy" by allowing remote access to "Virginia-barred attorneys" participating directly in Virginia's court system. JA546.

CNS argues that "the Commonwealth's stated justifications for the [remote access] restrictions," including the risk of "disseminat[ion] [of] personally identifying information," demonstrate that the statute is content-based. CNS Br. 40. But protecting sensitive personal information to prevent fraud has nothing to do with suppressing a disfavored message and therefore does not render the provisions content-based. See, *e.g.*,

Dahlstrom v. Sun-Times Media, LLC, 777 F.3d 937, 947 (7th Cir. 2015) (for statutes that "limit public access to sensitive information . . . the constitutionality of those limitations is widely accepted"). Indeed, many statutes restrict access to personal information for the same reasons; that purpose does not render them "content-based" speech restrictions subject to strict scrutiny. See, *e.g.*, 5 U.S.C. § 552a (barring disclosure by federal government of certain "records maintained on individuals"); 42 U.S.C.§ 1320d–6 (setting out criminal penalties for disclosure of individual health information); 42 U.S.C. § 2721 (restricting disclosure of personal information from motor vehicle records).

CNS also does not support its conclusory argument by reference to anything in the record tending to show that the "legislature designed [the statute] to target [particular] speakers and their messages for disfavored treatment" or that it "imposes burdens that are based on the content of speech." *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 565 (2011). As the district court correctly observed, Virginia's access regulation "applies to all civil court records in the same fashion, and merely controls *how* individuals . . . may access these same records electronically." JA548. The content of any particular record is irrelevant to the regulation's

application. Although the protection of sensitive personal information animated the regulation, it applies to all electronic records irrespective of what they contain. The district court correctly held that the challenged provisions here are content-neutral.

B. The challenged provisions are narrowly tailored to serve significant governmental interests

Second, the district court also correctly held that the challenged provisions are "narrowly tailored to serve a significant governmental interest." *Ross*, 746 F.3d at 552.

1. The governmental interests are significant

CNS does not dispute that the governmental interests at stake here are "significant" and "important." *Ross*, 746 F.3d at 552; *Schaefer*, 2 F.4th at 328. The provisions serve two significant governmental interests: protecting sensitive personal information contained in court records and furthering the orderly and efficient administration of justice.

CNS does not dispute that Virginia's interest in protecting sensitive personal information is "substantial." JA550. CNS concedes that "courts share an interest in preventing harm caused by misuse of personal identifiers." CNS Br. 53. Indeed, it is well-established that there is a "substantial governmental interest" in protecting the "privacy interests

of litigants and third parties." *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 34–35 (1984); *National Fed. of the Blind v. Fed. Trade Comm'n*, 420 F.3d 331, 339 (2005) (recognizing that "safeguarding . . . privacy" for the "prevention of fraud" is a "strong" state interest); see also, *e.g.*, *Florida Bar v. Went For It, Inc.*, 515 U.S. 618, 625 (1995) ("Our precedents also leave no room for doubt that 'the protection of potential clients' privacy is a substantial state interest.'" (quoting *Edenfield v. Fane*, 507 U.S. 761, 769 (1993)); *Lanphere & Urbaniak v. State of Colo.*, 21 F.3d 1508, 1515 (10th Cir. 1994) (recognizing "[t]he State's interest in protecting privacy" in court records).

The governmental interest in "the orderly and efficient administration" of the Commonwealth's court system is also a significant one. JA560. This Court has recognized that states have an "important interest" in their "court[s'] . . . fair and orderly administration of justice." *Schaefer*, 2 F.4th at 328 (quoting *Planet III*, 947 F.3d at 585); see also *Planet III*, 947 F.3d at 596 (recognizing substantial governmental interest in "the orderly filing and processing of cases"). Again, CNS does not dispute that this governmental interest is significant.

2. The provisions are narrowly tailored

The access regulations are narrowly tailored to serve these important governmental interests. "A regulation is narrowly tailored under [the time, place, and manner] standard if it 'promotes a substantial government interest that would be achieved less effectively absent the regulation' and does not 'burden substantially more speech than is necessary to further the government's legitimate interests.'" *Ross*, 746 F.3d at 552–53 (quoting *Ward*, 491 U.S. at 799).

This narrow-tailoring requirement differs significantly from the narrow-tailoring prong of the strict scrutiny test. For a "time, place, or manner regulation[] . . . the same degree of tailoring is not required" as under the strict scrutiny test. *Ward*, 491 U.S. at 798 n.6. Most significantly, "a regulation of the time, place, or manner of protected speech . . . need not be the least restrictive or least intrusive means" of serving the governmental interest. *Id.* at 798; see also *Ross*, 746 F.3d at 553 ("[T]he regulation need not be the least restrictive or least intrusive means of serving the government's significant interests." (internal quotation marks omitted)). Thus, under the time, place, and manner standard, "[s]o long as the means chosen are not substantially broader

than necessary to achieve the government's interest, . . . the regulation will not be invalid simply because a court concludes that the government's interest could be adequately served by some less-speech-restrictive alternative." *Ward*, 491 U.S. at 799.

There is a close connection between the Commonwealth's interest in protecting sensitive personal information and the provision prohibiting public access to court records containing such information "on the internet." Va. Code § 17.1-293(B). The provision "is specifically targeted to prevent data mining and keep such information out of the hands of third parties who could . . . misuse that information," without "restrict[ing] access to that information entirely." JA553–54. Data mining typically requires easy access to large volumes of data, which "bots" programmed to seek personal information can quickly search. See p. 9, *supra*. In-person access at the courthouse largely eliminates the data-mining concern, but still permits any person to access any nonconfidential civil record. It therefore represents a reasonable balance of the right to access court records with the governmental interest in protecting the privacy of litigants and witnesses. See pp. 42–43, *supra*.

Thus, as the district court held, the provision is narrowly tailored "because it allows the public and press access to all nonconfidential civil court records physically at the courthouse." JA553. It "simply makes that information unavailable to the public over the internet, where it would be much easier to access significant amounts of data from anywhere in the world with an internet connection and quickly republish it or download it for illegitimate or improper purposes." JA554. Restricting access to public records in this manner is a well-recognized method of protecting privacy, sometimes known as "practical obscurity." *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 762–64 (1989) ("Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files . . . and a computerized summary located in a single clearinghouse of information"); see Ardia, *supra*, at 1399.

The access provision is also narrowly tailored to advance the Commonwealth's interest in the orderly and efficient administration of justice. Protecting the privacy of sensitive personal information in court records "ensur[es] that potential litigants have unimpeded access to the courts." *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 36 n.22 (1984)

(quoting *Rhinehart v. Seattle Times Co.*, 98 Wash. 2d 226, 254 (1982)). In the absence of effective privacy protections, "individuals may well forgo the pursuit of their just claims," thus making "the utilization of [the judicial system's] remedies so onerous that the people will be reluctant or unwilling to use it, resulting in frustration of a right as valuable as that of speech itself." *Ibid.*

Providing remote access to certain government agencies and Virginia attorneys also advances the administration of justice. As "officers of the court," attorneys "stand on entirely different footing than members of the general public" with regard to court records. JA554. "Attorneys are an essential part of the justice system and their access to this information is necessary for them to perform their professional obligations." *Ibid.* Requiring attorneys to travel to the courthouse to access court filings would make it significantly more difficult for them to serve their clients effectively and cost-efficiently, thereby hampering the administration of justice and making it more difficult for potential litigants to access justice at all. At the same time, OCRA protects privacy by limiting online access to "a self-policing, pre-vetted group subject to codified Rules of Professional Conduct and serious professional sanctions

for violating those Rules." JA556. If attorneys abuse personal information in court records, Virginia's courts can "revoke their license and put them out of business," a method of enforcement that simply does not apply to members of the general public. JA438; see also Va. Sup. Ct. R. Pro. Conduct 1.6; Va. Sup. Ct. R. Pt. 6, § 4, ¶ 13.

CNS contends that the provision is not narrowly tailored because it does not limit attorneys' remote access to cases in which they are the counsel of record. CNS Br. 8. But there are many instances in which attorneys need access to court filings in other cases. For instance, attorneys may be advising clients in cases in which they are not counsel of record, preparing for an anticipated appeal, or participating in separate but closely related proceedings. Court orders in other cases may also be highly relevant to attorneys' arguments. See, *e.g.*, *Funny Guy, LLC v. Lecego, LLC*, 293 Va. 135, 141 (2017) (discussing res judicata principles).

The challenged dissemination provision is likewise narrowly tailored. Again, as the district court noted, Code § 17.1-293(H) does not bar CNS, or any member of the public, from "selling, posting, or redistributing data obtained in . . . the courthouse to third parties"—it

merely bars them from downloading and reposting data *obtained over OCRA*. JA558–59. Without the dissemination provision, a single subscriber with OCRA access could easily circumvent the system's privacy safeguards by downloading the entirety of a circuit court's OCRA database and publishing it online. See Va. Code § 17.1-293(H); see JA552; see generally JA414–428. Indeed, because OCRA does not charge subscribers additional fees for document access, a subscriber could download the entire database at no additional charge. JA85–86; see p. 6, *supra*.

OCRA's privacy safeguards would be wholly ineffective without the provision limiting dissemination. As the district court held, "common sense and logic" demonstrate that allowing any OCRA subscriber to freely sell or republish all OCRA records "could jeopardize citizens' privacy and security." JA562. Providing "public access to records at a physical courthouse" rather than online "serves as a bulwark against widespread dissemination of this private information," particularly "where, as here, the burden on speech is relatively small." *Ibid.*

C. The challenged provisions leave open ample alternative channels to access court records

Third, Virginia's system "leave[s] open ample alternative channels" to access court records because the very same records are already available contemporaneously at the courthouse. *Ross*, 746 F.3d at 552 (quoting *Ward*, 491 U.S. at 791).

CNS, and the rest of the public, may obtain substantially all non-confidential court documents at the courthouse "on the day of filing." See *Schaefer*, 2 F.4th at 329; see pp. 4, 6–7, *supra*. CNS has made "no showing that the remaining avenues of communication are inadequate," *Ward*, 491 U.S. at 802, only that they are less convenient and profitable for it.

CNS suggests that the availability of alternative channels is not relevant. CNS Br. 65. But the cases on which CNS relies did not consider this prong only because those cases involved total bars on timely access to court records, and alternative channels therefore did not exist. See *Schaefer*, 2 F.4th at 322 (challenge to delay in *any* access to newly filed complaints); *Planet III*, 947 F.3d at 596 n.9 (holding prong was "inapplicable" because the regulation barred the "*one way* CNS c[ould] access the new complaints") (emphasis added). Courts that provide alternative means to access records "have generally been allowed to

decide for themselves how to manage access," and the availability of alternatives weighs strongly in favor of constitutionality. Ardia, *supra*, at 1442; see *Nixon v. Warner Comm'cns, Inc.*, 435 U.S. 589 (1978) (press had no First Amendment right to physical access to Watergate tapes when it was provided with transcripts of tapes).

Here, the Commonwealth's provision of unlimited access to records at the courthouse satisfies CNS's qualified "First Amendment right of access." *Schaefer*, 2 F.4th at 328. Obtaining records essentially contemporaneously with filing at the courthouse is an "ample alternative." *Ross*, 746 F.3d at 552 (quoting *Ward*, 491 U.S. at 791).

D. CNS's arguments regarding the time, place, and manner test lack merit

1. The Commonwealth presented sufficient evidence of the harms of data mining

CNS's arguments that the challenged provisions do not satisfy the time, place, and manner test lack merit. CNS primarily contends that the Commonwealth did not meet its "evidentiary burden" to show there is a genuine threat that data miners would target OCRA if it were opened to the public. CNS Br. 51. That argument is incorrect.

The Commonwealth need not "present a panoply of empirical evidence" in support of its substantial interest; rather, it need only "make some evidentiary showing that the recited harms are real, not merely conjectural." *Ross*, 746 F.3d at 556 (internal quotation marks omitted). Further, the Commonwealth need not wait for the harms to occur before it may take action: "It . . . is not unreasonable, or violative of the Constitution, for a State to respond with what in effect is a prophylactic rule." *Ohralik v. Ohio State Bar Ass'n*, 436 U.S. 447, 467 (1978). And the Commonwealth may rely on "common sense" and "anecdote" as well as empirical data. *Fla. Bar*, 515 U.S. at 628. As the district court correctly found, the Commonwealth adequately demonstrated that "the electronic publication of litigants' personal data is a plausible threat to citizens' privacy and the fair and orderly administration of justice." JA548–53.

The Commonwealth presented evidence that Virginia's public online databases have been "subjected to manual and/or automated data mining," typically by "internet bots" that "consum[ed] an inordinate amount of processing power." JA129. Virginia tried several methods to deter data mining of these databases, but the bots circumvented the limits. See pp. 9–10, *supra*. Further, Virginia presented evidence that

data miners can "piece together the PII underlying" the database, even if that personal information is not publicly displayed. JA130.

CNS argues that this evidence is insufficient because it did not detail the exact quantity or nature of the data mining that occurred in these other Virginia databases. CNS Br. 55. But the evidence demonstrates that data mining of public online databases of government records is a "real, not merely conjectural," threat. *Ross*, 746 F.3d at 556 (quoting *Satellite Broad. & Commc'ns Ass'n v. FCC*, 275 F.3d 337, 356 (4th Cir. 2001)). Indeed, CNS's own declarant agreed that "bots are not unusual and it is estimated that bot traffic currently represents more than half of all internet activity." JA411. He also agreed that some bots engage in "abusive data mining." *Ibid.* If OCRA is made accessible to the public, it will face data mining attempts. See JA129.

CNS also contends that the threat of data mining is overly speculative because "there is no evidence those harms have arisen with respect to remote access in other courts." *Ibid.*[6] That contention is

[6] CNS's repeated contention that 38 States have public remote access to court records is highly misleading. See, *e.g.*, CNS Br. 58. That

inaccurate. In fact, the evidence shows that court records are a "major avenue[]" for data mining. JA330–32. For instance, a Vermont report specifically identified court records as a "common[]" source of data for those trafficking in aggregated personal information. Vermont Attorney General Report, *supra*, at 4. Court records, including names and personal information of crime victims and police officers, as well as individual health information, have been mined and sold by data miners. JA331–32; see Ardia, *supra*, at 1399 ("[T]he heaviest users of electronic court records have been commercial entities, particularly data brokers and other information resellers, who benefit tremendously from the economies of scale electronic-record systems offer"). The federal PACER system has also suffered from data mining, including for the identities of government informants. See p. 11, *supra*; House Judiciary Hearing, *supra*, at 27; Data Broker Report, *supra*, at 1, 15.

---

figure includes a State if *any* court in the State offers remote access, even if the vast majority do not. JA79. For instance, the 38 States include Virginia itself, because the Alexandria Circuit Court offers remote access. JA80, 159. In addition, as the district court found, the bare number of states with some remote access is "irrelevant" because CNS presented no evidence of how those systems functioned, and no "explanation of the effectiveness of protective measures" in safeguarding personal information and the orderly administration of justice. JA557.

CNS contends that this evidence of data mining of online court records should be "set aside" because "secondary sources [are] . . . inadmissible and irrelevant." CNS Br. 54, 56. That contention misunderstands both the Federal Rules of Evidence and the rules governing summary judgment. Sources that would be inadmissible at trial can properly be considered on a motion for summary judgment, so long as the information could be put forward in admissible form at trial. See *Humphreys & Partners Architects, L.P. v. Lessard Design, Inc.*, 790 F.3d 532, 538 (4th Cir. 2015). In any event, many of the secondary sources the Commonwealth cites are government reports that are admissible because they are excluded from the hearsay bar. See Fed. R. Evid. 803(8)(A)(iii). Government reports are also judicially noticeable. *United States v. Cecil*, 836 F.2d 1431, 1452 (4th Cir. 1988) ("[C]ourts may take judicial notice of official governmental reports and statistics."); Fed. R. Evid. 902(5).[7]

[7] The district court did not hold that any of the secondary sources the Commonwealth cited below were improper. Rather, it merely noted CNS's objection to the sources and stated that it "did not rely upon" them. JA549 n.13.

CNS also argues that the risk of data mining is overly speculative because there is insufficient evidence that "personal identifiers are common in public documents." CNS Br. 56. But the source CNS cites found that the vast majority of court records contain at least one piece of sensitive personal information: of the 504 nonconfidential briefs sampled, only 37 had no such personal information. David S. Ardia & Anne Klinefelter, *Privacy and Court Records: An Empirical Study*, 30 Berkeley Tech. L.J. 1807, 1860, Table 4. Even if personal information makes up a small fraction of most individual court records, data miners program bots to sift through millions of documents to piece together personal information. See p. 9–10, *supra*; Data Broker Report, *supra*, at 11.

Finally, CNS contends that data mining can be used for innocuous purposes, "including for news reporting" and to "keep their ongoing projects up to date." CNS Br 57. But the contention that *some* data mining is used for legitimate purposes does not make the harm overly speculative. Data mining of sensitive personal information is frequently used in crimes such as identity theft and other financial frauds. See p. 12–14, *supra*. It is also used to target vulnerable populations, such as elderly people with dementia, or low-income immigrants facing financial

crises, for exploitation. See pp. 13–14, *supra*. And as the district court noted, CNS's own marketing materials for its "case search engine" show that, "[i]f CNS, or any other third party, were given access to [online] records, there would be nothing stopping such entities from downloading all content . . . and then posting such information on their own website for profit, exploitation, or to sell." JA552; see generally JA414–428.

The Commonwealth presented evidence that online databases of government records, including in Virginia, are targeted for data mining; that OCRA records contain sensitive personal information; that CNS is—directly or indirectly—a broker of such personal information; and that data mining of sensitive personal information harms citizens. The record is more than sufficient to "make some evidentiary showing that the recited harms are 'real, not merely conjectural.'" *Ross*, 746 F.3d at 556 (quoting *Satellite Broad. & Commc'ns Ass'n*, 275 F.3d at 356).

2. CNS's proposed alternatives do not demonstrate that the provisions are inadequately tailored

CNS also argues that the challenged provisions do not satisfy the time, place, and manner test because there are "readily available, less-speech-restrictive alternatives," including expanding redaction and sealing requirements, and employing "commonly-used bot management,

mitigation and protection practices." CNS Br. 60. But again, a "least-restrictive-alternative analysis is wholly out of place" in the time, place, and manner test. *Ward*, 491 U.S. at 798 n.6. Instead, the test asks only whether the government's interests would be achieved less effectively without the provisions, and whether the provisions "burden substantially more speech than is necessary to further the government's legitimate interests." *Ross*, 746 F.3d at 552–53. The challenged provisions here satisfy that standard.

CNS does not show that its proposal to require greater redaction, and to prohibit public access to certain "case types where identifiers commonly appear," is actually less speech-restrictive. CNS Br. 58–59. Virginia law currently gives court clerks the choice between requiring the redaction of only the most sensitive personal information while making records publicly accessible at the courthouse, see Va. Code § 8.01-420.8, or requiring greater redaction if they wish to make the records publicly available online, given the greater dangers of data mining, Va. Code § 17.1-293(B). That CNS prefers the latter option does not demonstrate that it restricts less speech. Because physical access mitigates the risk of automated collection and exposure of "private information," court clerks

can safely allow *more* public access at courthouses than they could with an online system. JA562.

CNS's proposals further demonstrate that Virginia could not allow public access to OCRA without endangering the privacy of its citizens. OCRA was not designed for public access and has never been open to the general public. See pp. 7, 14–15, *supra*. The access and dissemination regulations *are* the privacy safeguards the Commonwealth has reasonably chosen. See JA128. A public online database would require numerous new resource-intensive protective measures, such as, in CNS's own account, new and expanded redaction requirements, new categories of confidential case types, new subscriber agreements and fee arrangements, and new methods to detect and deter bots. See CNS Br. 60.

In other words, CNS proposes a wholesale overhaul of Virginia's court-record system that would require "the State . . . to pass a host of legislative measures to protect the widespread distribution of PII," with the result that "the State and clerks would be forced to expend substantial resources to police OCRA user activity to limit exploitation of personal information." JA555. In effect, CNS would force Virginia to

abandon OCRA, and either entirely cease providing any online access to court records or design a very different system. The district court correctly held that such a "significant policy change is not one that this Court should mandate upon the State." *Ibid.* The First Amendment does not require States to choose between providing online access to court records for the entire public or providing no online access to anyone.

Such stringent limits on courts are particularly improper given that a public online system would require far greater resources to create and maintain than the current public access at courthouse terminals. The current system costs local court clerks $1.2 million annually. JA134. "[I]t would cost substantial additional funds to modify" the system for public online access: one court clerk estimated that his redaction costs alone would quadruple. JA138. The bot-management and other security tactics CNS proposes are also resource-intensive. See JA138. These costs, financial and otherwise, would hinder the Commonwealth's "important interest" in the "fair and orderly administration of justice." *Schaefer*, 2 F.4th at 328.

CNS argues that costs are irrelevant, contending that "concern about maintaining a government monopoly over the dissemination of

public records to protect the sizeable revenue streams" has "no place" in the First Amendment analysis. CNS Br. 58. This argument misconstrues both the issues at stake and the First Amendment. Virginia courts are not competitors in a marketplace for judicial records seeking to extract "monopoly" rents. They are public institutions charged with allocating limited taxpayer resources to operate the Commonwealth's judicial system. "The First Amendment does not require courts, public entities with limited resources, to set aside their judicial operational needs to satisfy the immediate demands of the press." *Planet III*, 947 F.3d at 596. This Court should decline to "second guess the careful deliberations the state court undertook in deciding how to manage scarce resources." *Id.* at 600.

Further, CNS's proposed alternative would be "less effective[]" in furthering "the government's legitimate interests." *Ross*, 746 F.3d at 552–53. Even with CNS's costly proposed mitigation measures, a public online access system would not protect the privacy of sensitive personal information as effectively as the current courthouse access system. Filers do not always follow redaction requirements, and data miners can pierce

some attempted redactions and extract the underlying personal data.[8] Data miners also can and do circumvent bot management tactics. JA130–31.

At the same time, prohibiting Virginia courts from granting attorneys greater online access to court records than the general public would make it more difficult, and more expensive, for attorneys to serve their clients—and thereby more difficult for clients to access justice. Attorneys would face more onerous redaction and sealing requirements, as well as reduced access to court records. Indeed, if clerks concluded that they could not afford to run a public online access system, CNS would have succeeded only in eliminating lawyer access to electronic court records. See pp. 5, 59–60, *supra*. In short, the district court correctly held that CNS's proposed alternative "would be a dramatic policy change for the State, riddled with labor- and resource-intensive repercussions, and it would be less effective than the State's current regulation." JA557.

[8] See Letter from Carl Malamud to The Honorable Lee H. Rosenthal, Chair, Committee on Rules of Practice and Procedure, Judicial Conference of the United States (Oct. 24, 2008), https://tinyurl.com/58azbt76; Timothy B. Lee, *Studying the Frequency of Redaction Failures in PACER*, Freedom to Tinker (May 25, 2011), https://tinyurl.com/5em9t4x2.

Federal courts are "not positioned to mandate this change in policy upon the State, nor is that the legal standard." *Ibid.*

III. The district court correctly dismissed CNS's Equal Protection Clause claim because the challenged provisions have a rational basis

The district court also correctly dismissed CNS's equal protection claim. The challenged provisions are subject to rational basis review, which they easily satisfy.

The Equal Protection Clause requires the application of strict scrutiny only if a state regulation classifies on the basis of "suspect distinctions" such as race or national origin, or if it "burdens the exercise of a fundamental constitutional right." *Willis v. Town of Marshall, N.C.*, 426 F.3d 251, 262 (4th Cir. 2005) (quoting *Star Scientific, Inc. v. Beales*, 278 F.3d 339, 351 (4th Cir. 2002)). CNS does not contend that the provisions draw suspect classifications; as the district court correctly held, "non-attorneys are not a suspect class." JA73.

Rather, CNS argues that strict scrutiny applies because the access regulations implicate "fundamental" First Amendment rights. CNS Br. 32–33. CNS asserts obliquely that the "fundamental First Amendment right is not satisfied by limiting the press and public to 'physical access.'"

CNS Br. 33 (quoting JA124). But, as the district court held, CNS did "not argue that there is any fundamental right to access civil court records *remotely*." JA73. That Virginia has not established an access system that maximizes CNS's profits does not implicate a fundamental First Amendment right. See Part I.A, *supra*.

In any event, CNS cannot bootstrap its First Amendment claims into a higher tier of scrutiny by repackaging them under the Equal Protection Clause. CNS's First Amendment claims are subject to the time, place, and manner test, *not* strict scrutiny. See Part I.B, *supra*. Strict scrutiny is therefore likewise inapplicable to an equal-protection claim based on the same alleged First Amendment rights. "If every time, place, and manner regulation were subject to strict scrutiny under the Equal Protection Clause simply because it burdened constitutionally protected speech, *Ward*'s intermediate-scrutiny test would be rendered obsolete." *Brown v. City of Pittsburgh*, 586 F.3d 263, 283 n.22 (3d Cir. 2009). Thus, when an "ordinance is a content-neutral time, place and manner restriction, [it] therefore is not an unconstitutional infringement of the right to free speech" under the Equal Protection Clause. *Williams v. City of Columbia*, 906 F.2d 994, 999 (4th Cir. 1990). Rather, it "passes

muster under the Equal Protection Clause for the same reasons that it passes muster under the First Amendment." *Brown*, 586 F.3d at 283 (quoting *McGuire v. Reilly*, 260 F.3d 36, 49–50 (1st Cir. 2001)).

Where, as here, an equal-protection claim grounded on the First Amendment "do[es] not merit a more intense form of scrutiny, rational basis review is appropriate." *Farm Lab. Org. Comm. v. Stein*, 56 F.4th 339, 354 (4th Cir. 2022). Under rational basis review, the statute "is accorded a strong presumption of validity." *Heller v. Doe*, 509 U.S. 312, 319 (1993). The burden to demonstrate that a law is irrational rests with "the one attacking the legislative arrangement," who must "negative every conceivable basis which might support it." *Armour v. City of Indianapolis, Ind.*, 566 U.S. 673, 685 (2012) (quoting *Madden v. Kentucky*, 309 U.S. 83, 88 (1940)). A legislative distinction "will be sustained 'if there is a rational relationship between the disparity of treatment and some legitimate governmental purpose.'" *King v. Rubenstein*, 825 F.3d 206, 221 (4th Cir. 2016) (quoting *Heller* at 319–20). "It is enough [for rational basis review] that there is an evil at hand for correction, and that it might be thought that the particular legislative

measure was a rational way to correct it." *Williamson v. Lee Optical of Oklahoma Inc.*, 348 U.S. 483, 488 (1955).

Because Virginia Code § 17.1-293 satisfies intermediate scrutiny under the time, place, and manner test, it also necessarily satisfies the more deferential rational basis review. *Williams*, 906 F.2d at 999. The Commonwealth has identified the high risk that its citizens' personal information would be compromised, and the efficiency of its courts impeded, if online access to court records were available to the public at large. It rationally serves those important interests to make court records publicly available at the courthouse instead, where it is more difficult for those with nefarious aims to collect data en masse. Virginia's approach is rational. Although CNS would like Virginia to adopt a system more suited to CNS's business model, that is a policy question for "the Virginia General Assembly, not the federal judiciary." JA558.

CONCLUSION

This Court should affirm the judgment of the district court.

Respectfully submitted,

COMMONWEALTH OF VIRGINIA

By: */s/ Erika L. Maley*
ERIKA L. MALEY
Principal Deputy Solicitor General

JASON S. MIYARES
Attorney General
STEVEN G. POPPS
Deputy Attorney General
ROBERT B. MCENTEE, III
Assistant Attorney General
ERIN R. MCNEILL
Assistant Attorney General

ANDREW N. FERGUSON
Solicitor General
GRAHAM K. BRYANT
Deputy Solicitor General
M. JORDAN MINOT
Assistant Solicitor General

Office of the Attorney General
202 North Ninth Street
Richmond, Virginia 23219
(804) 786-2071 – Telephone
(804) 786-1991 – Facsimile

Counsel for Defendant-Appellee the Commonwealth of Virginia

April 20, 2022

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because it contains 12,897 words, excluding the parts of the brief exempted by Rule 32(f). This brief complies with the typeface requirements of Rule 32(a)(5) and the type style requirements of Rule 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Century typeface.

/s/ Erika L. Maley

Erika L. Maley

CERTIFICATE OF SERVICE

I certify that on April 20, 2023, I electronically filed the foregoing brief with the Clerk of this Court by using the appellate CM/ECF system. The participants in the case are registered CM/ECF users and service will be accomplished by the appellate CM/ECF system.

/s/ Erika L. Maley

Erika L. Maley