United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued November 2, 2018 Decided June 21, 2019

No. 17-5217

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION,

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO, ET AL.,
APPELLEES

NATIONAL TREASURY EMPLOYEES UNION, ET AL.,
APPELLANTS

v.

OFFICE OF PERSONNEL MANAGEMENT, ET AL.,
APPELLEES

Consolidated with 17-5232

Appeals from the United States District Court
for the District of Columbia
(No. 1:15-mc-01394)

Peter A. Patterson argued the cause for Arnold Plaintiffs-Appellants in No. 17-5232. With him on the briefs were *David H. Thompson*, *Daniel C. Girard*, *Jordan Elias*, *Tina Wolfson*, *Gary E. Mason*, and *Richard B. Rosenthal.*

Paras N. Shah argued the cause for appellants National Treasury Employees Union, et al. in No. 17-5217. With him on the briefs were *Gregory O'Duden*, *Larry J. Adkins*, and *Allison C. Giles*.

Marc Rotenberg and *Alan Butler* were on the brief for *amici curiae* Electronic Privacy Information Center (EPIC) and Forty-Four Legal Scholars and Technical Experts in support of appellants.

Sonia M. Carson, Attorney, U.S. Department of Justice, argued the cause for federal appellees. With her on the brief was *Mark B. Stern*.

Jason J. Mendro argued the cause for appellee KeyPoint Government Solutions, Inc. With him on the brief were *F. Joseph Warin*, *Matthew S. Rozen,* and *Jeremy M. Christiansen*.

Alan Charles Raul, *Kwaku A. Akowuah*, *Daniel J. Hay*, and *Steven P. Lehotsky* were on the brief for *amicus curiae* The Chamber of Commerce of the United States of America in support of appellees.

Before: TATEL and MILLETT, *Circuit Judges*, and WILLIAMS, *Senior Circuit Judge*.

Opinion for the Court filed PER CURIAM.

Opinion concurring in part and dissenting in part filed by *Senior Circuit Judge* WILLIAMS.

PER CURIAM: In 2014, cyberattackers breached multiple U.S. Office of Personnel Management ("OPM") databases and allegedly stole the sensitive personal information—including

birth dates, Social Security numbers, addresses, and even fingerprint records—of a staggering number of past, present, and prospective government workers. All told, the data breaches affected more than twenty-one million people. Unsurprisingly, given the scale of the attacks and the sensitive nature of the information stolen, news of the breaches generated not only widespread alarm, but also several lawsuits. These suits were ultimately consolidated into two complaints: one filed by the National Treasury Employees Union and three of its members, and another filed by the American Federation of Government Employees on behalf of several individual plaintiffs and a putative class of others similarly affected by the breaches. Both sets of plaintiffs alleged that OPM's cybersecurity practices were woefully inadequate, enabling the hackers to gain access to the agency's treasure trove of employee information, which in turn exposed plaintiffs to a heightened risk of identity theft and a host of other injuries. The district court dismissed both complaints for lack of Article III standing and failure to state a claim. For the reasons set forth below, we reverse in part and affirm in part.

I

As its name suggests, the U.S. Office of Personnel Management serves as the federal government's chief human resources agency. In that capacity, OPM maintains electronic personnel files that contain, among other information, copies of federal employees' birth certificates, military service records, and job applications identifying Social Security numbers and birth dates.

The agency also oversees more than two million background checks and security clearance investigations per year. To facilitate these investigations, OPM collects a tremendous amount of sensitive personal information from current and prospective federal workers, most of which it then

stores electronically in a "Central Verification System." Consolidated Amended Complaint, *In re United States Office of Pers. Mgmt. Data Security Breach Litig.*, No. 1:15-mc-01394, ¶ 65 (D.D.C. March 14, 2016) ("Arnold Plaintiffs' Compl."), J.A. 61. The investigation-related information stored by OPM includes birth dates, Social Security numbers, residency details, passport information, fingerprints, and other records pertaining to employees' criminal histories, psychological and emotional health, and finances. In recent years, OPM has relied on a private investigation and security firm, KeyPoint Government Solutions, Inc. ("KeyPoint"), to conduct the lion's share of the agency's background and security clearance investigation fieldwork. KeyPoint investigators have access to the information stored in OPM's Central Verification System and can transmit data to and from the agency's network through an electronic portal.

It turns out that authorized KeyPoint investigators have not been the only third parties to access OPM's data systems. Cyberattackers hacked into the agency's network on several occasions between November 2013 and November 2014. Undetected for months, at least two of these breaches resulted in the theft of vast quantities of personal information. According to the complaint, after breaching OPM's network "using stolen KeyPoint credentials" around May 2014, Arnold Plaintiffs' Compl. ¶ 127, J.A. 73, the cyberintruders extracted almost 21.5 million background investigation records from the agency's Central Verification System. They gained access to another OPM system near the end of 2014, stealing over four million federal employees' personnel files. Among the types of information compromised were current and prospective employees' Social Security numbers, birth dates, and residency details, along with approximately 5.6 million sets of fingerprints. The breaches also exposed the Social Security numbers and birth dates of the spouses and cohabitants of those

who, in order to obtain a security clearance, completed a Standard Form 86. According to the complaints, since these 2014 breaches, individuals whose information was stolen have experienced incidents of financial fraud and identity theft; many others whose information has not been misused—at least, not yet—remain concerned about the ongoing risk that they, too, will become victims of financial fraud and identity theft in the future.

After announcing the breaches in the summer of 2015, OPM initially offered individuals whose information had been compromised fraud monitoring and identity theft protection services and insurance at no cost for either eighteen months or three years, depending on whether their Social Security numbers had been exposed. But OPM's offer failed to address the concerns of all such parties, and the agency soon found itself named as a defendant in breach-related lawsuits across the country. The Judicial Panel on Multidistrict Litigation transferred these actions to the U.S. District Court for the District of Columbia for coordinated pretrial proceedings. The suits were ultimately consolidated into two complaints: one brought by the American Federation of Government Employees on behalf of thirty-eight individuals affected by the breaches and a putative class of similarly situated breach victims ("Arnold Plaintiffs") and another for declaratory and injunctive relief brought by the National Treasury Employees Union ("NTEU") and three of its members ("NTEU Plaintiffs"). Below we summarize the relevant allegations and claims contained in each complaint, accepting all factual allegations "as true" and drawing "reasonable inferences * * * in the plaintiffs' favor." *Philipp v. Federal Republic of Germany*, 894 F.3d 406, 409 (D.C. Cir. 2018) (internal quotation marks omitted).

Arnold Plaintiffs allege that KeyPoint's "information security defenses did not conform to recognized industry standards" and that the company unreasonably failed to protect the security credentials that the hackers used to unlawfully access one of OPM's systems in mid-2014. Arnold Plaintiffs' Compl. ¶ 222, J.A. 98. Specifically, they assert that "KeyPoint knew or should have known that its information security defenses did not reasonably or effectively protect Plaintiffs' and Class members' [personal information] and the credentials used to access it on KeyPoint's and OPM's systems." *Id.* As for OPM, Arnold Plaintiffs allege that the agency had long been on notice that its systems were prime targets for cyberattackers. OPM experienced data breaches related to cyberattacks in 2009 and 2012, and it is no secret that its network is regularly subject to a strikingly large number of hacking attempts. Despite this, say Arnold Plaintiffs, OPM repeatedly failed to comply with the Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541 *et seq.* (repealed 2014), and its replacement, the Federal Information Security Modernization Act of 2014, 44 U.S.C. §§ 3551 *et seq.* (collectively, "Information Security Act"), which require agencies to "develop, implement, and maintain a security program that assesses information security risks and provides adequate security for the operations and assets of programs and software systems under agency and contractor control." Arnold Plaintiffs' Compl. ¶ 83, J.A. 65.

As early as 2007, Information Security Act compliance audits conducted by OPM's Office of the Inspector General regularly identified major information security deficiencies that left the agency's network vulnerable to attack. Such problems included "severely outdated" security policies and procedures, understaffed and undertrained cybersecurity personnel, and a lack of a centralized information security management structure. Arnold Plaintiffs' Compl. ¶¶ 92–95,

J.A. 67–68. As a result, in every year from 2007 through 2013, the Inspector General identified "serious concerns that * * * pose an immediate risk to the security of assets or operations"—termed "material weaknesses"—in the agency's information security governance program. *Id.* ¶¶ 87–88, J.A. 66; *see also id.* ¶¶ 90–97, J.A. 66–68 (listing those weaknesses). Although in 2014 the Inspector General, acting on the basis of "imminently planned improvements," *id.* ¶ 98, J.A. 68, reclassified OPM's security governance program as a "significant deficiency" (an improvement over the more serious "material weakness"), other serious issues resurfaced at that time. Specifically, in 2014, the agency failed to complete an Information Security Act-required Security Assessment and Authorization for eleven of the twenty-one OPM systems due for reauthorization. Because the agency was unable to ensure the functionality of security controls for the systems that lacked a valid authorization—one of which was "a general system that supported and provided the electronic platform for approximately two-thirds of all information systems operated by OPM"—the Inspector General advised the agency to shut them down. *Id.* ¶¶ 102–103, J.A. 69–70. Despite the Inspector General's recommendation, OPM continued to operate the systems. The agency compounded existing security vulnerabilities by failing to encrypt sensitive data—including Social Security numbers—and failing to enforce multifactor authentication requirements. To make matters worse, when the 2014 data breaches occurred, the agency lacked a centralized network security operations center from which it could continuously and comprehensively monitor all system security controls and threats.

The 2014 cyberattacks were "sophisticated, malicious, and carried out to obtain sensitive information for improper use." Arnold Plaintiffs' Compl. ¶¶ 128, 132, J.A. 73–74. Arnold Plaintiffs assert that as a result of these attacks, they have

suffered from a variety of harms, including the improper use of their Social Security numbers, unauthorized charges to existing credit card and bank accounts, fraudulent openings of new credit card and other financial accounts, and the filing of fraudulent tax returns in their names. At least three named Arnold Plaintiffs purchased credit monitoring services after falling victim to such fraud; others have spent time and money attempting to unwind fraudulent transactions made in their names. And some Arnold Plaintiffs who have yet to experience a fraud incident purchased credit monitoring services and spent extra time monitoring their accounts to mitigate the "increased risk" of identity theft caused by the breaches. *Id.* ¶ 163, J.A. 81–83.

Arnold Plaintiffs assert several claims against OPM, but they press only one on appeal: that the agency "willfully failed" to establish appropriate safeguards to ensure the security and confidentiality of their private information, in violation of Section 552a(e)(10) of the Privacy Act of 1974. Arnold Plaintiffs' Compl. ¶ 182, J.A. 89; *see also* 5 U.S.C. § 552a(e)(10) (requiring the agency to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained"). They also bring a variety of common-law and statutory claims against KeyPoint, alleging that the company's "actions and inactions constitute[d] negligence, negligent misrepresentation and concealment, invasion of privacy, breach of contract, and violations of the Fair Credit Reporting Act and state statutes." Arnold Plaintiffs' Compl. ¶ 9, J.A. 38. Arnold Plaintiffs seek damages from OPM under the Privacy Act; from KeyPoint, they request money damages and an order requiring the company to extend

free lifetime identity theft and fraud protection services to all putative class members, among other things.

The other complaint, filed by the National Treasury Employees Union, seeks declaratory and injunctive relief against the Acting Director of OPM in her official capacity based on essentially the same set of facts. NTEU Plaintiffs assert that when they provided OPM with the sensitive personal information ultimately exposed in the breaches, they did so upon the agency's assurance that it "would be safeguarded" and kept confidential. Amended Complaint for Declaratory and Injunctive Relief, *In re United States Office of Pers. Mgmt. Data Security Breach Litig.*, No. 1:15-mc-01394, ¶ 75 (D.D.C. June 3, 2016) ("NTEU Plaintiffs' Compl."), J.A. 179. They allege that OPM's "reckless failure to safeguard [NTEU Plaintiffs'] personal information," which ultimately "resulted in [its] unauthorized disclosure" during the 2014 attacks, *id.* at 3, J.A. 155, amounted to a violation of what they describe as their "constitutional right to informational privacy," *id.* ¶ 98, J.A. 186.

NTEU Plaintiffs further allege that, despite the fallout from the 2014 breaches, OPM has yet to make the cybersecurity improvements necessary to protect their personal information from future attacks. According to the complaint, the agency's Inspector General warned at the end of 2015 that OPM was ill-equipped to protect itself from another attack, given "the overall lack of compliance that seems to permeate the agency's IT security program." NTEU Plaintiffs' Compl. ¶ 88, J.A. 182 (quoting United States Office of Pers. Mgmt., Office of the Inspector General, Office of Audits, *Final Audit Report: Federal Information Security Modernization Act Audit FY 2015*, at 5 (Nov. 10, 2015)). NTEU Plaintiffs seek a declaration that OPM's failure to protect their information violated their putative constitutional right to informational

privacy and an order requiring the agency to provide them with free lifetime credit monitoring and identity theft protection. They also request an injunction requiring OPM "to take immediately all necessary and appropriate steps to correct deficiencies in [its] IT security program so that NTEU members' personal information will be protected from unauthorized disclosure" in the future. *Id.* at 35, J.A. 187.

OPM and KeyPoint moved to dismiss Arnold Plaintiffs' complaint, arguing that they lacked Article III standing, that their claims were barred by sovereign immunity, and that they failed to state valid claims under the state and federal statutes and common-law theories invoked. OPM moved to dismiss NTEU Plaintiffs' complaint for lack of standing and failure to state a claim upon which relief could be granted—that is, failure to allege a cognizable constitutional violation. The district court granted both motions to dismiss on the ground that neither Arnold Plaintiffs nor NTEU Plaintiffs pled sufficient facts to demonstrate Article III standing. Rejecting plaintiffs' argument that they faced a heightened risk of identity theft due to the breaches, the court held that the facts alleged failed to plausibly support the conclusion that this risk of future injury was either substantial or clearly impending. The district court ultimately concluded that only those plaintiffs who specifically identified out-of-pocket losses stemming from the actual misuse of their data had suffered an injury in fact sufficient for standing purposes. But even those plaintiffs lacked standing, the district court concluded, because they failed to allege facts demonstrating that the misuse of their information was traceable to the OPM breaches in particular.

The district court went on to explain that it also lacked subject matter jurisdiction over Arnold Plaintiffs' claims for the additional reasons that (i) they failed to plead the actual damages necessary to bring them within the Privacy Act's

waiver of sovereign immunity; and (ii) as a government contractor, KeyPoint enjoyed derivative sovereign immunity from suit. Finally, the court concluded that Arnold Plaintiffs failed to plausibly allege a Privacy Act claim and that NTEU Plaintiffs' complaint failed to state a constitutional claim. Both sets of plaintiffs have appealed.

We reverse in part and affirm in part the district court's judgment. We hold that both sets of plaintiffs have alleged facts sufficient to satisfy Article III standing requirements. Arnold Plaintiffs have stated a claim for damages under the Privacy Act, and have unlocked OPM's waiver of sovereign immunity, by alleging OPM's knowing refusal to establish appropriate information security safeguards. KeyPoint is not entitled to derivative sovereign immunity because it has not shown that its alleged security faults were directed by the government, and it is alleged to have violated the Privacy Act standards incorporated into its contract with OPM. Finally, we agree with the district court that, assuming a constitutional right to informational privacy, NTEU Plaintiffs have not alleged any violation of such a right.

II

"[T]he irreducible constitutional minimum of standing consists of three elements." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016) (internal quotation marks omitted). First, plaintiffs must demonstrate that they suffered an injury in fact that is "concrete and particularized and actual or imminent, not conjectural or hypothetical." *Id.* at 1548 (internal quotation marks omitted). "An allegation of future injury" passes Article III muster only if it "is 'certainly impending,' or there is a 'substantial risk' that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 & n.5 (2013)). Second, plaintiffs must demonstrate causation; that is, they must show

that their claimed injury is "fairly traceable to the challenged conduct of the defendant." *Spokeo*, 136 S. Ct. at 1547. "Article III standing does not require that the defendant be the most immediate cause, or even a proximate cause, of the plaintiffs' injuries; it requires only that those injuries be 'fairly traceable' to the defendant." *Attias v. Carefirst, Inc.*, 865 F.3d 620, 629 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018). And third, plaintiffs must demonstrate that "it is likely, as opposed to merely speculative, that the[ir] injury will be redressed by a favorable decision." *Friends of the Earth, Inc. v. Laidlaw Environmental Servs. (TOC), Inc.*, 528 U.S. 167, 181 (2000).

Where, as here, defendants challenge standing at the pleading stage without disputing the facts alleged in the complaint, "we accept the well-pleaded factual allegations as true and draw all reasonable inferences from those allegations in the plaintiff's favor," but we do not assume the truth of legal conclusions or accept inferences that are unsupported by the facts alleged in the complaint. *Arpaio v. Obama*, 797 F.3d 11, 19 (D.C. Cir. 2015). "We review de novo the district court's dismissal for lack of standing." *Id.* The question at this early juncture in the litigation is whether plaintiffs have plausibly alleged standing. Contrary to the district court's ruling, plaintiffs need not yet establish each element of standing by a preponderance of the evidence. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992) ("[E]ach element [of standing] must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.,* with the manner and degree of evidence required at the successive stages of the litigation.").

A

We begin with NTEU Plaintiffs. For standing purposes, we assume that NTEU Plaintiffs have, as they claim, a "constitutional right to informational privacy" that was

violated "the moment that [cyberattackers stole] their inherently personal information * * * from OPM's deficiently secured databases." NTEU Br. 11; *see also Estate of Boyland v. Department of Agric.*, 913 F.3d 117, 123 (D.C. Cir. 2019) ("[W]hen considering whether a plaintiff has Article III standing, a federal court must assume, *arguendo*, the merits of his or her legal claim.") (internal quotation marks omitted). Furthermore, given NTEU Plaintiffs' allegations regarding OPM's continued failure to adequately secure its databases, it is reasonable to infer that there remains a "substantial risk" that their personal information will be stolen from OPM again in the future. NTEU Plaintiffs' Compl. ¶ 88, J.A. 182. With respect to this claim, the loss of a constitutionally protected privacy interest itself would qualify as a concrete, particularized, and actual injury in fact. And the ongoing and substantial threat to that privacy interest would be a concrete, particularized, and *imminent* injury in fact. Both claimed injuries are plausibly traceable to OPM's challenged conduct, and the latter is redressable either by a declaration that the agency's failure to protect NTEU Plaintiffs' personal information is unconstitutional or by an order requiring OPM to immediately correct deficiencies in its cybersecurity programs. *Cf. ACLU v. Clapper*, 785 F.3d 787, 801 (2d Cir. 2015) (holding that, where plaintiffs allege a Fourth Amendment "injury [stemming] from the very collection of their telephone metadata," they "have suffered a concrete and particularized injury fairly traceable to the challenged program and redressable by a favorable ruling"). Accordingly, NTEU Plaintiffs have standing based on their claimed constitutional injury.

B

Arnold Plaintiffs allege no such constitutional injury, but they do claim to have suffered a variety of past and future data-breach related harms. *See, e.g.*, Arnold Plaintiffs' Compl. ¶ 22,

J.A. 44–45 (alleging that Plaintiff Jane Doe has "suffer[ed] stress resulting from concerns for her personal safety and that of her family members" since being informed by the FBI that her personal information "had been acquired by the so-called Islamic State of Iraq and al-Sham ('ISIS')"). For purposes of our standing analysis, we focus on one injury they all share: the risk of future identity theft. As we have already recognized, "identity theft * * * constitute[s] a concrete and particularized injury." *Attias*, 865 F.3d at 627; *see also Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 514 (D.C. Cir. 2016) (offering the "increased risk of fraud or identity theft" as an "example" of a "concrete consequence" for standing purposes). Yet, the district court concluded that Arnold Plaintiffs' complaint provided an insufficient basis from which to infer that, in the wake of the OPM breaches, Arnold Plaintiffs faced any meaningful risk of future identity theft, much less a "substantial" one. *In re United States Office of Pers. Mgmt. Data Security Breach Litig.* ("*In re OPM*"), 266 F. Supp. 3d 1, 35 (D.D.C. 2017). Furthermore, finding that "the risk of identity theft was neither clearly impending nor substantial," the district court concluded that any expenses that Arnold Plaintiffs incurred attempting to mitigate that risk likewise failed to qualify as an Article III injury in fact. *Id.* at 36; *see also Clapper*, 568 U.S. at 416 ("[R]espondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.").

Arnold Plaintiffs argue that the district court's conclusion is incompatible with our decision in *Attias v. CareFirst*. In that case, we determined that the victims of a cyberattack on CareFirst, a health insurance company, "cleared the low bar to establish their standing at the pleading stage" by plausibly alleging that they faced a substantial risk of identity theft as a result of the company's negligent failure to thwart the attack.

Attias, 865 F.3d at 622. Specifically, the complaint alleged that the breach exposed "all of the information wrongdoers need for appropriation of a victim's identity": personal identification information, credit card numbers, and Social Security numbers. *Id.* at 628 (internal quotation marks omitted). Based largely on the nature of the information compromised in the attack, we concluded that it was reasonable to infer that the cyberattackers had "both the intent and the ability to use that data for ill." *Id.*; *see also id.* at 628–629 ("Why else would hackers break into a * * * database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.") (quoting *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015)). Accordingly, we explained, "[n]o long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken." *Id.* at 629.

Although the OPM cyberattacks differ in several respects from the breach at issue in *Attias*, there is no question that the OPM hackers, too, now have in their possession all the information needed to steal Arnold Plaintiffs' identities. Arnold Plaintiffs have alleged that the hackers stole Social Security numbers, birth dates, fingerprints, and addresses, among other sensitive personal information. It hardly takes a criminal mastermind to imagine how such information could be used to commit identity theft. Indeed, several Arnold Plaintiffs claim that they have already experienced various types of identity theft, including the unauthorized opening of new credit card and other financial accounts and the filing of fraudulent tax returns in their names. Moreover, unlike existing credit card numbers, which, if compromised, can be changed to prevent future fraud, Social Security numbers and

addresses cannot so readily be swapped out for new ones. And, of course, our birth dates and fingerprints are with us forever. Viewing the allegations in the light most favorable to Arnold Plaintiffs, as we must, we conclude that not only do the incidents of identity theft that have already occurred illustrate the nefarious uses to which the stolen information may be put, but they also support the inference that Arnold Plaintiffs face a substantial—as opposed to a merely speculative or theoretical—risk of future identity theft.

It is worth noting that several Arnold Plaintiffs also allege that unauthorized charges have appeared on their existing credit card and bank account statements since the breaches. According to OPM, because none of these Arnold Plaintiffs "specifically alleged the OPM incidents affected their existing account information," the reported incidents of fraud on existing accounts (and, presumably, the risk of future fraud on those accounts) cannot plausibly be attributed to the OPM breaches. Gov't Br. 21. But we need not travel down that road because, regardless of whether the hackers obtained all the information necessary to make unauthorized charges to existing accounts, it is undisputed that the other forms of fraud alleged—the opening of new accounts and the filing of fraudulent tax returns—may be accomplished using the information stolen during the breaches at issue.

OPM argues that Arnold Plaintiffs' allegations of "scattered instances of widely varying fraud" are insufficient to support a plausible inference that Arnold Plaintiffs face an ongoing, substantial risk of identity theft. Gov't Br. 20. Specifically, OPM contends that despite the sensitive nature of the information stolen in the attacks, "[i]t is impossible under these circumstances to 'easily construct any kind of colorable theory' that a desire to commit fraud motivated" the OPM breaches. *Id.* at 21 (quoting *In re OPM*, 266 F. Supp. 3d at 38).

This is especially the case, OPM argues, because "this is not just a data breach," but rather "a data breach arising out of a particular sort of cyberattack" against the United States. *Id.* at 23 (quoting *In re OPM*, 266 F. Supp. 3d at 9). According to OPM, it is illogical to assume that the same goals that typically motivate hackers of commercial databases animated the "sophisticated" actors who engineered these data breaches. *Id.* at 27. The district court agreed with OPM on this point. Although neither amended complaint contains any allegations regarding the cyberattackers' identity, the court noted that news articles and congressional reports had suggested that the suspected perpetrator was not a common criminal, but rather the Chinese government. Despite acknowledging that "a finding concerning the source of the breach" was "beyond the scope of [the] proceeding at this juncture," the court appears to have relied at least partially on this external information in reaching the conclusion that it was implausible that the OPM hackers intended to steal Arnold Plaintiffs' identities. *In re OPM*, 266 F. Supp. 3d at 34.

As an initial matter, the district court should not have relied even in part on its own surmise that the Chinese government perpetrated these attacks. Absent any factual allegations regarding the identity of the cyberattackers, the district court was not free to conduct its own extra-record research and then draw inferences from that research in OPM's and KeyPoint's favor. *See Arpaio*, 797 F.3d at 19 (explaining that where the defendant challenges the plaintiff's standing at the motion-to-dismiss stage, we "draw all reasonable inferences * * * in the plaintiff's favor"). Beyond that, although a cyberattack on a government system might well be motivated by a purpose other than identity theft, given the type of information stolen in the OPM breaches and Arnold Plaintiffs' allegations regarding the subsequent misuse of that information, it is just as plausible to infer that identity theft is

at least one of the hackers' goals, even if those hackers are indeed affiliated with a foreign government.

Our dissenting colleague takes a different tack, suggesting that because this case involves *government* databases, "espionage * * * is * * * an 'obvious alternative explanation'" for the attacks. *See* Dissenting Op. at 4 (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 682 (2009)). We disagree as to just how obvious an explanation this is based on the facts alleged in the complaint. Furthermore, given that espionage and identity theft are not mutually exclusive, the likely existence of an espionage-related motive hardly renders implausible Arnold Plaintiffs' claim that they face a substantial future risk of identity theft and financial fraud as a result of the breaches. *See, e.g.*, *Watson Carpet & Floor Covering, Inc. v. Mohawk Indus., Inc.*, 648 F.3d 452, 458 (6th Cir. 2011) ("Ferreting out the most likely reason for the defendants' actions is not appropriate at the pleadings stage * * * . [T]he plausibility of [one particular] reason for the refusals to sell carpet does not render all other reasons implausible."). By contrast, in the cases cited by the dissent, the obvious alternative explanations were necessarily incompatible with the plaintiffs' versions of events. *See Iqbal*, 556 U.S. at 682 (rejecting claims of invidious discrimination as implausible where there existed an obvious, nondiscriminatory law enforcement justification for the challenged acts); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 567–568 (2007) (rejecting a conspiracy claim as implausible where history and market forces provided "a natural explanation" for the defendants' behavior).

In any case, although we found in *Attias* that the circumstances of that breach made it at least plausible that the hackers there had "both the intent and the ability to use [the plaintiffs'] data for ill," 865 F.3d at 628, a hacker's "intent" to use breach victims' personal data for identity theft becomes

markedly less important where, as here, several victims allege that they have *already* suffered identity theft and fraud as a result of the breaches. When considered in combination with the obvious potential for fraud presented by the information stolen during the breaches, the fact that certain Arnold Plaintiffs have already had fraudulent accounts opened and tax returns filed in their names moves the risk of future identity theft across the line from speculative to substantial, at least at this early stage in the proceedings. *See id.* at 625 (explaining that at the pleading stage, "plaintiffs are required only to state a *plausible* claim that each of the standing elements is present") (internal quotation marks omitted).

The circumstances here differ markedly from those in the two cases OPM cites in support of its argument that Arnold Plaintiffs' risk of future identity theft is merely conjectural. In *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), a laptop containing patients' unencrypted personal information, "including names, birth dates, the last four digits of social security numbers, and physical descriptors," and four boxes of medical records that contained names and Social Security numbers went missing from a Veterans Affairs medical center. *Id.* at 267–269. The Fourth Circuit held that the risk of future identity theft stemming from the incidents was too speculative to satisfy the injury-in-fact requirement because the plaintiffs failed to allege either (i) that the thief "intentionally targeted" the personal information contained in the laptop and boxes or (ii) that the thief subsequently used that information to commit identity theft. *Id.* at 274–275 ("[E]ven after extensive discovery, the * * * plaintiffs [who sued over the theft of the laptop] have uncovered no evidence that the information contained on the stolen laptop has been accessed or misused or that they have suffered identity theft, nor, for that matter, that the thief stole the laptop with the intent to steal their private information."); *id.* at 275 ("Watson's complaint suffers from

the same deficiency with regard to the four missing boxes of pathology reports."). Without such allegations, the Fourth Circuit explained, there was nothing to "push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent." *Id.* at 274.

In the other case, *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), an unknown hacker infiltrated a payroll processing firm's database, "potentially" gaining access to employees' "personal and financial information." *Id.* at 40. It was "not known whether the hacker read, copied, or understood the data," *id.*, and none of the affected parties alleged that their data had since been misused, *id.* at 44 ("Appellants have alleged no misuse."). Because the plaintiffs' claimed risk of future identity theft therefore rested solely on "hypothetical speculations concerning the possibility of future injury," the Third Circuit held that the risk was insufficient to support standing. *Id.* at 43.

Here, in contrast to those two cases, Arnold Plaintiffs both allege that the OPM cyberattackers intentionally targeted their information and point out the subsequent misuse of that information. *See* Arnold Plaintiffs' Compl. ¶¶ 128, 130, J.A. 73–74 (alleging that the hackers targeted—and extracted data from—the agency's "Electronic Official Personnel Folder system" and the database used to collect background check information); *see, e.g.*, *id.* ¶¶ 21–22, 24, 26, J.A. 44–48 (alleging incidents involving misuse of information). These are precisely the types of allegations missing in *Beck* and *Reilly*. *See Beck*, 848 F.3d at 275 ("[T]he mere theft of these items, *without more*, cannot confer Article III standing.") (emphasis added); *Reilly*, 664 F.3d at 44 ("Here, there is no evidence that the intrusion was intentional or malicious. Appellants have alleged no misuse * * * . Indeed, no

identifiable taking occurred; all that is known is that a firewall was penetrated.").

Although it is true, as a general principle, that "'as * * * breaches fade further into the past,' * * * threatened injuries become more and more speculative," we are unpersuaded by the dissent's suggestion that the passage of less than two years between these particular attacks and Arnold Plaintiffs' filing of the operative complaint is enough to render the threat of future harm insubstantial. Dissenting Op. at 7 (quoting *Beck*, 848 F.3d at 275). The plaintiffs in *Beck* suffered no misuse of their data prior to filing their complaint. *See supra* at 19–20. And the same was true of the plaintiffs in *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564 (D. Md. 2016), the case cited by the dissent and the court in *Beck* for the proposition that the threat of future injury diminishes over time. *See id.* at 570 (noting that plaintiffs had not experienced "*any* misuse" of their data prior to filing their complaint). Although the passage of two years in a run-of-the-mill data breach case might, absent allegations of subsequent data misuse, suggest that a claim of future injury is less than plausible, that is not the situation we face here. Conducted over several months by sophisticated and apparently quite patient cyberhackers, the attacks at issue in this case affected over twenty-one million people and involved information far more sensitive than credit card numbers. Cyberhacking on such a massive scale is a relatively new phenomenon, and we are unwilling at this stage to assume that the passage of a year or two without any clearly identifiable pattern of identity theft or financial fraud means that all those whose data was compromised are in the clear.

Drawing all reasonable inferences in Arnold Plaintiffs' favor, we conclude that they have alleged facts sufficient to support their claim of future injury, notwithstanding the passage of time and the governmental character of the

databases at issue here. Given the nature of the information stolen and the fact that several named Arnold Plaintiffs have already experienced some form of identity theft since the breaches, it is at least plausible that Arnold Plaintiffs run a substantial risk of falling victim to other such incidents in the future. *See Hutton v. National Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 621–622 (4th Cir. 2018) (finding a substantial risk of identity theft where the plaintiffs alleged not only that their information had been stolen by hackers, but also that it was subsequently "used in a fraudulent manner"). Because Arnold Plaintiffs adequately allege a substantial risk of future identity theft, any expenses they have reasonably incurred to mitigate that risk likewise qualify as injury in fact. *See id.* at 622 ("[T]he [Supreme] Court has recognized standing to sue on the basis of costs incurred to mitigate or avoid harm when a substantial risk of harm actually exists.") (citing *Clapper*, 568 U.S. at 414 n.5); *see also* Hearing Tr. 35 (Oct. 27, 2016) (credit protection services for victims of the breaches announced in June 2015 were not "up and running until September" of that year); Arnold Plaintiffs' Compl. ¶ 28, J.A. 48–49 (Plaintiff Kelly Flynn purchased credit monitoring in July 2015).

The district court evaluated the second element of Article III standing, causation, only as to the incidents of identity theft and fraud that Arnold Plaintiffs had already experienced. Observing that such incidents were "separated across time and geography, and they follow no discernable pattern," *In re OPM*, 266 F. Supp. 3d at 38, the court determined that it could not reasonably infer causation because Arnold Plaintiffs had not alleged "any facts that plausibly connect the various isolated incidents of the misuse * * * to the breaches at issue here," *id.* at 37. The district court did not go on to consider whether Arnold Plaintiffs plausibly alleged that a risk of *future* identity theft was fairly traceable to OPM's and KeyPoint's

cybersecurity failings, presumably because it had already rejected that risk as merely speculative. We can make relatively short work of such an inquiry here.

Arnold Plaintiffs have alleged facts supporting a reasonable inference that their claimed data breach-related injuries are fairly traceable to OPM's failure to secure its information systems. Not only do Arnold Plaintiffs detail OPM's failure to heed repeated warnings by its own Inspector General regarding serious vulnerabilities in the agency's systems, but they also allege that as a result of that failure, hackers managed to breach key OPM systems on several different occasions.

With respect to KeyPoint, Arnold Plaintiffs further allege that the company's failure to properly secure its login credentials "was a substantial factor in causing the Data Breaches." Arnold Plaintiffs' Compl. ¶ 228, J.A. 99. KeyPoint contends that Arnold Plaintiffs' complaint fails to trace the breaches to any actual misconduct by KeyPoint, but that argument lacks merit. Arnold Plaintiffs' complaint alleges not only that the hackers accessed OPM's systems "using stolen KeyPoint credentials," *id.* ¶ 127, J.A. 73, but also that the company was negligent in "failing to protect and secure its * * * credentials," *id.* ¶ 228, J.A. 99, by, among other things, "failing to * * * comply with industry-standard data security practices," *id.* ¶ 223(b), J.A. 98. It is reasonable to infer that "data security practices" would cover practices related to securing credentials. It is likewise reasonable to infer, based on the allegations contained in the complaint, that KeyPoint is at least partially to blame for the breaches due to its failure to comply with such practices.

As previously explained, even if the breaches in question did not expose all information necessary to make fraudulent

charges on victims' existing financial accounts, the personal data the hackers did manage to obtain is enough, by itself, to enable several forms of identity theft. That fact, combined with the allegations that at least some of the stolen information was actually misused after the breaches, suffices to support a reasonable inference that Arnold Plaintiffs' risk of future identity theft is traceable to the OPM cyberattacks. Neither the likelihood that some Arnold Plaintiffs experienced other types of unrelated fraud nor the speculative possibility that they might also have been the victims of other data breaches renders causation implausible here. *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1029 (9th Cir. 2018) ("That hackers might have stolen Plaintiffs' [personal identifying information] in unrelated breaches, and that Plaintiffs might suffer identity theft or fraud caused by the data stolen in those other breaches * * *, is less about standing and more about the merits of causation and damages."), *cert. denied*, 139 S. Ct. 1373 (2019). Nor are we troubled, as OPM suggests we should be, by certain Arnold Plaintiffs' failure to specify exactly when, in relation to the data breaches, fraudsters first misused their data. The Supreme Court has explained that "[a]t the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the claim." *Lujan*, 504 U.S. at 561 (formatting altered). Accordingly, as in *Attias*, at this early stage, we have "little difficulty concluding," 865 F.3d at 629, that Arnold Plaintiffs have met their "relatively modest" burden of alleging that their risk of future identity theft is fairly traceable to OPM's and KeyPoint's challenged conduct, *Bennett v. Spear*, 520 U.S. 154, 171 (1997).

This brings us, then, to the final element of standing, where, as previously noted, we ask whether "it is likely, as opposed to merely speculative" that Arnold Plaintiffs' claimed

injury "will be redressed by a favorable decision." *Friends of the Earth*, 528 U.S. at 181. Although the district court never reached this question, we think Arnold Plaintiffs have easily demonstrated that their substantial risk of future identity theft and related mitigation expenses are redressable.

Granting that it may well be impossible at this point to eliminate the risk of future identity theft stemming from the OPM breaches, the money damages Arnold Plaintiffs seek can redress certain proven injuries related to that risk (such as reasonably-incurred credit monitoring costs). *See, e.g.*, *In re Zappos.com*, 888 F.3d at 1030 ("The injury from the risk of identity theft is also redressable by relief that could be obtained through this litigation. If Plaintiffs succeed on the merits, any proven injury could be compensated through damages.") (citation omitted); *Attias*, 865 F.3d at 629 ("The fact that plaintiffs have reasonably spent money to protect themselves against a substantial risk creates the potential for them to be made whole by monetary damages.").

In sum, like the *Attias* plaintiffs, both sets of plaintiffs here have "cleared the low bar to establish their standing at the pleading stage." 865 F.3d at 622. Arnold Plaintiffs have plausibly alleged a substantial risk of future identity theft that is fairly traceable to OPM's and KeyPoint's cybersecurity failings and likely redressable, at least in part, by damages, and NTEU Plaintiffs have plausibly alleged actual and imminent constitutional injuries that are likewise traceable to OPM's challenged conduct and redressable either by a declaration that the agency's failure to protect plaintiffs' personal information is unconstitutional or by an order requiring OPM to correct deficiencies in its cybersecurity program. We therefore have no need to address the other bases for standing asserted by NTEU and Arnold Plaintiffs. *See, e.g.*, *id.* at 626 n.2 (explaining that when plaintiffs have standing "based on their

heightened risk of future identity theft," it is unnecessary to address their other theories of injury in fact).

Having resolved the standing issue in NTEU and Arnold Plaintiffs' favor, we turn to another potential jurisdictional stumbling block: sovereign immunity.

III

It is "axiomatic" that a waiver of sovereign immunity is a jurisdictional "prerequisite" for Arnold Plaintiffs' claims against OPM to get out of the starting gate. *United States v. Mitchell*, 463 U.S. 206, 212 (1983); *accord Federal Deposit Ins. Corp. v. Meyer*, 510 U.S. 471, 475 (1994). The Privacy Act, 5 U.S.C. § 552a, provides just such a waiver of sovereign immunity. That statute "safeguards the public from unwarranted collection, maintenance, use and dissemination of personal information contained in agency records." *Henke v. Department of Commerce*, 83 F.3d 1453, 1456 (D.C. Cir. 1996) (quoting *Bartel v. Federal Aviation Admin.*, 725 F.2d 1403, 1407 (D.C. Cir. 1984)). As part of that obligation, the Act mandates that federal agencies "protect the privacy of individuals identified in information systems maintained by [them]." Pub. L. No. 93-579, § 2(a)(5), 88 Stat. 1896, 1896 (1974). The Privacy Act waives sovereign immunity by expressly authorizing a cause of action for damages against federal agencies that violate its rules protecting the confidentiality of private information in agency records. *See Tomasello v. Rubin*, 167 F.3d 612, 617–618 (D.C. Cir. 1999).

The district court nonetheless ruled that OPM's sovereign immunity remained intact, reasoning that Arnold Plaintiffs failed to allege the type of harms covered by the Privacy Act. Reviewing the district court's dismissal of the Privacy Act claim *de novo*, *Skinner v. Department of Justice*, 584 F.3d

1093, 1096 (D.C. Cir. 2009), we reverse. OPM's allegedly willful failure to protect Arnold Plaintiffs' sensitive personal information against the theft that occurred falls squarely within the Privacy Act's ambit.

To unlock the Privacy Act's waiver of sovereign immunity and state a cognizable claim for damages, a plaintiff must allege that (i) the agency "intentional[ly] or willful[ly]" violated the Act's requirements for protecting the confidentiality of personal records and information; and (ii) she sustained "actual damages" (iii) "as a result of" that violation. 5 U.S.C. § 552a(g)(4); *see Chichakli v. Tillerson*, 882 F.3d 229, 233 (D.C. Cir. 2018). At this threshold stage of the litigation, Arnold Plaintiffs have plausibly alleged each of those elements.

A

To start, Arnold Plaintiffs have straightforwardly alleged a "willful" violation of the Privacy Act's requirements. 5 U.S.C. § 552a(g)(4). OPM was necessarily aware that the Privacy Act requires it to "establish appropriate administrative, technical, and physical safeguards" that "insure the security and confidentiality of records," and to "protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." 5 U.S.C. § 552a(e)(10).

The complaint alleges in no uncertain terms that OPM dropped that ball because appropriate safeguards were not in place. *See, e.g.*, Arnold Plaintiffs' Compl. ¶ 134, J.A. 74 ("OPM's decisions not to comply with [Information Security Act] requirements for critical security safeguards enabled hackers to access and loot OPM's systems for nearly a year

without being detected."); *id.* ¶ 178, J.A. 87 ("Despite known and persistent threats from cyberattacks, OPM allowed multiple 'material weaknesses' in its information security systems to continue unabated. As a result, Plaintiffs' and Class members' [government investigation information] under OPM's control was exposed, stolen, and misused.").

Of course, violating the Privacy Act is not by itself enough. The agency's transgression must have been "intentional or willful." 5 U.S.C. § 552a(g)(4). Under the Privacy Act, willfulness means more than "gross negligence." *Maydak v. United States*, 630 F.3d 166, 179 (D.C. Cir. 2010); *see also Coleman v. United States*, 912 F.3d 824, 836–837 (5th Cir. 2019) ("at least gross negligence"); *Beaven v. Department of Justice*, 622 F.3d 540, 549 (6th Cir. 2010) ("something greater than gross negligence"); *Hogan v. England*, 159 F. App'x 534, 537 (4th Cir. 2005) ("somewhat greater than gross negligence") (formatting altered); *Johnston v. Horne*, 875 F.2d 1415, 1422 (9th Cir. 1989) ("conduct amounting to more than gross negligence"), *overruled on other grounds*, *Irwin v. Department of Veterans Affairs*, 498 U.S. 89 (1990). Allegations that the agency's conduct was "disjointed" or "confused," or that errors were "inadvertent[]" will not suffice. *Maydak*, 630 F.3d at 180 (internal quotation marks omitted).

Instead, a complaint must plausibly allege that the agency's security failures were "in flagrant disregard of [their] rights under the Act," were left in place "without grounds for believing them to be lawful," or were "so patently egregious and unlawful that anyone undertaking the conduct should have known it unlawful." *Maydak*, 630 F.3d at 179; *accord* 120 Cong. Rec. 40406 (1974) ("Analysis of House and Senate Compromise Amendments to the Federal Privacy Act") ("On a continuum between negligence and the very high standard of willful, arbitrary, or capricious conduct, this standard is viewed

as only somewhat greater than gross negligence."); *see also Beaven*, 622 F.3d at 549 (requiring defendants to have "committ[ed] the act without grounds for believing it to be lawful, or flagrantly disregard[ed] others' rights under the Privacy Act") (formatting altered); *Andrews v. Veterans Admin.*, 838 F.2d 418, 425 (10th Cir. 1988) (agency "action [must be] so patently egregious and unlawful that anyone undertaking the conduct should have known it unlawful, or conduct committed without grounds for believing it to be lawful or [an] action flagrantly disregarding others' rights under the Act") (formatting altered).[1]

Arnold Plaintiffs' complaint clears that hurdle by plausibly and with specificity alleging that OPM was willfully indifferent to the risk that acutely sensitive private information was at substantial risk of being hacked. According to the complaint, at the time of the breach, OPM had long known that its electronic record-keeping systems were prime targets for hackers. The agency suffered serious data breaches from hackers in 2009 (millions of users' personal information stolen) and 2012 (OPM access credentials stolen and posted online), and is subject to at least *ten million* unauthorized electronic

[1] *Cf. McLaughlin v. Richland Shoe Co.*, 486 U.S. 128, 132–133 (1988) ("willful" under the Fair Labor Standards Act includes "reckless[]" violations); *Trans World Airlines, Inc. v. Thurston*, 469 U.S. 111, 126 (1985) (willfulness in the Age Discrimination in Employment Act includes "reckless disregard for the matter of whether [the defendant's] conduct was prohibited by" the Act); *United States v. Murdock*, 290 U.S. 389, 395 (1933) ("willful" violation of the Revenue Acts of 1926 and 1928 is "marked by careless disregard [for] whether or not one has the right so to act"); *Dayton Tire v. Secretary of Labor*, 671 F.3d 1249, 1254 (D.C. Cir. 2012) (willful violation of the Occupational Safety and Health Act is "an act done voluntarily with either an intentional disregard of, or plain indifference to, the Act's requirements").

intrusion attempts *every month*. Arnold Plaintiffs' Compl. ¶¶ 78–79, J.A. 64.

Despite that pervading threat, OPM effectively left the door to its records unlocked by repeatedly failing to take basic, known, and available steps to secure the trove of sensitive information in its hands. Information Security Act audits by OPM's Inspector General repeatedly warned OPM about material deficiencies in its information security systems. Among the identified flaws were

- severely outdated security policies and procedures;
- permitting employees to leave open, or to not terminate, remote access;
- understaffed and undertrained cybersecurity personnel;
- failure to implement or enforce multi-factor identification in *any* of its major information systems;
- declining to patch or install security updates for its systems promptly;
- lacking a mature vulnerability scanning program to find and track the status of security weaknesses in its systems;
- failure to maintain a centralized information security management structure that would continuously monitor security events and controls;
- lacking the ability to detect unauthorized devices connected to its network; and
- failure to engage in appropriate oversight of its contractor-operated systems.

So forewarned, OPM chose to leave those critical information security deficiencies (and more) in place. On top of that, in the year that the hacks occurred, OPM (allegedly)

also left undone mandated security assessments and authorizations for half of its electronic record-keeping systems. 44 U.S.C. § 3554(b); *id.* § 3544(b) (repealed 2014); Arnold Plaintiffs' Compl. ¶¶ 101–102, J.A. 69 (no information security assessments conducted for eleven of the twenty-one systems). The risk created by these lapses was so serious that the Inspector General took the unprecedented step of advising OPM to shut down all the systems lacking valid authorizations until adequate security measures could be put in place. OPM declined, choosing instead to continue operating these systems.

The complaint's plausible allegations that OPM decided to continue operating in the face of those repeated and forceful warnings, without implementing even the basic steps needed to minimize the risk of a significant data breach, is precisely the type of willful failure to establish appropriate safeguards that makes out a claim under the Privacy Act. *See American Fed'n of Gov't Employees v. Hawley*, 543 F. Supp. 2d 44, 52 (D.D.C. 2008) (Department of Homeland Security's failure to establish appropriate safeguards to prevent losing a computer hard drive was "intentional and willful" given the Inspector General's repeated warnings of "recurring, systemic, and fundamental deficiencies" in the agency's information security); *In re Department of Veterans Affairs (VA) Data Theft Litig.*, No. 06–0506 (JR), 2007 WL 7621261, at *4–5 (D.D.C. Nov. 16, 2007) (Department of Veterans Affairs' failure to establish appropriate safeguards to protect against theft of laptop and hard drive was "intentional and willful" in light of the Government Accountability Office's repeated warnings of "deficiencies" in the agency's "information security").

B

Arnold Plaintiffs' lawsuit is not in the clear yet. The complaint must also allege facts showing that they suffered

"actual damages" as "a result of" OPM's Privacy Act violation. 5 U.S.C. § 552a(g)(4). The complaint rises to that task as well.

1

"Actual damages" within the meaning of the Privacy Act are limited to proven pecuniary or economic harm. *Federal Aviation Admin. v. Cooper*, 566 U.S. 284, 298–299 (2012). The district court concluded that only two Arnold Plaintiffs had properly alleged that they suffered "actual damages": Jane Doe, who incurred legal fees when she retained a law firm to close fraudulent accounts opened in her name, and Charlene Oliver, whose electricity account had been fraudulently accessed and saddled with unauthorized charges.

While those harms certainly qualify as actual damages, the complaint contains still more relevant allegations of injury.

First, nine of the named Arnold Plaintiffs purchased credit protection and/or credit repair services after learning of the breach. Paul Daly, for example, purchased credit monitoring services after a fraudulent 2014 tax return was filed in his name. And Teresa J. McGarry subscribed to a monthly credit and identity protection service to prevent identity theft. Those reasonably incurred out-of-pocket expenses are the paradigmatic example of "actual damages" resulting from the violation of privacy protections. *See Cooper*, 566 U.S. at 298.[2]

OPM counters that those individual purchases were unnecessary because Congress provided credit monitoring

[2] Congress authorized the expenditure of hundreds of millions of taxpayer dollars to purchase ten years' worth of fraud and credit monitoring services to protect victims of the data breach. *See* Consolidated Appropriations Act, Pub. L. No. 115-31, § 633(a), 131 Stat. 135, 376 (2017).

services for potentially affected individuals. Congress, though, did not offer credit repair services. Anyhow, the argument wrongly assumes facts in OPM's favor at the complaint stage, such as that the services offered were equal or superior to those obtained privately, or that they took effect in a timely manner and for a sufficient period of time. *See Agnew v. District of Columbia*, 920 F.3d 49, 53 (D.C. Cir. 2019) (on a motion to dismiss "we assume the truth of all plaintiffs' plausibly pleaded allegations, and draw all reasonable inferences in their favor"). Notably, at least one named plaintiff purchased credit monitoring services *before* OPM's offered services were "up and running." *Compare* Hearing Tr. 35*, with* Arnold Plaintiffs' Compl. ¶ 28, J.A 48–49.

Second, seven of the named Arnold Plaintiffs had accounts opened and purchases made in their names. For example, Kelly Flynn and her husband had several new credit card accounts fraudulently opened in their names. They also discovered that two separate loans totaling $6,400 had been taken out in their names without their permission and were now delinquent. Those financial losses qualify as "actual damages." *See Cooper*, 566 U.S. at 298–299.

The district court deemed those damages insufficient because Arnold Plaintiffs did not further allege that their costs went unreimbursed. That was error. At this stage of the litigation, all facts and reasonable inferences must be drawn in favor of Arnold Plaintiffs, and the complaint provides no basis for disregarding the claimed financial losses based on OPM's speculation that Arnold Plaintiffs were indemnified. *See Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 513–514 (D.C. Cir. 2016).

Anyhow, "an injured person may usually recover in full from a wrongdoer regardless of anything he may get from a

collateral source unconnected with the wrongdoer." *Kassman v. American Univ.*, 546 F.2d 1029, 1034 (D.C. Cir. 1976) (per curiam) (formatting altered); *accord* Restatement (Second) of Torts § 920A(2). That rule prevents the victim's benefits from becoming the tortfeasor's windfall. *See Hudson v. Lazarus*, 217 F.2d 344, 346 (D.C. Cir. 1954). So too here.

OPM also objects that only some forms of reimbursement qualify for the collateral source rule. Gov't Br. 45. Again, OPM gets the cart before the horse, because the complaint contains no allegations about recompense at all, let alone what their sources were. OPM's argument also offers an overly cramped vision of the collateral source rule. *See Hudson*, 217 F.2d at 346 (without limiting the collateral source rule's application, observing that it applies to "gift[s] or the product of a contract of employment or of insurance"); Restatement (Second) of Torts § 920A cmt. c (offering a non-exclusive list of "types of benefits" to which the collateral source rule applies); *see also, e.g.*, *Temme v. Bemis Co.*, 762 F.3d 544, 549 (7th Cir. 2014) (per curiam) (applying the collateral source rule to attorneys' fees payments).

Third, Plaintiffs Kelly Flynn and six others had false tax returns filed using their information and have experienced delays in receiving federal and state tax refunds. The delay in those Plaintiffs' receipt of their refunds, and the forgone time value of that money, is an actual, tangible pecuniary injury.

OPM argues "no harm, no foul" because the Internal Revenue Service must pay taxpayers interest due for delayed refunds. *See* 26 U.S.C. § 6611. That misses the mark. To start, interest on tax overpayments is itself taxable income, *id.* § 61(a)(4); *Megibow v. Commissioner*, 102 T.C.M. (CCH) 232 (2011), while interest incurred in taking out loans to cover the delayed refunds is not deductible, 26 U.S.C. § 163(h)(1). That

makes the IRS's payment scheme inherently under compensatory. On top of that, the IRS pays interest only on delayed *federal* refunds, not state tax refunds. Arnold Plaintiffs' Compl. ¶ 28, J.A. 49 (alleging delay in state tax refund); *see generally* 26 U.S.C. § 6611(a) ("Interest shall be allowed and paid upon any overpayment in respect of any *internal revenue tax*.") (emphasis added).

Lastly, one Plaintiff, Lillian Gonzalez-Colon, spent more than 100 hours to resolve the fraudulent tax return filing and to close a fraudulently opened account. Those efforts "required her to take time off work[]" to address the consequences of the OPM breach. Arnold Plaintiffs' Compl. ¶ 31, J.A. 50–51; *see Beaven*, 622 F.3d at 557–559 (concluding that plaintiffs could claim damages for "lost time" spent "dealing with the disclosure" of their Bureau of Prison personnel files).

OPM urges us to hold Gonzalez-Colon to Federal Rule of Civil Procedure 9(g)'s requirement that "special damages" be "specifically stated." Fed. R. Civ. P. 9(g). We have not yet addressed whether Rule 9(g)'s heightened pleading standard applies to Privacy Act claims, and we have no occasion to do so here. Gonzalez-Colon's specific allegations about the time lost from work addressing the fraudulent tax return and Verizon Wireless account suffice either way. *See* 5A Charles A. Wright & Arthur R. Miller, Federal Practice & Procedure § 1311 (4th ed. 2019) ("[A]llegations of special damage will be deemed sufficient for the purpose of Rule 9(g) if they are definite enough to notify the opposing party and the court of the nature of the damages and enable the preparation of a responsive pleading.").

For all of those reasons, Arnold Plaintiffs have adequately alleged actual damages within the meaning of the Privacy Act.

2

The complaint also explains how Arnold Plaintiffs' actual damages were the "result of" OPM's Privacy Act violations. 5 U.S.C. § 552a(g)(4)(A).

To meet the Privacy Act's causation requirement, Arnold Plaintiffs must plausibly allege that the OPM hack was the "proximate cause" of their damages. *Dickson v. Office of Pers. Mgmt.*, 828 F.2d 32, 37 (D.C. Cir. 1987). That is, OPM's conduct must have been a "substantial factor" in the sequence of events leading to Arnold Plaintiffs' injuries, and those injuries must have been "reasonably foreseeable or anticipated as a natural consequence" of OPM's conduct. *Owens v. Republic of Sudan*, 864 F.3d 751, 794 (D.C. Cir. 2017). To be the proximate cause is not necessarily to be the sole cause. *See Hecht v. Pro-Football, Inc.*, 570 F.2d 982, 996 (D.C. Cir. 1977). OPM was the proximate cause of the harm befalling Arnold Plaintiffs so long as its conduct created a foreseeable risk of harm through the hackers' intervention. *See Staub v. Proctor Hosp.*, 562 U.S. 411, 420 (2011); Restatement (Second) of Torts § 442A.

The complaint alleges facts demonstrating proximate cause. Arnold Plaintiffs contend that OPM's failure to establish appropriate information security safeguards opened the door to the hackers, giving them ready access to a storehouse of personally identifiable and sensitive financial information. In particular, the complaint explains that OPM's failure to adopt basic protective measures "foreseeably heightened the risk of a successful intrusion into OPM's systems." Arnold Plaintiffs' Compl. ¶ 134, J.A. 74. And its decisions to disregard the Inspector General's repeated warnings and "not to comply with [Information Security Act] requirements for critical security safeguards enabled hackers to

access and loot OPM's systems for nearly a year without being detected." *Id.*; *see id.* ¶¶ 105–113, J.A. 70–71.

The proof is in the pudding: Numerous Arnold Plaintiffs suffered forms of identity theft accomplishable only with the type of information that OPM stored and the hackers accessed. That directly links the hack to the theft of the victims' private information, the pecuniary harms suffered, and the ongoing increased susceptibility to identity theft or financial injury. *See* Arnold Plaintiffs' Compl. ¶¶ 14, 17, 21–22, 24–26, 28–29, 31–32, 34, 39–41, 45, 49, J.A. 40–59; *Attias v. CareFirst, Inc.*, 865 F.3d 620, 629 (D.C. Cir. 2017) (plaintiffs plausibly alleged risk of identity theft for Article III standing purposes based on the nature of the stolen data), *cert. denied*, 138 S. Ct. 981 (2018).[3] To argue, as OPM does, that the presumed occurrence of other data breaches defeats a causal connection as a matter of law at this early stage again wrongly construes inferences drawn from generic assertions about the general risk of data breaches in the government's favor. The law would embody quite a "perverse

[3] *See also Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1327 (11th Cir. 2012) (plaintiffs plausibly alleged that data breach proximately caused their identity theft for purposes of Florida law by "alleg[ing] that the sensitive information on the stolen laptop was the same sensitive information used to steal Plaintiffs' identity"); *Stollenwerk v. Tri–West Health Care All.*, 254 F. App'x 664, 667 (9th Cir. 2007) (plaintiff established that data breach proximately caused identity theft for purposes of Arizona law where plaintiff provided his personal information to defendant, the identity fraud incidents began six weeks after defendant's systems were compromised, and plaintiff had not previously suffered from identity theft); *In re Community Health Sys., Inc.*, No. 15-CV-222-KOB, 2016 WL 4732630, at *25 (N.D. Ala. Sept. 12, 2016) (plaintiff plausibly alleged causal link between data breach and identity theft by "alleg[ing] misuse occurring subsequent to the breach that would be consistent with the type of data stolen").

incentive" were it to hold at this threshold stage of litigation that, "so long as enough data breaches take place," agencies "will never be found liable." *In re Equifax, Inc., Customer Data Security Breach Litig.*, 362 F. Supp. 3d 1295, 1318 (N.D. Ga. 2019) (formatting altered); *accord In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 988 (N.D. Cal. 2016).

In any event, OPM makes no claim that these particular plaintiffs have been subjected to hacks of equivalent breadth and depth, sweeping in such acutely sensitive personal information as Social Security numbers, fingerprints, and birth certificates.

In sum, Arnold Plaintiffs have adequately alleged (i) that OPM willfully chose not to establish basic and necessary information security safeguards in violation of Section 552a(e)(10) of the Privacy Act, and (ii) that those actions proximately caused (iii) actual damages in multiple, specific ways. Because the complaint, at this threshold stage, states a viable Privacy Act claim, OPM's sovereign immunity has been waived.

IV

In addition to their Privacy Act claim against OPM, Arnold Plaintiffs assert statutory and common law claims against OPM's contractor, KeyPoint Government Solutions. Arnold Plaintiffs' Compl. ¶¶ 208–275, J.A. 94–110 (alleging negligence, negligent misrepresentation and concealment, invasion of privacy, violation of the Fair Credit Reporting Act, 15 U.S.C. § 1681, violation of "State Statutes Prohibiting Unfair and Deceptive Trade Practices," violation of "State Data Breach Acts," and breach of contract).

OPM tasked KeyPoint with performing background and security clearance investigations and inputting the sensitive information it collected into OPM's electronic recordkeeping system. The hackers allegedly were able to obtain KeyPoint credentials and then used them to gain access to OPM's network. *See* Arnold Plaintiffs' Compl. ¶ 106, J.A. 70.

The district court held that, as OPM's contractor, KeyPoint enjoyed "derivative sovereign immunity" from those claims. We review the applicability of derivative sovereign immunity *de novo*, *see Cunningham v. General Dynamics Info. Tech., Inc.*, 888 F.3d 640, 645 (4th Cir. 2018), *cert. denied*, 139 S. Ct. 417 (2018), and find no basis for its application in this case. OPM's contract obligated KeyPoint to meet the same standards for protecting personal information that the Privacy Act imposes directly on OPM. Because the improper conduct alleged would have violated the Privacy Act if committed by OPM itself and because KeyPoint's challenged misconduct was not directed by OPM, there is no sovereign immunity for KeyPoint to derive.[4]

As a private company, KeyPoint ordinarily would not enjoy immunity against the statutory and tort claims asserted by Arnold Plaintiffs. But government contractors may sometimes "obtain certain immunity in connection with work which they do pursuant to their contractual undertakings with the United States." *Campbell-Ewald Co. v. Gomez*, 136 S. Ct. 663, 672 (2016) (internal quotation marks omitted) (quoting *Brady v. Roosevelt S.S. Co.*, 317 U.S. 575, 583 (1943)).

[4] Neither OPM nor the Justice Department in its brief in this case has endorsed KeyPoint's claim of derivative sovereign immunity.

Derivative sovereign immunity, though, is less "embracive" than the immunity a sovereign enjoys. *Campbell-Ewald*, 136 S. Ct. at 672. It applies only when a contractor takes actions that are "authorized and directed by the Government of the United States," and "performed pursuant to the Act of Congress" authorizing the agency's activity. *Id.* at 673. In that way, derivative sovereign immunity ensures that "'there is no liability on the part of the contractor' who simply performed as the Government directed." *Id.* (quoting *Yearsley v. W.A. Ross Constr. Co.*, 309 U.S. 18, 21 (1940)); *id.* at 673 n.7 ("Critical in *Yearsley* was not the involvement of public works, but the contractor's performance in compliance with all federal directions."). Said another way, a government contractor that "violates both federal law and the government's explicit instructions" loses the shield of derivative immunity and is subject to suit by those adversely affected by the contractor's violations. *Id.* at 672.

Like the plaintiff in *Campbell-Ewald*, Arnold Plaintiffs have plausibly alleged that KeyPoint's failure to secure its credentials ran afoul of both OPM's explicit instructions and federal law standards, rendering derivative sovereign immunity unavailable.

At the outset, KeyPoint's failure to place in the record its contract with OPM makes it particularly difficult for it to establish, on a motion to dismiss, that its alleged security lapses were "authorized and directed" by OPM, *Campbell-Ewald*, 136 S. Ct. at 673 (quoting *Yearsley*, 309 U.S at 20). *See generally Banneker Ventures, LLC v. Graham*, 798 F.3d 1119, 1133 (D.C. Cir. 2015).

In fact, Privacy Act regulations require OPM, when contracting "for the operation * * * of a system of records to accomplish an agency function," to "cause the requirements"

of the Privacy Act to be "applied to such system." 5 U.S.C. § 552a(m)(1); *see* 48 C.F.R. §§ 24.102(a), 24.104, 52.224-2. KeyPoint does not deny that. So KeyPoint was obligated by contract and regulation to, among other things, establish "appropriate safeguards to insure the security and confidentiality of records." 5 U.S.C. § 552a(e)(10); *see* Arnold Plaintiffs' Compl. ¶ 123, J.A. 72–73.

The complaint expressly asserts that KeyPoint failed to fulfill those obligations, which led to the break-in. KeyPoint allegedly violated its regulatory and contractual obligations, among other things, to (i) "secure its systems for gathering and storing" government investigation information despite "knowing of [its] vulnerabilities;" (ii) "comply with industry-standard data security practices;" (iii) "perform requisite due diligence and supervision in expanding its workforce;" (iv) "encrypt [government investigation information] at collection, at rest, and in transit;" (v) "employ adequate network segmentation and layering;" (vi) "ensure continuous system and event monitoring and recording;" and (vii) "otherwise implement security policies and practices sufficient to protect * * * [government investigation information] from unauthorized disclosure." Arnold Plaintiffs' Compl. ¶ 223, J.A. 98. Notably, it was KeyPoint's alleged failure to secure and protect its employees' log-in credentials that allowed the hackers to access OPM's system in May 2014, and it was from there that the hackers ultimately stole 21.5 million background investigation records.

Unsurprisingly, KeyPoint does not argue that OPM "authorized and directed" it to design its system with the security flaws that Arnold Plaintiffs identify. *Campbell-Ewald*, 136 S. Ct. at 673. So KeyPoint cannot wrap itself in derivative immunity garb on the ground that it "simply performed as the Government directed." *Id.*

The district court felt differently, concluding that derivative immunity applied because the Privacy Act is wholly inapplicable to KeyPoint. It is true that the Privacy Act itself does not apply directly to government contractors like KeyPoint. *See Abdelfattah v. Department of Homeland Security*, 787 F.3d 524, 533 n.4 (D.C. Cir. 2015) ("[T]he Privacy Act creates a cause of action against only federal government agencies and not private corporations or individual officials.").

But that is beside the point. To claim immunity, KeyPoint had to establish "compliance with all federal directions" pertaining to its relevant conduct, including the regulatory and contractual obligation to meet the Privacy Act's standards in its contract operations. *Campbell-Ewald*, 136 S. Ct. at 673 n.7.

So what matters for derivative sovereign immunity purposes is KeyPoint's (i) inability to point to a contractual provision or other OPM direction authorizing or directing the very gaps in security protections over which Arnold Plaintiffs are suing, and (ii) its *regulatory* duty to ensure informational security equivalent to that demanded by the Privacy Act. 48 C.F.R. §§ 24.102(a), 24.104, 52.224-2. Add to that the absence of sovereign immunity protections for OPM from the Privacy Act claims in this case, and the sovereign immunity well from which KeyPoint seeks to draw has run dry.

The district court also pointed to Section 552a(m)(1) of the Privacy Act, which provides that the contractor and its employees "shall be considered employees of the agency[,]" and to a regulation providing that "the system of records operated under the contract is deemed to be maintained by the agency." *In re OPM*, 266 F. Supp. 3d at 48–49 (quoting 48

C.F.R. § 24.102(c)). Neither supports the application of derivative sovereign immunity here.

Even under the district court's reading, Section 552a(m)(1) hurts rather than helps KeyPoint. OPM's and its employees' own immunity has been waived. So treating KeyPoint employees like OPM employees gets KeyPoint nowhere. It cannot derive an immunity that OPM itself does not have. *See Campbell-Ewald*, 136 S. Ct. at 666 (asking whether "*the sovereign's* immunity from suit shield[s] the [contractor] * * * as well") (emphasis added); *see also Contango Operators, Inc. v. United States*, 965 F. Supp. 2d 791, 814 (S.D. Tex. 2013) (because "[n]o sovereign immunity has been established," the court "therefore concludes that there is no governmental immunity from which an immunity may be derived for the benefit of" the contractor), *aff'd sub nom. Contango Operators, Inc. v. Weeks Marine, Inc.*, 613 F. App'x 281 (5th Cir. 2015); *cf. McMahon v. Presidential Airways, Inc.*, 502 F.3d 1331, 1345 (11th Cir. 2007) (reasoning that if a federal officer cannot claim complete derivative immunity, then neither can a mere common law agent, because otherwise "a prison guard employed by the government would have only qualified immunity, while a private contractor who works in the prison but is no more than a common law agent would have absolute immunity").

After all, the driving purpose of derivative sovereign immunity "is to prevent the contractor from being held liable when the government is actually at fault but is otherwise immune from liability." *In re World Trade Center Disaster Site Litig.*, 456 F. Supp. 2d 520, 560 (S.D.N.Y. 2006) (internal quotation marks omitted), *aff'd*, 521 F.3d 169 (2d Cir. 2008); *cf. Filarsky v. Delia*, 566 U.S. 377, 390–391 (2012) (if qualified immunity is withheld from private individuals "acting on behalf of the government," "government employees will

often be protected from suit by some form of immunity, [while] those working alongside them could be left holding the bag—facing full liability for actions taken in conjunction with government employees who enjoy immunity for the same activity").

In any event, the district court overread the statute. When the Privacy Act speaks of contractors as "employees" of the agency, it does so for the purpose of extending *criminal* liability to contractors and their employees if they violate certain Privacy Act requirements. 5 U.S.C. § 552a(i), (m)(1). Congress's decision to subject federal contractors to the same Privacy Act criminal prohibitions as their agency employers hardly augurs in favor of according those same contractors *more* protection from civil liability than the agency itself.

As for the district court's reliance on 48 C.F.R. § 24.102(c), that regulation says nothing about contractors' responsibility for complying with their contractual and regulatory obligations. The rule simply holds the contracting agency responsible for "the system of records operated under the contract." 48 C.F.R. § 24.102(c), (d). Which makes sense. Otherwise, the government would be able to contract itself out of the Privacy Act obligations that Congress imposed.

Beyond that, KeyPoint's argument frequently mixes apples and oranges, citing preemption cases in an effort to substantiate its claim to derivative immunity. KeyPoint Br. 24–26. That tactic will not work. Those preemption cases do not turn on the applicability of derivative sovereign immunity. And KeyPoint has not raised a preemption argument in this court, so any argument to that effect is forfeited for purposes of this appeal. *See Al-Tamimi v. Adelson*, 916 F.3d 1, 6 (D.C. Cir. 2019) ("A party forfeits an argument by failing to raise it in his opening brief.").

In sum, derivative sovereign immunity has its limits. KeyPoint exceeded those limits, and for that reason cannot don the cloak of derivative sovereign immunity.

V

Finally, we turn to NTEU Plaintiffs' constitutional claim. In that claim, NTEU Plaintiffs do not allege that OPM intentionally disclosed the records at issue or performed the functional equivalent of such a disclosure. *See, e.g.*, NTEU Plaintiffs' Compl. ¶ 97, J.A. 186 (alleging "reckless indifference"). Instead, NTEU Plaintiffs challenge OPM's internal record-management and storage practices and policies as unconstitutionally trenching on their asserted constitutional right to privacy. *See, e.g.*, *id.* at 3, J.A. 155 ("Although on notice of serious flaws in its data system security, OPM failed to adequately secure personal information in its possession—a failure that was reckless under the circumstances."). They appear to rely on two closely related threads of constitutional doctrine, one couched in terms of privacy and relying mainly on dicta from *Whalen v. Roe*, 429 U.S. 589 (1977), the other phrased more directly in terms of substantive due process and relying mainly on cases providing relief for persons harmed through government neglect of their personal safety. We address them in that order.

A

As NTEU Plaintiffs see it, the Constitution creates a "zone of privacy" that protects an individual's "interest in avoiding disclosure of personal matters." NTEU Br. 36 (quoting *Whalen*, 429 U.S. at 598–599). This putative right to "informational privacy," they contend, is violated not only where government agents intentionally disclose an individual's

personal information, but where, as alleged here, the agents "reckless[ly]" fail to prevent a third party from stealing it. NTEU Plaintiffs' Compl. 3, J.A. 155; *see also* Oral Arg. Tr. 44:23–45:5.

Even assuming "without deciding[] that the Constitution protects" some "sort" of privacy "interest in avoiding disclosure of personal matters," *NASA v. Nelson*, 562 U.S. 134, 138 (2011) (quoting *Whalen*, 429 U.S. at 599–600), NTEU Plaintiffs have failed to state a legally cognizable claim. There is no authority for their contention that the Constitution imposes on the government an affirmative duty—untethered to specific constitutional provisions such as the First Amendment, *see, e.g.*, *Americans for Prosperity Found. v. Becerra*, 903 F.3d 1000, 1019 (9th Cir. 2018)—to "safeguard personal information" from the criminal acts of third parties, NTEU Plaintiffs' Compl. ¶ 97, J.A. 186.

The asserted duty to "adequately secure" government computer networks finds no support in the Constitution or our history. NTEU Plaintiffs' Compl. 3, J.A. 155. Not once do NTEU Plaintiffs quote the very document from which they purport to derive their claimed right: the Constitution of the United States. Nor, for that matter, do they invoke this "Nation's history and tradition," *Aka v. United States Tax Court*, 854 F.3d 30, 34 (D.C. Cir. 2017) (quoting *Washington v. Glucksberg*, 521 U.S. 702, 720–721 (1997))—an integral part of the formula for identifying *unenumerated* rights.

NTEU Plaintiffs instead ground their claim in a single line of Supreme Court dictum from more than 40 years ago that describes "[t]he cases sometimes characterized as protecting 'privacy'" as involving, among other interests, a vague "individual interest in avoiding disclosure of personal matters." NTEU Br. 36 (quoting *Whalen*, 429 U.S. at 599). But neither

we nor the Supreme Court has ever held that this interest is a constitutional right. *American Fed'n of Gov't Employees v. Department of Hous. & Urban Dev.*, 118 F.3d 786, 791 (D.C. Cir. 1997) ("The Supreme Court has addressed the issue in recurring dicta without, we believe, resolving it."). Both courts have, so far, steadfastly rejected all informational privacy claims purporting to rest on the Constitution, while simply "assum[ing]"—but never "deciding"—that the Constitution protects a "right of the sort mentioned in *Whalen*." *NASA*, 562 U.S. at 138; *see Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425, 457–458 (1977); *Whalen*, 429 U.S. at 605; *American Fed'n of Gov't Employees*, 118 F.3d at 791. Indeed, neither this court nor the Supreme Court has ever elaborated on the rationale for—or even defined the "precise contours of"—the putative right to informational privacy. *American Fed'n of Gov't Employees*, 118 F.3d at 793; *see also, e.g.*, *NASA*, 562 U.S. at 147–148. Rather, we have underlined its "ambiguity." *National Fed'n of Fed. Employees v. Greenberg*, 983 F.2d 286, 293 (D.C. Cir. 1993); *cf. Siegert v. Gilley*, 500 U.S. 226, 233–234 (1991) (holding that even malicious government defamation does not trigger constitutional protection) (citing *Paul v. Davis*, 424 U.S. 693 (1976)).

Other circuits, to be sure, have embraced a form of the putative right. *See, e.g.*, *In re Crawford*, 194 F.3d 954, 958 (9th Cir. 1999); *see also NASA*, 562 U.S. at 146 n.9 (collecting cases). *But see Doe v. Wigginton*, 21 F.3d 733, 740 (6th Cir. 1994). But NTEU Plaintiffs have identified no case in which the government has been held to have violated the alleged right without having "*affirmatively provid[ed]* the protected information to those unauthorized to view it." NTEU Br. 47 (emphasis added). Neither have we. Absent any plausible mooring in the Constitution's text or the Nation's history and tradition, we join the district court in declining to recognize the proposed constitutional right to informational privacy that

would be violated not only when information is intentionally disclosed (or the functional equivalent), but also "when a third party *steals* it." *In re OPM*, 266 F. Supp. 3d at 46.

Troubled as we are by NTEU Plaintiffs' allegations regarding the severity and scope of OPM's data security shortcomings, we are nonetheless reluctant to constitutionalize an information security code for the government's "internal operations." *NASA*, 562 U.S. at 151 (citing *Engquist v. Oregon Dep't of Agric.*, 553 U.S. 591, 598–599 (2008)). OPM "collect[ed] and store[d]" the information at issue here not as sovereign, but as employer—in "its role as the federal civil service's personnel manager." NTEU Plaintiffs' Compl. ¶ 10, J.A. 159. In this capacity—"'as proprietor' and manager of [the government's] 'internal operation,'" *NASA*, 562 U.S. at 148 (quoting *Cafeteria & Rest. Workers Union v. McElroy*, 367 U.S. 886, 896 (1961))—OPM was "dealing 'with citizen *employees*,'" and thus had a "much freer hand" than it would have had if it had brought "its sovereign power to bear on citizens at large," *id.* (emphasis added) (quoting *Engquist*, 553 U.S. at 598). That "freer hand" exists for good reason. Whereas the "Constitution requires that a President chosen by the entire Nation oversee the execution of the laws," albeit by a "vast and varied federal bureaucracy," *Free Enter. Fund v. Public Co. Accounting Oversight Bd.*, 561 U.S. 477, 499 (2010), constitutionally micromanaging employment records management systems, reaching down to the details of "how [best] to protect" the "information systems" holding employee data, NTEU Br. 48, would shift a material part of that oversight function to the judiciary, which generally lacks established standards or guideposts for making such administrative judgments—at least in the absence of congressional direction. *Cf. Bishop v. Wood*, 426 U.S. 341, 349–350 (1976).

Another reason counsels hesitation. Establishing judicial supervision over the security of the government's employee data would "short-circuit" the response that Congress has already launched. *District Attorney's Office for Third Judicial Dist. v. Osborne*, 557 U.S. 52, 73 (2009) (citing *Glucksberg*, 521 U.S. at 720). As the Supreme Court observed in *NASA*, Congress has in the Privacy Act adopted significant "protections against disclosure" of personal information that "'evidence a proper concern' for individual privacy." 562 U.S. at 156 (quoting *Whalen*, 429 U.S. at 605). Here, as there, the Act limits the government's ability to maintain records "about an individual," 5 U.S.C. § 552a(e)(1), and "imposes criminal liability for willful violations of its nondisclosure obligations," 562 U.S. at 156 (citing 5 U.S.C. § 552a(i)(1)). NTEU Plaintiffs, of course, allege that OPM has "fail[ed] to satisfy" these obligations, NTEU Plaintiffs' Compl. ¶ 97, J.A. 186, and argue that their "inherently personal information remains at substantial risk of additional breaches because" of OPM's failures, Oral Arg. Tr. 49:17–19. But if NTEU Plaintiffs are right (as we must assume in the current posture of the case), then they may invoke the remedial provisions found by Congress to best balance privacy and competing interests. *See* 5 U.S.C. § 552a(g)(1)(D), (g)(4); *cf. supra* Part III.A (reversing dismissal of Arnold Plaintiffs' Privacy Act claims).

Establishing a freestanding constitutional right to informational privacy that creates a duty to safeguard personal information from unauthorized access by third parties would force us to develop a labyrinth of technical rules. *See Osborne,* 557 U.S. at 73–74. For example, does the Constitution require data "encrypt[ion]"? NTEU Br. 6 (citing NTEU Plaintiffs' Compl. ¶¶ 51–52, J.A. 172–173). If so, must all data be encrypted in transit, as well as at rest? *Cf.* Arnold Plaintiffs' Compl. ¶¶ 136, 223, J.A. 75, 98. What of the encryption key: Is 256 bits necessary—or would 128 bits scrape by,

constitutionally speaking? *See* Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L.J. 989, 993 (2018) (illustrating the difference). How about "personal identity verification (PIV) credentials"—are they constitutionally mandated? NTEU Plaintiffs' Compl. ¶ 47, J.A. 171 (internal quotation marks omitted). And most significant: What "tools" should "federal courts * * * use to answer" these questions? *Osborne*, 557 U.S. at 74. NTEU Plaintiffs do not say; more important, neither does the Constitution.

We therefore hold that, assuming (without deciding) the existence of a constitutional right to informational privacy, *see, e.g.*, *NASA*, 562 U.S. at 138; *American Fed'n of Gov't Employees*, 118 F.3d at 791, it affords relief only for intentional disclosures or their functional equivalent—which NTEU Plaintiffs do not allege.

B

NTEU Plaintiffs also seek to ground their claim in the Due Process Clause of the Fifth Amendment, contending specifically that, in some instances, "reckless or deliberate indifference" (as opposed to intentional misconduct) "may 'shock the conscience sufficiently to violate due process.'" NTEU Reply Br. 13 (quoting *Smith v. District of Columbia*, 413 F.3d 86, 93 (D.C. Cir. 2005)); *see also* NTEU Br. 47–48; Oral Arg. Tr. 74:3–9. True enough. *See, e.g.*, *United States v. Salerno*, 481 U.S. 739, 746 (1987) (citing *Rochin v. California*, 342 U.S. 165, 172 (1952)).

But the conscience's susceptibility to shock varies radically with whether the government has previously taken an "affirmative act of restraining the individual's freedom to act on his own behalf—through incarceration, institutionalization, or similar restraint of personal liberty." *DeShaney v. Winnebago Cnty. Dep't of Soc. Servs.*, 489 U.S. 189, 200

(1989). Thus, a prisoner who has "already been deprived of [his] liberty," for example, has a plausible claim to affirmative governmental protection. *Collins v. City of Harker Heights*, 503 U.S. 115, 127 (1992); *see also Smith*, 413 F.3d at 94–95 (same for "juvenile delinquent held 'against his will'"). Absent such a restraint, however, the government's "failure to protect an individual from private [acts], even in the face of known danger, [generally] 'does not constitute a violation of the Due Process Clause.'" *Butera v. District of Columbia*, 235 F.3d 637, 647 (D.C. Cir. 2001) (quoting *DeShaney*, 489 U.S. at 197). "The state must protect those it throws into snake pits, but the state need not guarantee that volunteer snake charmers will not be bitten." *Walker v. Rowe*, 791 F.2d 507, 511 (7th Cir. 1986) (explaining that although a state has a constitutional duty to protect prisoners in its custody, it has no such obligation toward prison guards who have voluntarily accepted employment with the state).

Here, NTEU Plaintiffs' claims fall on the wrong side of this line; they assert an affirmative government duty to safeguard personal information that current and prospective employees *voluntarily* submitted to the government.

This lack of compulsion makes all the difference. In *Collins*, for example, the Supreme Court rejected the claim—made by the widow of a city sanitation worker killed in the performance of his duties—that the Due Process Clause required the government to "provide its employees with certain minimal levels of safety and security." 503 U.S. at 127. A government employee, the Court reasoned, could not maintain "that the [government] deprived [him] of his liberty"—and thus incurred a "continuing obligation" to protect that liberty by guaranteeing him a minimum level of safety and security—"when it made, and he voluntarily accepted, an offer of employment." *Id.* at 128. That is precisely why, applying the

principle in cases posing the distinction most directly, we have rejected claims by prison guards. *See Fraternal Order of Police Dep't of Corrs. Labor Comm. v. Williams*, 375 F.3d 1141, 1147 (D.C. Cir. 2004); *Washington v. District of Columbia*, 802 F.2d 1478, 1482 (D.C. Cir. 1986).

Similar logic applies here. Like the sanitation worker in *Collins*—and the prison guards in *Williams* and *Washington*—NTEU Plaintiffs "voluntarily" sought and "accepted" an "offer of [government] employment." *Collins*, 503 U.S. at 128. In doing so, they voluntarily submitted personal information "as part of a background investigation." NTEU Plaintiffs' Compl. ¶ 60, J.A. 176. In no sense, then, did the government compel NTEU Plaintiffs to seek government employment; it therefore bore no constitutional duty under the Due Process Clause to protect them from the risks associated with applying for such positions. With no triggering deprivation of liberty or property to speak of, there arose no constitutional governmental duty to "provide [NTEU Plaintiffs] with certain minimal levels of safety and security," *Collins*, 503 U.S. at 127—physical or digital.

VI

In sum, we reverse in part and affirm in part. We hold that (i) NTEU and Arnold Plaintiffs have adequately alleged Article III standing; (ii) Arnold Plaintiffs have stated a claim under the Privacy Act, which waives OPM's sovereign immunity; (iii) KeyPoint is not protected by derivative sovereign immunity; and (iv) NTEU Plaintiffs have failed to state a claim that flaws in OPM's information-storage measures violated the Constitution. We remand for further proceedings consistent with this opinion.

So ordered.

WILLIAMS, *Senior Circuit Judge*, concurring in part and dissenting in part:

Why did "sophisticated" cyberintruders spend several months systematically and covertly extracting 21.5 million highly sensitive background investigation records for federal government employees from the Office of Personnel Management? Arnold Plaintiffs' Compl. ¶ 128, J.A. 73. Plaintiffs' answer is identity theft. Might the hackers have been members of a criminal syndicate looking to sell the information to identity thieves on the dark web to bilk victims such as Mr. Travis Arnold out of "approximately $125"? *Id.* ¶ 13, J.A. 40. Yes, theoretically. But as a basis for standing for most Arnold Plaintiffs the garden-variety identity theft theory lacks the necessary plausibility in light of an obvious alternative explanation: The breach "d[oes] not plausibly suggest" identity theft as the motive (and hence a source of future harm) because it is "more likely explained" as the handiwork of foreign spies looking to harvest information about millions of federal workers for espionage or kindred purposes having nothing to do with identity theft. *Ashcroft v. Iqbal*, 556 U.S. 662, 680 (2009); see Br. of Chamber of Commerce of U.S. as *Amicus Curiae* in Support of Appellees 6 ("Nation-states frequently target personally identifying information . . . in order to spy on certain individuals." (brackets omitted)).

My colleagues do not deny the possibility. See *Maj. op.* 17 ("[A] cyberattack on a government system might well be motivated by a purpose other than identity theft . . . ."). Yet, in assessing standing, they conclude that "all" 21.5 million Arnold Plaintiffs have "plausibly alleged a substantial risk" that they will, due to this particular data breach, suffer "future identity theft." *Id.* at 14, 25.

Respectfully, I disagree. Because Arnold Plaintiffs have failed to allege facts that would tend to negate the "obvious

alternative explanation" for the breach (i.e., espionage), they have not, in my view, "nudged [their] claims . . . across the line from conceivable to plausible." *Iqbal*, 556 U.S. at 680, 682 (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 567, 570 (2007)). I would therefore affirm the dismissal of Arnold Plaintiffs' claims for lack of standing—with one exception, discussed below. As a result, I join the court's opinion in full except with respect to any portions that are inconsistent with this dissent, including but not limited to Parts II.B (holding that Arnold Plaintiffs stated a plausible claim to standing) and III.B.2 (holding that Arnold Plaintiffs stated a plausible claim that their injuries were the "result of" the breach).

* * *

Two aspects of the standing analysis are important here. First, standing "depends on the facts as they exist[ed] when the complaint [was] filed." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 569 n.4 (1992) (emphasis removed) (quoting *Newman-Green, Inc. v. Alfonzo-Larrain*, 490 U.S. 826, 830 (1989)). We therefore look, not to the apparent risk of future identity theft in, say, May *2014*—the date of the first major breach, see Arnold Plaintiffs' Compl. ¶ 127, J.A. 73—but to the risk apparent in March *2016*, when Arnold Plaintiffs filed their operative complaint.

Second, standing "must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Lujan*, 504 U.S. at 561). Thus, "at the motion to dismiss stage," Arnold Plaintiffs' standing allegations must satisfy the pleading requirements of *Twombly* and *Iqbal*—that is, the complaint must state "'a plausible claim' that each element of standing is

satisfied." *Hancock v. Urban Outfitters, Inc.*, 830 F.3d 511, 513 (D.C. Cir. 2016) (quoting *Iqbal*, 556 U.S. at 678–79). This standard "asks for more than a sheer possibility," *Iqbal*, 556 U.S. at 678, that Arnold Plaintiffs faced a "substantial risk" that future injury would occur, *Susan B. Anthony List*, 573 U.S. at 158 (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)). Facts "that are 'merely consistent with'" a substantial risk of future identity theft fall "'short of the line between possibility and plausibility of 'entitlement to relief.'" *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 557).

Under these standards, most Arnold Plaintiffs lack standing. This is not your typical case, where hackers break into a commercial entity's servers and steal consumer information. In those cases, it is generally fair to infer—as this court has inferred—that the hackers plan to, "sooner or later," "make fraudulent charges or assume [the victims'] identities." *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628–29 (D.C. Cir. 2017) (quoting *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015)). "Why else would hackers break into a . . . database and steal consumers' private information?" *Id*. at 628 (alteration in original) (quoting *Remijas*, 794 F.3d 693). In such cases there's no obvious alternative explanation.

But here there is. In this case, hackers infiltrated a *government* system and stole sensitive "government investigation information," Arnold Plaintiffs' Compl. ¶ 1, J.A. 36, about *government* employees shortly after a cyberattack on the same agency had "compromised critical security documents," *id*. ¶ 3, J.A. 37. It is thus fair to infer, as the majority quite rightly recognizes, that the hackers "might well [have been] motivated by a purpose other than identity theft," *Maj. op.* 17, such as obtaining secret information from the persons in the files by extortion or surveillance, enlisting them as agents, obtaining leverage over American businesses, or

otherwise jeopardizing U.S. national security, see Br. of Chamber of Commerce of U.S. as *Amicus Curiae* in Support of Appellees 6; cf. Arnold Plaintiffs' Compl. ¶ 1, J.A. 36 (explaining that exposed and stolen information includes "private facts collected in federal background and security clearance investigations"); see also *id*. ¶ 129, J.A. 73–74 (specifying that the theft covered "many million questionnaire forms containing highly sensitive personal, family, financial, medical, and associational information"). This espionage motive is, as *Iqbal* and *Twombly* put it, an "obvious alternative explanation"—an explanation that Arnold Plaintiffs, to survive a motion to dismiss, must deflect. *Iqbal*, 556 U.S. at 682 (quoting *Twombly*, 550 U.S. at 567).

This they fail to do. Just as "parallel conduct" in *Twombly* "does not suggest conspiracy" in antitrust cases because it is consistent with "independent action" in competitive markets, *Twombly*, 550 U.S. at 556–57; and just as detention of "thousands of Arab Muslim men" in *Iqbal* does not suggest discrimination because (given the identity of the September 11th attackers) it is consistent with legitimate law enforcement activity, *Iqbal*, 556 U.S. at 681–82, so too a "cyberattack on a government system" does not suggest identity theft (of the type alleged by plaintiffs) because it is consistent with an obvious alternative explanation—foreign espionage, *Maj. op.* 17; see also *Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir. 2017) (finding no standing based on a "risk of future identity theft" where there is no evidence that the thief stole the laptop "with the intent to steal [plaintiffs'] private information").

What of dual motives, asks the majority? Couldn't the hackers have been interested in espionage *and* identity theft? *Maj. op.* 18. Yes, that's *conceivable*. But does the conceivability actually render plaintiffs' theory plausible? I don't think so. The majority invokes a syllogism: Because

"espionage and identity theft are not mutually exclusive," it follows that ascribing an "espionage-related motive" doesn't "render[] implausible" an allegation of "future risk of identity theft and financial fraud" caused by the data breach. *Id*. But it does exactly that. To begin with, even if the alternative explanations in *Iqbal* and *Twombly* happened to be mutually exclusive with plaintiffs' theories, the Court has never suggested that mutual exclusivity is a *prerequisite* to one plausible explanation's rendering some other explanation implausible. This case shows why such a prerequisite would be overkill. Just because two states of affairs *can* co-occur doesn't make their co-occurrence *plausible*—the legal standard plaintiffs must clear—nor does an otherwise implausible theory get bootstrapped into a plausible one merely because it's conceivable that it could co-occur with an obvious alternative explanation.

So while a foreign government might theoretically have enlisted "sophisticated" hackers to execute a "massive" cyberattack on the U.S. government over the course of "several months" to steal highly "sensitive" information, *Maj. op.* at 21, both to (i) compromise U.S. national security *and* (ii) commit fraud by (for example) purchases through an unauthorized Best Buy account (Arnold Plaintiffs' Compl. ¶ 39, J.A. 54), this dual-motive hypothesis seems fanciful for at least two reasons. First, the goal of identity theft is financial gain. The notion that a foreign state pursuing a complex, risky, and possibly expensive cyberespionage scheme would have as even one of its goals the extraction of small-potatoes sums from individuals by, e.g., filing fraudulent returns with the *United States* IRS or creating a "My Social Security" account, see *id*. ¶ 14, J.A. 40–41, falls far short of plausibility. Second, and more important, a foreign power seeking leverage over the United States would be most unlikely to permit its agents to use or sell the data for identity theft purposes, as doing so would risk *sabotaging* the

espionage goal. If data gleaned from the hack is slated for counterintelligence use, identity theft would undercut this aim by alerting victims and causing them to alter their data. Since the expected value of successful counterintelligence likely far exceeds that of identity theft, an espionage explanation affirmatively suggests that identity theft *will not* co-occur. And that is precisely what the record suggests. There is, as discussed below, a striking dearth of allegations as to any pattern of unusual or higher-than-ordinary identity theft or fraud among Arnold Plaintiffs. What readily comes to mind is an obvious alternative explanation—hacking focused entirely on pursuit of espionage and kindred threats to national security.

Thus the Sixth Circuit's caution—that "[f]erreting out the most likely reason for the defendants' actions is not appropriate at the pleadings stage," *Watson Carpet & Floor Covering, Inc. v. Mohawk Industries, Inc.*, 648 F.3d 452, 458 (6th Cir. 2011)—is inapt here. The court states in the immediately preceding sentence: "Often, defendants' conduct has several *plausible* explanations." *Id*. (emphasis added). Sorting out which among them is "most likely" is, indeed, out of bounds at the pleadings stage. Yet the whole thrust of my argument is that we haven't got "several plausible explanations." We have one alleged theory—identity theft—that, I argue, is not plausible in view of an obvious alternative explanation of far greater probability. Though it's unimpeachable logic to say that "[t]he plausibility of [one particular] reason for the refusals to sell carpet does not render all other reasons implausible," *id*., the point—made in context of a discussion of "several plausible explanations"—is not at play here, and marshaling it only begs the question whether identity theft is, in fact, a plausible explanation.

More is needed to "nudge[]" Arnold Plaintiffs' identity theft claims "across the line from conceivable to plausible."

Iqbal, 556 U.S. at 680 (quoting *Twombly*, 550 U.S. at 570). That is especially true here given the passage of time. As the initial breach occurred nearly *two years* before Arnold Plaintiffs filed their operative complaint, one would expect to see—if plaintiffs were right about the hackers' motives—some allegation linking Arnold Plaintiffs as a whole to the breach—such as indications that persons in the OPM databases suffered a relatively high rate of identity thefts, or a pattern of *similar* thefts. But there are no such allegations. And "'as the breaches fade further into the past,' the Plaintiffs' threatened injuries become more and more speculative." *Beck*, 848 F.3d at 275 (quoting *Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 570 (D. Md. 2016)).

The majority generally agrees, conceding that the "passage of two years in a run-of-the-mill data breach might, absent allegation of subsequent data misuse, suggest that a claim of future injury is less than plausible." *Maj. op.* 21. Yet my colleagues think such an inference is not fair game here, where the breach occurred on "a massive scale" reflecting "a relatively new phenomenon." *Id*. Large-scale hacking is no doubt a recent phenomenon. But I can think of no attributes of such phenomena or their possible novelty that would invalidate a common sense expectation that future identity-theft-type injuries will become less plausible as time drags on without result. Whatever else may be true, if identity theft is an operative motive, time remains of the essence, given that much personal data—credit card numbers, bank account information, addresses—can go stale with time. If anything, the special features of this case make the passage of time exceptionally forceful in undermining plaintiffs' theory. The extraordinary volume of people affected and the exceptional sensitivity and range of the information captured should make it relatively easy to discern a "pattern of identity theft or financial fraud" among the pool of 21.5 million potential victims (and

litigants)—if there is one. *Id*. And yet, as the majority agrees, we have no "clearly identifiable pattern of identity theft or financial fraud" in the Complaint. *Id*.

To be sure, "certain Arnold Plaintiffs have already had fraudulent accounts opened and tax returns filed in their names." *Maj. op.* 19. But that is hardly probative. "In a society where around 3.3% of the population will experience some form of identity theft" in a given year, it is "not surprising" that a few plaintiffs in a putative class of 21.5 million would "have experienced some form of credit or bank-account fraud." *In re U.S. Office of Personnel Mgmt. Data Sec. Breach Litig.*, 266 F. Supp. 3d 1, 38 (D.D.C. 2017) (quoting *In re Science Applications Int'l Corp. Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 32 (D.D.C. 2014)). A handful of Arnold Plaintiffs, for instance, almost certainly experienced a home invasion since the data breach. But that doesn't imply a "substantial risk" that *these hackers* have plans to break into the homes of garden-variety government employees.

In sum, Arnold Plaintiffs have alleged no facts—disproportionate incidence of identity theft, a distinctive pattern of fraud, or anything else of that sort among the putative class—that can credibly nudge their theory into the realm of plausibility in the face of an obvious alternative explanation. So they cannot "all" meet the threshold requirement for standing under the pleading standards of *Iqbal* and *Twombly*. *Maj. op.* 14.

I grant, of course, that in the immediate aftermath of the cyber-intrusion, some putative class members might reasonably have been unwilling to assume that the attack was motivated by a purpose other than identity theft. Thus, individuals at that early time, before the paucity of identity theft data emerged, might have "reasonably spent money to

protect themselves" from identity theft and thus have a plausible claim to standing to recover their expenses. *Attias*, 865 F.3d at 629. But that says nothing about whether, when plaintiffs filed their operative complaint two years later, all 21.5 million putative class members could *still* "reasonably" fear "a substantial risk" of identity theft. *Id*. at 629. They have shown no such thing.

* * *

For the subset of Arnold Plaintiffs who, as I see it, have standing, I turn to the issue of sovereign immunity. Arnold Plaintiffs file a battery of state law claims against a contractor that OPM engaged to perform background checks of prospective federal employees. That contractor, KeyPoint Government Solutions, Inc., maintains that, as a government contractor, it is entitled to sovereign immunity. The court, however, disagrees, see *Maj. op.* Part IV—and I join that part of the opinion in full.

I write separately to address an important distinction between contractor immunity, which KeyPoint asserts, and federal preemption, which KeyPoint fails to raise, and about which the court therefore expresses no views. See, e.g., KeyPoint's Br. 25 (distinguishing between preemption and immunity); Oral Arg. Tr. 31:3–21 (same); see also *Cunningham v. Gen. Dynamics Info. Tech., Inc.*, 888 F.3d 640, 646 n.4 (4th Cir. 2018) (same); *In re KBR, Inc., Burn Pit Litig.*, 744 F.3d 326, 342 n.6 (4th Cir. 2014) (same). Contractor immunity, it seems to me, immunizes only those acts that agents of the government are expressly directed by the government to perform—such as building a particular dike as "directed by the Government of the United States." See, e.g., *Yearsley v. W.A. Ross Construction Co.*, 309 U.S. 18, 20 (1940). Preemption, in contrast, is broader, knocking aside

state tort law to the extent that it impermissibly interferes with a contractor's ability to perform its federal obligations.

As the Supreme Court explained in *Boyle v. United Technologies Corp.*, there are "a few areas, involving 'uniquely federal interests,'" that "are so committed by the Constitution and laws of the United States to federal control that state law is pre-empted and replaced, where necessary, by federal law." 487 U.S. 500, 504 (1988) (quoting *Texas Industries, Inc. v. Radcliff Materials, Inc.*, 451 U.S. 630, 640 (1981)). The "civil liabilities arising out of the performance of federal procurement contracts" is one of them. *Id*. at 505–06. That is because "the Federal Government's interest in the procurement of equipment is implicated by" state tort suits, even where, as here, "the dispute is one between private parties." *Id*. at 506. Specifically, the "imposition of liability on Government contractors will directly affect the terms of Government contracts: either the contractor will decline to manufacture the design specified by the Government, or it will raise its price. Either way, the interests of the United States will be directly affected." *Id*. at 507.

To protect these interests, state law may be "displace[d]." *Id*. at 507. This will occur only where "a 'significant conflict' exists between an identifiable 'federal policy or interest and the [operation] of state law,'" *id*. (alteration in original) (quoting *Wallis v. Pan Am. Petroleum Corp.*, 384 U.S. 63, 68 (1966)), "or the application of state law would 'frustrate specific objectives' of federal legislation," *id*. (quoting *United States v. Kimbell Foods, Inc.*, 440 U.S. 715, 728 (1979)). "In some cases, for example where the federal interest requires a uniform rule, the entire body of state law applicable to the area conflicts and is replaced by federal rules." *Id*. at 508 (citing *Clearfield Trust Co. v. United States*, 318 U.S. 363, 366–67 (1943)). "In others, the conflict is more narrow, and only particular

elements of state law are superseded." *Id*. (citing *United States v. Little Lake Misere Land Co.*, 412 U.S. 580, 595 (1973)).

Here, there is a plausible argument for preemption. This case involves a fundamental federal issue—the hiring, vetting, and protecting of federal employees, and the balancing of the costs of keeping the relevant data secure against the costs of error or neglect in providing that security. And Congress, it seems, has already created a detailed statutory scheme in the form of the Privacy Act to address these (and other) issues. See, e.g., 5 U.S.C. § 552a(e)(10) (requiring "appropriate . . . technical . . . safeguards"). Under that scheme, the agency must, by contract, "cause the requirements of [the Privacy Act] to be applied" to the contractor's "system of records," see 5 U.S.C. § 552a(m)(1)—and if the *agency* fails to do so, then it faces potential liability, see *id*. § 552a(g)(1)(D); see also 48 C.F.R. § 24.102(d) ("Agencies, which within the limits of their authorities, fail to require that systems of records on individuals operated on their behalf under contracts be operated in conformance with the Act may be civilly liable to individuals injured as a consequence of any subsequent failure to maintain records in conformance with the Act."). Allowing 50 states to pile on and impose liability on contractors, with the financial consequences falling back on federal agencies in contract negotiations as the *Boyle* Court foresaw, might be found to upset the balance intended by Congress.

KeyPoint, however, has not argued for preemption—only for sovereign immunity. So, while it may press these arguments at future stages of litigation, we need not resolve the issue now.

* * *

This brings me to a final issue—the propriety of five plaintiffs proceeding under pseudonyms. Although some of our sister circuits take the view that a court of appeals has no jurisdiction over plaintiffs who "fail[] to request permission from the district court before proceeding anonymously," *W.N.J. v. Yocom*, 257 F.3d 1171, 1172 (10th Cir. 2001); accord, e.g., *United States ex rel. Little v. Triumph Gear Systems, Inc.*, 870 F.3d 1242, 1249–50 (10th Cir. 2017); *Citizens for a Strong Ohio v. Marsh*, 123 F. App'x 630, 636–37 (6th Cir. 2005); *Nat'l Commodity & Barter Ass'n v. Gibbs*, 886 F.2d 1240, 1245 (10th Cir. 1989) (per curiam), that doctrine, if adopted by us (which it has not been), would not change our handling of this appeal's merits—given the presence of other, non-pseudonymous plaintiffs. Moreover, the five anonymous plaintiffs in this case, see Arnold Plaintiffs' Compl. ¶¶ 22–26, J.A. 44–48, offer reasons that seem highly likely to prove worthy of district court permission—once they request it. But because pseudonymous filing impinges on values key to fair adjudication and a free society, it is hard to see how the district court on remand can avoid the issue once it has been noticed.

Although pseudonymous plaintiffs were once a rarity, there appears now to be a trend permitting adult plaintiffs to litigate incognito, with little more than pro-forma gatekeeping, if any, by the district courts—even though the practice is aberrant from the perspective of core constitutional and rule of law norms, not to mention the federal rules of procedure.

Under the "customary and constitutionally-embedded presumption of openness" that inheres in the nature of an Anglo-American trial, those who invoke the state's coercive apparatus must do so openly, i.e., under "their real names." *United States v. Microsoft Corp.*, 56 F.3d 1448, 1464 (D.C. Cir. 1995) (citations omitted); accord, e.g., *Doe v. Blue Cross & Blue Shield United*, 112 F.3d 869, 872 (7th Cir. 1997) (Posner,

J.) ("The people have a right to know who is using their courts."). For good reason. Public openness may "cause all trial participants to perform their duties more conscientiously," "induce unknown witnesses to come forward with relevant testimony," *Gannett Co. v. DePasquale*, 443 U.S. 368, 383 (1979), and generally foster "an appearance of fairness, thereby heightening respect for the judicial process," *Globe Newspaper Co. v. Superior Court for Norfolk Cnty.*, 457 U.S. 596, 606 (1982), cf. *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 569–73 (1980) (explaining importance of openness in criminal trial context). Of course, it's less important that respect for the judicial process be "heighten[ed]" than that it be *deserved*, which is less likely if plaintiffs can routinely act anonymously. In short, public scrutiny is essential to "the integrity of judicial proceedings." *Metlife, Inc. v. Fin. Stability Oversight Council*, 865 F.3d 661, 665 (D.C. Cir. 2017) (quoting *United States v. Hubbard*, 650 F.2d 293, 315 (D.C. Cir. 1980)).

Indeed, it is a matter of "[b]asic fairness." *Microsoft*, 56 F.3d at 1463 (quoting *Southern Methodist Univ. Ass'n of Women Law Students v. Wynne & Jaffe*, 599 F.2d 707, 713 (5th Cir. 1979)). A case brought anonymously can let a winning plaintiff inflict "disgrace" on a defendant and can let a losing plaintiff launch defamatory charges "without shame or liability," *Doe v. Smith*, 429 F.3d 706, 710 (7th Cir. 2005); see also *Wynne*, 599 F.2d at 713; even in situations less drastic than *Doe v. Smith*, allowance of anonymity creates a structural asymmetry that can tilt the scales unfairly. If defendants get named, plaintiffs should too.

The principle of openness is far from an "arcane relic of ancient English law." *Hubbard*, 650 F.2d at 315 n.79 (citation omitted). Rule 10(a) of the civil rules says straightforwardly that the "title of [a] complaint *must* name *all* the parties." Fed.

R. Civ. P. 10(a) (emphases added). Perhaps "name" might be taken to mean something like "real or fictitious name." Cf. Carol M. Rice, *Meet John Doe: It Is Time for Federal Civil Procedure to Recognize John Doe Parties*, 57 U. Pitt. L. Rev. 883, 914–15 (1996) (denying that Rule 10(a) bars anonymous filings). This reading is questionable, not least because it appears to prove too much—it would mean that plaintiffs may proceed anonymously *as of right*, obviating a need for judicial approval or balancing, as discussed below. And Rule 10(a) contains no exception "for good cause," which features in many other contexts. See, e.g., Fed. R. Civ. P. 5(d)(3)(A), 6(c)(1)(C), 16(b)(4), 31(a)(5), 43(a); see also *Triumph Gear*, 870 F.3d at 1249 (stating that the federal rules "make no provision for suits by persons using fictitious names or for anonymous plaintiffs" (quoting *Commodity & Barter Ass'n*, 886 F.2d at 1245)); cf. *McKeever v. Barr*, 920 F.3d 842, 845 (D.C. Cir. 2019) (holding that when a rule of criminal procedure says "must," and provides no "residual exception," as the rules do elsewhere, the district court has no inherent power to create its own "exceptions").

Following our sister circuits, we've said in dictum that—even though anonymous filing is "an extraordinary break with precedent," *Microsoft*, 56 F.3d at 1464—a district court has discretion to "grant the 'rare dispensation' of anonymity against the world," *id*. (quoting *James v. Jacobson*, 6 F.3d 233, 238 (4th Cir. 1993)); cf. *Doe v. Frank*, 951 F.2d 320, 323 (11th Cir. 1992) ("It is the exceptional case in which a plaintiff may proceed under a fictitious name."). But, we explained, this "rare dispensation" can be granted only after the district court has conducted an inquiry into whether the circumstances justify an "extraordinary break" with the normal method of proceeding—openly—in federal court. *Microsoft*, 56 F.3d at 1464.

Anonymity for "rare" or "extraordinary" cases doesn't appear to be an apt description of current practice. Cf., e.g., *Coe v. Cnty. of Cook*, 162 F.3d 491, 498 (7th Cir. 1998) (Posner, J.) (criticizing the "overuse of pseudonyms in federal litigation"). Consider that in the twenty-five-year period between 1945 and 1969, only a single district court decision—anywhere in the country—featured a "John Doe"-like plaintiff as the lead or sole plaintiff (along with a single Supreme Court case reviewing a state court decision and three appellate rulings in administrative appeals). Adam A. Milani, *Doe v. Roe: An Argument for Defendant Anonymity When a Pseudonymous Plaintiffs Alleges a Stigmatizing Intentional Tort*, 41 Wayne L. Rev. 1659, 1660 (1995); see also Joan Steinman, *Public Trial, Pseudonymous Parties*, 37 Hastings L.J. 1, 1 n.2 (1985). And in the fifty years since that time, we have never "expressly condoned [the] practice." *Qualls v. Rumsfeld*, 228 F.R.D. 8, 9 (D.D.C. 2005). Yet there are now "two different but analogous tests . . . applied in this circuit" to rule on anonymity requests, *John Doe Co. v. Consumer Fin. Prot. Bureau*, 321 F.R.D. 31, 33 (D.D.C. 2017)—a six-factor test drawn from *United States v. Hubbard*, 650 F.2d 293, 317–21 (D.C. Cir. 1980), and a five-factor test elaborated in *National Association of Waterfront Employers v. Chao*, 587 F. Supp. 2d 90, 99 (D.D.C. 2008). Just last year, in this district alone, at least six published district court decisions featured "John Doe" as the lead or sole plaintiff.[1] That is to say nothing of the twenty or so other orders that permitted Doe and the like to (anonymously) level

[1] See *Doe 2 v. Trump*, 315 F. Supp. 3d 474 (D.D.C. 2018), *rev'd on other grounds sub nom. Doe 2 v. Shanahan*, 755 F. App'x 19 (D.C. Cir. 2019); *Doe 1 v. Buratai*, 318 F. Supp. 3d 218 (D.D.C. 2018); *Doe v. George Washington Univ.*, 305 F. Supp. 3d 126 (D.D.C. 2018); *Doe 1 v. FCC*, 302 F. Supp. 3d 160 (D.D.C. 2018); *Doe v. Mattis*, 288 F. Supp. 3d 195 (D.D.C. 2018); *Does 1–144 v. Chiquita Brands Int'l, Inc.*, 285 F. Supp. 3d 228 (D.D.C. 2018).

accusations against others; many of those orders were sealed[2] or lacked any reasoning at all (thereby omitting the "inquiry" required by *Microsoft*).[3] But cf., e.g., *EEOC v. Nat'l Children's Center, Inc.*, 98 F.3d 1406, 1410 (D.C. Cir. 1996) ("[I]t is imperative that a district court articulate its reasons for electing to seal or not to seal a record.").

Proceedings in this case appear to have gone yet further down the slope of anonymity. Here, five "Does" not only filed anonymously; they evidently never even bothered to *ask* the district court for permission to do so. The "docket sheet does not reflect any motion or proceeding dealing with whether" John Does I–III or Jane Does I–II "could proceed under pseudonyms." *Marsh*, 123 F. App'x at 636–37. In their amended Complaint the anonymous plaintiffs simply *announce*, in present participle form, that (for example) John Doe II "is using" a pseudonym "because of his personal safety concerns," as if such a cursory and conclusory statement suffices as belated justification in lieu of a court's permission. Arnold Plaintiffs' Compl. ¶ 25, J.A. 46. That simply cannot

---

[2] See *Zelda v. Sessions*, No. 1:18-cv-1966 (D.D.C. Aug. 22, 2018), ECF No. 2; *Voe v. Mattis*, No. 1:18-cv-1251 (D.D.C. June 6, 2018), ECF Nos. 8–9; *Kurd v. Repub. of Turkey*, No. 1:18-cv-1117 (D.D.C. May 11, 2018), ECF No. 4; *Doe A-1 v. Democratic People's Repub. of Korea*, No. 1:18-cv252 (D.D.C. Feb. 1, 2018), ECF No. 3.

[3] See *Garcia Ramirez v. ICE*, No. 1:18-cv-508 (D.D.C. Aug, 30, 2018) (minute order); *Dora v. Sessions*, No. 1:18-cv-1938 (D.D.C. Aug. 17, 2018), ECF No. 2; *Usoyan v. Repub. of Turkey*, No. 1:18-cv-1141 (D.D.C. May 15, 2018), ECF No. 5; *Damus v. Nielsen*, No. 1:18-cv-578 (D.D.C. Mar. 15, 2018), ECF No. 2; *Doe v. Kettler Mgmt., Inc.*, No. 1:18-cv-585 (D.D.C. Mar. 15, 2018), ECF No. 3; *Doe v. George Washington Univ.*, No. 1:18-cv-553 (D.D.C. Mar. 8, 2018), ECF No. 2; *Doe v. Kipp DC Supporting Corp.*, No. 1:18-cv-260 (D.D.C. Feb. 2, 2018), ECF No. 2; *Doe v. Syrian Arab Repub.*, No. 1:18-cv-66 (D.D.C. Jan. 11, 2018), ECF No. 2.

square with the federal rules or our longstanding commitment to openness, much less the rule referred to earlier of treating failure to *request* permission as fatal to jurisdiction over such parties.

On remand, then, the district court should consider the substantive and procedural questions relating to the Does' status in the lawsuit.