PRIORITIZING PRIVACY IN THE COURTS AND BEYOND

Babette Boliek†

Big data has affected American life and business in a variety of ways—inspiring both technological development and industrial change. The legal protections for a person's right to his or her own personal information, however, have not matched the growth in the collection and aggregation of data. These legal shortcomings are exacerbated when third party privacy interests are at stake in litigation. Judicial orders to compel sensitive data are expressly permitted even under the few privacy statutes that may limit data transfers. Historically, the Federal Rules of Civil Procedure favor generous disclosure of information. But as litigation becomes more technical and data collection and transfer costs are decreasing, this Article argues that the judiciary must take an invigorated role in discovery—in particular when third-party privacy interests are at stake.

First, this Article explores the existing legal support for informational privacy rights in constitutions, statutes, and tort. As explained, the legal protections that exist are slim. This Article employs a novel theoretical model to illustrate that the current law is particularly ill-suited to protect third-party privacy rights in discovery because the law does not penalize parties for acquiescence to overreaching discovery requests. Therefore, with the current legal backdrop, to protect informational privacy rights, the judge's role as the discovery gatekeeper is imperative. To emphasize the need for a privacy-sensitive judiciary, the Article examines an ongoing litigation, Morgan Hill Concerned Parents Ass'n v. California Dep't of

† Associate Professor of Law at Pepperdine University School of Law, J.D. Columbia University School of Law, Ph.D. Economics University of California, Davis. The author would like to thank the participants of the April 2016 Judicial Conference of the Federal District Court for the Central District of California for their support and encouragement of the core principles presented here. The author also thanks AEI for posting my commentary on the *Morgan Hill* case that sparked my interest in privacy and cybersecurity issues in litigation, the Silicon Flatirons INTX Conference participants, and the Antonin Scalia Law School faculty workshop attendees for their helpful comments. Thanks also to Professors Thomas W. Hazlett, Victoria Schwartz, Naomi Goodno, and Adam Candeub for their contributions in the development of these processes. And finally, the author thanks her research assistant Scott Morrison, without whose invaluable research, expert editing and critical feedback this project would not have been possible.

Education, *where the otherwise FERPA-protected school records of an estimated ten million students were ordered to be disclosed—including addresses, social security numbers, birthdates, disciplinary records, and test scores.*

This Article proposes a three-step framework to protect the privacy interest of litigants and affected third parties. The time is ripe for renewed judicial focus on privacy interests in the courts, and a recent amendment to the Federal Rules was made precisely to encourage litigants and the courts to limit the size and scope of civil discovery. In addition to discovery reforms, this Article proposes changes to the law to incentivize collectors of data to either decrease collection of sensitive data or increase investment in privacy protections.

INTRODUCTION

In this era of big data, how should a judge prudently measure the burdens of the parties—including privacy and cybersecurity concerns—yet permit discovery as a legitimate case may demand? It is a simple question of remarkable import. In the process of civil discovery, litigants request the release of incredibly sensitive, protected information possessed by others. The judiciary is given the unique authority to either grant or deny these requests using a recently enacted statutory test: is the request "proportional to the needs of the case"?[1] That procedural declaration demands a balancing of competing needs including a person's need to protect private information (the privacy interest)[2] against the plaintiff's need for disclosure of that information.

To protect a person's privacy interest, a balance is exactly what is needed. On the one extreme is complete exposure, with no privacy interest protection, and on the other extreme is zero exposure and complete privacy. The tension between these two absolutes is explained well by Justice Brandeis, an influential leader in the United States' privacy right discussions. Brandeis noted the need for personal privacy as follows:

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and

---

1 FED. R. CIV. P. 26(b)(1).

2 For ease of discussion, this Article refers to the "informational privacy interest" as the "privacy interest" or "privacy." Although technically the term "informational privacy interest" has been invoked in relation to government collected data, this Article assumes that an informational privacy interest may arise when sensitive, personal data is in the hands of another—whether that "other" is a private (non-governmental) or public entity. The distinction between private and public collection of personal data is reflected in the discussion where appropriate.

> privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[3]

On the other hand, Brandeis also praised the beneficial impact of information disclosure on the democratic process: "Sunlight is said to be the best of disinfectants; electric light the most efficient policeman."[4] Both protecting privacy and disclosing certain information are clearly opposite but valuable actions—the socially ideal mix involves a balance of the two. Like any balancing test, the legal and social emphasis can swing from one extreme to the other. This Article squarely sets forth that the current legal framework—constitutional, statutory, and tort protections for privacy—overly favors disclosure. Further, this Article argues that the undervaluation of the privacy interest (unnecessarily) increases cybersecurity risks. Finally, this Article shows that even if the undergirding legal framework for privacy protection is strengthened, judges will still be granted the special right to override constitutional, statutory, and tort law privacy protections when they order disclosure of information by judicial order. Because of this unique gatekeeper role, this Article specifically addresses the privacy and cybersecurity issues that judges should consider when they compel discovery.

Part of why the privacy interest is legally undervalued is that modern technological realities have outstripped the privacy protections that were largely drafted to protect paper records held in file cabinets. Information is quantitatively different in today's age. Little traces of information in the wrong hands can aggregate to unravel and destroy trade secrets, private reputations, and more. That said, the United States' legal framework for protecting the privacy interest has yet to fully recognize the challenges that advancing technologies bring. Unlike other countries that not only recognize but actively protect the privacy interest of their citizens,[5] the United States has

---

3 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

4 Louis D. Brandeis, *Louis D. Brandeis Quotes*, BRANDEIS U., http://www.brandeis.edu/legacyfund/bio.html [https://perma.cc/AA6T-LP3V] (last visited Mar. 2, 2017) (originally stated in Louis D. Brandeis, *What Publicity Can Do*, HARPER'S WKLY. Dec. 20, 1913, at 10).

5 *See, e.g.*, *Factsheet on the "Right to be Forgotten" Ruling* (C-131/12), EUR. COMM'N, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf [https://perma.cc/K63T-K86N] (last visited Aug. 7, 2016) (explaining the Court of Justice for the European Union's recognition of the right to be forgotten in certain circumstances); *see also* Alex Hern, *Google Takes*

been content to take a rather laissez-faire approach to the privacy interest.[6] There is evidence, however, that American citizens have a growing concern about who has access to their data and for what purpose.[7] In a related but distinct concern, the American public's desire for increased cybersecurity of private data has risen as reports of hacking and data breaches surge.[8]

As this Article sets forth, legal privacy protections in the United States are few.[9] There are no constitutional privacy rights to one's own data, for example. Nor are there currently many statutory protections for information providers whose personal data may become caught up in a litigation to which they are not a direct party. Even tort law, which can incentivize protecting private data of third parties by imposing data disclosure liability, currently delivers very limited satisfaction to information providers. But even if all these constitutional, statutory, and tort law regimes were strengthened to protect third party privacy interests, the judiciary would still stand alone as an essential, irreplaceable protector of the privacy interest. Only the judiciary plays the solemn role of gatekeeper to discovery requests and is therefore the ultimate guardian of this country's corporate, governmental, and individual private information.[10]

Right to Be Forgotten Battle to France's Highest Court, GUARDIAN (May 19, 2016, 8:20 PM) https://www.theguardian.com/technology/2016/may/19/google-right-to-be-forgotten-fight-france-highest-court [https://perma.cc/Z778-7MR9] (describing Google's appeal of France's recognition of the right to be forgotten).

6 *See* Steven C. Bennett, *The "Right to Be Forgotten": Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L L. 161, 166–67 n.20 (2012).

7 *See* Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security, and Surveillance*, PEW RES. CTR.: INTERNET & TECH., (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ [https://perma.cc/8SHY-643Y] (describing surveys indicating that 93% of adults state that being in control of who can get information about them is either "very important" or "somewhat important").

8 *See* Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, WASH. POST (Jul. 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.cc75c149c6bf [http://perma.cc/G8V4-X7XA] (describing alarm following security breaches of U.S. government databases holding personnel records and security-clearance files of over 22 million people).

9 *See* discussion *infra* Part I.

10 *See* 20 U.S.C. § 1232g(b)(2)(B) (2018) (permitting release of otherwise protected education records pursuant to a judicial order); 26 U.S.C. § 6103(e)(5)(C), (2018) (allowing disclosure of otherwise protected tax records by judicial order); 45 C.F.R. § 164.512(f)(1)(ii)(A) (2016) (permitting release of otherwise protected health records pursuant to a judicial order); Graham H. Todd, *Protecting Privileged Communications in the Age of the New DOD Notice and Consent Banner*, 36

There are few government institutions that can match the judiciary for comprehensive power over personal data held by both private and public entities. As a starting point, an individual's constitutional right to his or her own information is dubious at best. Without such a right, in the absence of statutory or common law rights to privacy, it is difficult to argue for the legal protection of privacy once private information is given to any entity.[11] The lack of protection might even include information taken by coercion—for example, information a public school district requires for admission. While limited, certain statutory privacy protections do exist, such as the Federal Educational Rights and Privacy Act[12] (FERPA), the Health Insurance Portability and Accountability Act[13] (HIPAA), and sections of the Internal Revenue Code,[14] which protect federal tax records from disclosure. Common to all these statutes, however, is an exception for the release of information by judicial order.[15]

The judicial exemption is necessary to permit evidence of legal wrongdoing to come to light. Perhaps the public assumes that the judiciary will limit the scope of discovery to protect privacy and will not permit disclosure of data that is unnecessary to the case. But in making decisions on the scope of discovery, the judiciary may rely heavily on the discovery agreements reached among private litigants, perhaps merely rubber stamping the agreed-upon data and procedures to be turned over.[16] This means, for example, if a public school is

---

REPORTER 18, 21 n.9 (2009) (suggesting a change to Department of Defense investigations of employee computers to allow for investigation but to prevent disclosure of information except by judicial order); Steven C. Henricks, *A Fourth Amendment Privacy Analysis of the Department of Defense's DNA Repository for the Identification of Human Remains: The Law of Fingerprints Can Show Us the Way*, 181 MIL. L. REV. 69, 69 (2004) (describing how the Department of Defense releases DNA information collected from service members by judicial order).

11 For example, with respect to the Fourth Amendment, an individual does not have a "reasonable expectation of privacy" in certain information that is voluntarily disclosed to a third party. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

12 *See* 20 U.S.C. § 1232g (2018).

13 *See* 45 C.F.R. §§ 160, 162 (2016).

14 *See* 26 U.S.C. § 6103 (2016) (keeping tax return records confidential unless an exception applies).

15 *See* 20 U.S.C. § 1232g(b)(2)(B) (2018) (withholding funds from a public school that discloses student records without written consent from the parent or a judicial order or lawfully issued subpoena); 45 C.F.R. § 164.512(f)(1)(ii)(A) (2016) (allowing the disclosure of medical records for law enforcement purposes if a judicial order so requires); *see also supra* note 9.

16 *See* Chief Justice John G. Roberts, Jr., *2015 Year-End Report on the Federal Judiciary*, SUP. CT. U.S., https://www.supremecourt.gov/publicinfo/year-end/2015year-endreport.pdf [https://perma.cc/J5ZB-A7TZ] (last visited July 17,

sued, and the school agrees to give the plaintiff private information about a child (e.g. social security number, date of birth, disciplinary actions, test scores, etc.) it is possible that a judge will agree and compel the discovery.[17] There are certainly times when sensitive information is *not* essential to a case, and a defendant (like the school in this example) may simply agree to release information because it is easier or cheaper to hand over the data than to litigate the issue or redact the data. This is particularly true when the information at issue is about a third party, not about the information recipient (holder) itself. In economic terms, this is an example of misaligned interests. In other words, the defendant (the recipient of the information) may bear little cost by disclosing information to the plaintiff—costs of disclosure will be largely borne by the third party (the information provider). But, in contrast, the defendant may bear high costs if he or she fights against such disclosure. Unless the defendant internalizes the consequences the disclosure has on the information provider (e.g. public embarrassment, identity theft, loss of employment due to the exposure of the personal information, etc.) a private discovery agreement between the plaintiff and that defendant will never protect the third-party privacy interests.[18]

Add to this scenario the risk of cybersecurity breaches in the transfer, storage, and disposal of sensitive data, and the risks associated with an ill-conceived judicial order explode.[19]

2016) (encouraging the judiciary to take a more active role in managing the scope of discovery rather than letting the litigants dictate the scope of discovery and pace of the litigation). *See also* FED. R. CIV. P. 26 advisory committee's note to 2015 amendment (justifying the amendment by recycling reasoning for the 1985 and 1995 amendments: courts are not involved enough in managing the scope of discovery).

17 It should be noted that the judge ordering disclosure may be the district judge or a magistrate judge with delegated authority from the district judge to handle pre-trial discovery matters. FED. R. CRIM. P. 59 (providing that district judges have broad authority to delegate duties to magistrate judges). A district judge may review—on motion or sua sponte—a magistrate judge's order and must set aside an order that is "contrary to law or clearly erroneous." *Id.* Accordingly, the framework proposed in this Article applies to magistrate judges and district judges alike.

18 Arguably a third party could intervene to protect their privacy interests. However, the legal cost to such individuals is high, the ability to join in a class action with others to intervene is limited, and notice that personal information is even vulnerable is often scant or after-the-fact.

19 The Department of Justice reported that 17.6 million Americans were victims of identity theft in 2014, with losses totaling approximately $15.4 billion. *See* Erika Harrell, *Victims of Identity Theft, 2014*, NCJ 248991, U.S. DEP'T OF JUST. (Sept. 2015), http://www.bjs.gov/content/pub/pdf/vit14.pdf [https://perma.cc/TTU9-UUA4]. However, identity theft can have a persistent effect that is especially difficult to quantify. It can take months or years to fix the damage an

In particular, private litigants may have little incentive to incur security costs to protect third-party information. Indeed, the only immediate liability litigating parties may face related to a data breach covered by judicial order is the cost associated with notifying affected individuals and entities that the breach occurred.[20]

Many people, including judges, may be unconcerned at first with the potential of privacy loss by judicial order. This may be in large part because privacy awareness and concern varies among ordinary citizens,[21] perhaps because individuals discount the likelihood, or the consequences, of their own privacy being put in jeopardy. But what if the threat of a massive privacy invasion of millions was not in some hypothetical future? What if the disclosure of incredibly sensitive data such as names, social security numbers, birthdates, addresses, mental health records, medication lists, disciplinary records and more was not a threat, but the very real result of a judicial order?[22] And what if the data to be released were the data of children?[23]

The scenario is almost too surreal to comprehend but is exactly the reality faced by parents and guardians of children who attended any California public school at any time since January 1, 2008.[24] A federal judge issued a judicial order for

---

identity thief may cause to one's credit score, which can significantly impair one's ability to get a credit card, buy a car or house, or get approved for student loans. *See* Rod J. Rosenstein & Tamera Fine, *Identity Theft: Coordination Can Defeat the Modern-Day "King" and "Duke"*, OFFS. OF THE U.S. ATT'YS https://web.archive.org/web/20150619222016/https://www.justice.gov/usao/priority-areas/financial-fraud/identity-theft [https://perma.cc/68V2-T2CM] (last updated Dec. 8, 2014); *see also* Kimberly Rotter, *The Staggering Costs of Identity Theft in the U.S.*, CREDIT SESAME https://www.creditsesame.com/blog/credit/staggering-costs-of-identity-theft-2/ [https://perma.cc/ZE9H-L9R8] (last updated Jan. 3, 2018). Finally, that damage may go undetected for years, especially when the identity stolen is that of a juvenile who will not apply for a credit card or loan until the child reaches majority.

20 *See, e.g.*, Morgan Hill Concerned Parents Ass'n v. Cal. Dep't of Educ., No. 2:11-CV-03471-KJM-AC, 2016 WL 304564, at *7 (E.D. Cal. Jan. 26, 2016) (ordering the defendant to be responsible for all costs associated with posting the Notice and Objection Form pursuant to FERPA).

21 *See* Tim Cook, *A Message To Our Customers*, APPLE INC. (Feb. 16, 2016), http://www.apple.com/customer-letter/ [https://perma.cc/SA7Z-TTXX]. *See also*, Victoria Schwartz, *Corporate Privacy Failures Start at the Top*, 58 B.C. L. REV. 1693, 1697 (2016) (discussing why executives of companies who are not themselves privacy-aware jeopardize the information of others).

22 *See* discussion *infra* Part V.

23 *See id.*

24 *See* Notice of Disclosure of Student Records, Morgan Hill Concerned Parents Ass'n v. Cal. Dep't of Educ., No. 2:11-CV-03471 (E.D.Cal. Mar. 29, 2013), 2013 WL 1326301.

the California Department of Education to gather, consolidate, and disclose to plaintiffs the complete student records of all California public school children[25]—an estimated ten million student records between 2008 and 2015 alone.[26] The records are to be disclosed in connection with the legal action *Morgan Hill Concerned Parents Ass'n v. California Dep't of Educ.*[27] The case is sympathetic to be sure—a parent organization in the southern tip of Silicon Valley is concerned that some special-needs children are not being appropriately accommodated by the school district.[28] The plaintiffs hope that student data collected throughout the state will prove their case.[29] But the case, described at greater length in Part V, is an example of a failure to protect the privacy and cybersecurity interests of third parties—school-aged children and their parents and guardians.

Consider the following two questions set in the *Morgan Hill* example. First, why should private plaintiffs (parents in a local school district) have access to highly private identifying information of any other students, let alone access to the information of all the public school children across the state of California?[30] Second, after private plaintiffs run their analyses (whatever those searches may be) how are the results to be stored and transferred?

The first question is a privacy concern, and the second is primarily a cybersecurity concern. As argued here, a judge

---

25 *Id.*

26 *See Enrollment by Grade for 2014–15: Statewide Enrollment by Ethnicity and Grade*, CAL. DEP'T OF EDUC.: EDUC.DEMOGRAPHICS UNIT, http://dq.cde.ca.gov/dataquest/Enrollment/GradeEnr.aspx?cChoice=StEnrGrd&cYear=2014-15&cLevel=State&cTopic=Enrollment&myTimeFrame=S&cTypeALL&cGender=B [https://perma.cc/6D59-NKY9] (last visited Mar. 23, 2016). *See also Enrollment, Graduates and Dropouts in California Public Schools, 1974–75 Through 2013–14*, CAL. DEP'T OF EDUC.: EDUC. DEMOGRAPHICS UNIT, http://dq.cde.ca.gov/dataquest/EnrGradDrop.asp [https://perma.cc/QU8Q-WF8K] (last visited March. 23, 2016). Looking at the data, approximately 6,235,000 students in grades K–12 were enrolled in California public schools in the 2014–15 academic year. Then, approximately 2,837,000 students graduated from California public schools between 2008 and 2014. That results in nearly 9.1 million students but does not account for dropouts and students that transfer out of the California public school system.

27 Morgan Hill Concerned Parents Ass'n v. Cal. Dep't of Educ., No. 2:11-CV-03471-KJM-AC, 2013 WL 1326301 (E.D. Cal. Mar. 29, 2013).

28 *Id.* at *1.

29 *Id.* at *2.

30 *See e.g.*, Letter from Patrick A. Chabot, Superintendent, Sonora Union High School District, to Kimberly J. Mueller, *Morgan Hill*, No. 2:11-CV-03471-KJM-AC (E.D. Cal. Apr. 11. 2016), ECF No. 173-1 (criticizing the disclosure of student records).

must be concerned with both. In *Morgan Hill*, for example, a Special Master was appointed to facilitate the technical discovery requests that this case requires.[31] This common practice is helpful, but understandably the special master is primarily focused on the cybersecurity concern. However, that judicially delegated authority does nothing to limit data exposure in the first instance. Indeed, the court may be the only actor that can protect the privacy interests of third parties by weighing the privacy burden, limiting discovery, and ordering redactions.

This Article presents a set of common sense principles for judges and practitioners to properly frame the privacy and cybersecurity issues that judges should consider when issuing a discovery order. Part I of this Article sets forth the current legal framework for a legal person's informational privacy rights: individuals have no clear constitutional right to informational privacy, statutes provide a few protections for private information (with many exceptions), and the tort regime severely limits an individual's ability to sue and recover for the wrongful disclosure of his or her private information.

Part II of this Article sets forth the historical judicial treatment of the privacy interest. This Part also discusses the recent changes to the Federal Rules of Civil Procedure that unmistakably envision greater judicial involvement in limiting the scope of discovery orders—a rule change that can be embraced by practitioners and judges alike to consider and protect the privacy interests of the parties and third parties. Part III sets out how judicial discovery orders may also include a cybersecurity calculation.

Part IV sets forth a simple three-part framework to help the judiciary balance affected parties' privacy interests and cybersecurity concerns against the need for trial discovery. As described fully in Part IV, this Article recommends that the court should protect privacy and determine how much weight to place on the privacy interest at risk by evaluating a proposed set of factors. If the privacy concerns are demonstrably high, as established by the privacy screen suggested in this Article, the judge may wish to consider appointing a special "privacy master" to monitor the privacy issues during discovery. Second, the court must limit the data exposed in light of that weighted privacy interest and protect the disclosed data by ordering redactions and data aggregation. Third, the court must promote cybersecurity to keep the data from being dis-

---

31 *See* Order, *Morgan Hill*, No. 2:11-CV-03471-KJM-AC (Jul. 2, 2015), ECF No. 116 (appointing a special master to the case).

seminated further. Part V describes in-depth the ongoing cautionary tale that catalyzed this discussion: *Morgan Hill Concerned Parents Ass'n v. California Dep't of Educ.*

Finally, Part VI suggests additional contexts in which the recommendations for judicial orders set forth here would be beneficial. For example, to protect the privacy interest, privacy statutes and government agencies, as well as the courts, should emphasize limits on data collection rather than merely repeat historic reliance on post data collection security and post disclosure liabilities. In particular, this Article argues that the need for data gathering limits by government entities is acute in the age of big data. Accordingly, this Article suggests a new cause of action, a type of Pigovian tax, to incent public entities to limit data collection and protect data retention.

I
THE LEGAL FRAMEWORK TO PROTECT THE PRIVACY INTEREST

As a general matter, it is difficult to define what exactly a legal person's privacy interest is, although extensive literature has attempted to do so.[32] It is especially difficult to define because each individual, each company, and even each country may define their own privacy interest in a different way.[33] In one home, for example, there may be an attorney with an incredibly high valuation of personal privacy living with a teenage son who has little to no such regard for his personal privacy. However, one thing is common to all: once personal information is disclosed, that privacy is gone forever.[34] Therefore, the following discussion focuses on legal protections for the informational privacy interest, however that interest may be defined.

Broadly speaking, the legal framework for privacy interest protection relies heavily on data disclosure liability and data

---

32 *See, e.g.*, Victoria Schwartz, *Disclosing Corporate Disclosure Policies*, 40 FLA. ST. U. L. REV. 487, 497–505 and accompanying footnotes (discussing "privacy interests as a potential cost of a disclosure policy, or something to be considered as a competing consideration against the disclosure interest").

33 *See, e.g.*, *Factsheet on the "Right to be Forgotten" Ruling*, (C-131/12), EUR. COMM'N, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf [https://perma.cc/K63T-K86N] (last visited Aug. 7, 2016) (explaining a Court of Justice of the European Union ruling on data privacy).

34 *See* William G. Childs, *When the Bell Can't Be Unrung: Document Leaks and Protective Orders in Mass Tort Litigation*, 27 REV. LITIG. 565, 579 (2008) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1971794 [https://perma.cc/53HB-E6MM].

collection security measures (the analog version to cybersecurity). These regimes were developed largely before the existence of the Internet and are showing their age. As will be discussed below, the added value of heightened privacy interest legal protections[35]—whether by constitutional, statutory, or tort regimes—are the incentives such protections create for entities to limit data collection in the first instance and to invest in post-collection data protection systems, thereby creating a self-disciplining privacy protection market.[36] Yet, this may not be the case in all instances, especially if a government entity is the information collector.[37] Due to the unique coercive nature of government requests for data, and the unique risks associated with government-held data, government entities are particularly likely to overcollect data and underinvest in data protection.[38]

A. Constitutional Protection for Informational Privacy Rights

The Supreme Court has not directly addressed whether a legal person has a right of informational privacy. Informational privacy is not the same as decisional privacy, which the Supreme Court deemed a fundamental right over fifty years ago in *Griswold v. Connecticut*.[39] Decisional privacy is the fundamental right of individuals to exercise "independence in making

---

35 There are also strong reputational effects that can incent investment in privacy-protection regimes. *See infra* subpart I.C.

36 Vice president of global cybersecurity at CGI Group, John Proctor, said "If you can't protect it, don't collect it." Christine Wong, *Customer Data: If You Can't Protect It, Don't Collect It, Says Cyber Security Expert*, IT BUS. (Feb. 25, 2016), https://www.itbusiness.ca/news/customer-data-if-you-cant-protect-it-dont-collect-it-says-cyber-security-expert/65756 [https://perma.cc/N65H-A7XR].

37 *See* Jennifer A. Brobst, *Reverse Sunshine in the Digital Wild Frontier: Protecting Individual Privacy Against Public Records Requests for Government Databases*, 42 N. KY. L. REV. 191, 195 (2015).

38 *See* Hal Scott & John Gulliver, *The SEC Plans to Collect Too Much Information*, WALL ST. J. (Oct. 2, 2017), https://www.wsj.com/articles/the-sec-plans-to-collect-too-much-information-1506983751 [https://perma.cc/GEZ2-6E89] (describing the new plan by the SEC requiring the U.S. stock exchanges and the FINRA to establish a database of "the names, birth dates, Social Security numbers and brokerage accounts of tens of millions of U.S. investors" by November 2018). The October 2017 announcement of the SEC to expand the Consolidated Audit Trail and collect more sensitive personal information of investors came only a month after the SEC announced that its EDGAR database had been hacked in 2016. *See* Dave Michaels, *SEC Discloses Edgar Corporate Filing System was Hacked in 2016*, WALL ST. J. (Sept. 20, 2017), https://www.wsj.com/articles/sec-discloses-edgar-corporate-filing-system-was-hacked-in-2016-1505956552 [https://perma.cc/XF6Y-ZJAS].

39 *See* 381 U.S. 479, 484–86 (1965).

certain kinds of important decisions."[40] In contrast, informational privacy is "the freedom from having private affairs made public by the government."[41] The Court has danced with the right of informational privacy on three separate occasions, but in each case the Court merely assumed without deciding that such a right did receive constitutional protection.[42] Furthermore, rather than applying a specified level of scrutiny to the state actions at issue in those cases, the Court applied "a balancing test to determine the scope of the right by weighing the individual interest in privacy against the government's interest . . . ."[43] As explained in more detail below, since the Court has given considerable weight in this balancing test to the "protections" provided by statute—protections that are questionable at best and vaporware at worst—the Court's balance is of little comfort to the privacy concerned. In the absence of clear Supreme Court precedent, nearly all circuits have recognized a constitutional right to informational privacy, with only the D.C. Circuit expressing skepticism that the right exists.[44] However, even the circuits that recognize the right are split on their approach to two issues: 1) the level of scrutiny to apply when the right is infringed and 2) what type of information triggers the right.

As to the level of scrutiny to apply when the right to informational privacy is infringed, most courts apply some degree of intermediate scrutiny,[45] while a minority apply strict scrutiny,[46] and at least one applies a varying level of scrutiny de-

---

40 Caleb A. Seeley, *Once More unto the Breach: The Constitutional Right to Informational Privacy and the Privacy Act*, 91 N.Y.U. L. REV. 1355, 1359 n.25 and accompanying text (2016) (internal quotation marks omitted) (quoting Whalen v. Roe, 429 U.S. 589, 599–600 (1977)).

41 *Id.* at 1360.

42 *See* NASA v. Nelson, 562 U.S. 134, 138 (2011). ("In two cases decided more than 30 years ago, this Court referred broadly to a constitutional privacy 'interest in avoiding disclosure of personal matters.' . . . We assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*." (internal citations omitted)). *See also* Whalen v. Roe, 429 U.S. 589, 599–600 (1977); Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 457 (1977).

43 Seeley, *supra* note 40, at 1360–61.

44 *Leading Cases*, 125 HARV. L. REV. 172, 237 nn.68–69 and accompanying text (2011).

45 *See In re* Crawford, 194 F.3d. 954, 959 (9th Cir. 1999) (requiring only a legitimate government interest but also requiring narrow tailoring of the regulation); Doe v. City of New York, 15 F.3d 264, 269 (2d Cir. 1994) (requiring a substantial government interest and using a balancing test to evaluate the regulation).

46 *See* Anderson v. Blake, 469 F.3d 910, 915 (10th Cir. 2006); Bloch v. Ribar, 156 F.3d 673, 686 (6th Cir. 1998).

pending on the sensitivity of the information at issue.[47] As to the type of information that triggers the right to informational privacy, some circuits only extend protection to information concerning "another constitutional right or fundamental liberty interest,"[48] and other circuits extend protection "to any information in which an individual has a reasonable expectation of privacy."[49] If courts determine that keeping personal, sensitive information private is a fundamental right, then that data may be legally well protected. If, by contrast, it is considered simply an important right, it will be less protected. In the latter case the government need only show the court that it has a "substantial state interest" in collecting or disseminating the data.[50]

Arguably, a "substantial state interest" for disclosing data has been declared in the Federal Freedom of Information Act[51] (FOIA) and its state counterparts, colloquially called "sunshine laws."[52] Sunshine laws provide citizens access to public records to ensure government transparency and good behavior.[53] However, "the stated policy of Sunshine laws [] to 'provide[] for liberal access to public records' is a double-edged sword when public records primarily contain information on private individuals rather than information on government officials."[54] In other words, the personally identifying information held in those public records is disclosed along with relevant data of government action—the personal data exposure is collateral damage to FOIA goals, and citizens cannot protect against it.

As one author puts it, "what is occurring is a Reverse Sunshine effect, in which the lives of individuals, at times, are made more transparent than government action."[55] Additionally, there is a "strong presumption in favor of disclosure,"

---

47 *See* United States v. Westinghouse Elec. Corp., 638 F.2d 570, 580–82 (3d Cir. 1980).

48 *Leading Cases*, supra note 44, at 238. *See Bloch* 156 F.3d at 683–84.

49 *Leading Cases*, supra note 44, at 238. *See* Doe v. Se. Pa. Transp. Auth., 72 F.3d 1133, 1138 (3d Cir. 1995).

50 *See* United States v. Virginia, 518 U.S. 515, 573 (1996) (Scalia, J., dissenting); Roe v. Wade, 410 U.S. 113, 155 (1973); Griswold v. Connecticut, 381 U.S. 479, 497 (1965) (Goldberg, J., concurring).

51 The Freedom of Information Act, 5 U.S.C. § 552 (2018).

52 *See* Brobst, *supra* note 37, at 196–97.

53 This is Brandeis' "sunshine as disinfectant" regime—disclosure of government activity increases transparency and accountability. *See* LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 92 (1914) ("Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the efficient policeman.").

54 Brobst, *supra* note 37, at 197–98.

55 *Id.* at 191.

which "places the burden on the agency to justify the withholding of any requested documents" or "the redaction of identifying information in a particular document[ ]."[56] To make matters worse, an individual requesting a public record does not necessarily have to justify his or her request because Sunshine laws are concerned with promoting government transparency and not with what the public does with the information.[57]

Counter to government information disclosures, the Privacy Act of 1974[58] was passed to give citizens a cause of action against the government when their information is disclosed. As discussed in the next section, the Privacy Act's efficacy has been limited by its judicial interpretation and application.

B. Statutory Protections for Informational Privacy Rights

Ironically, the judicial application of the Privacy Act of 1974 exemplifies how far the pendulum has swung away from protecting the privacy interest. This statute, like many privacy statutes, was imagined, drafted, and passed before the existence of the Internet.[59] Rather than focusing *ex ante* on minimal data collection, this statute emphasizes protecting data once it has been accumulated.[60] In turn, this statutory emphasis on post-data collection arguably has heavily influenced the privacy focus of the judiciary.[61]

The Privacy Act of 1974 is often criticized by legal scholars as resulting in the overcollection of personal data and in very limited liability for noncompliance.[62] Admittedly, the Privacy Act's purpose is noble in theory but toothless in practice due to

---

56 Dep't of State v. Ray, 502 U.S. 164, 173 (1991).

57 *See* Brobst, *supra* note 37, at 201.

58 5 U.S.C. § 552a (2018).

59 *See* Erin Corken, *The Changing Expectation of Privacy: Keeping Up with the Millennial Generation and Looking Toward the Future*, 42 N. KY. L. REV. 287, 295–303 (2015) (providing a chronological list of the most significant information and privacy-concerned statutes, their purposes, and what has changed about the world since each statute's inception).

60 *See* Wade A. Schilling, *You Want to Know What?* NASA v. Nelson *and the Constitutional Right to Informational Privacy in an Ever-Changing World*, 82 UMKC L. REV. 823, 834 (2014).

61 *See* Seeley, *supra* note 40, at 1364 (discussing that the Supreme Court heavily considered statutory protections of personal information when balancing the individual's interest in keeping information private against the government's interest in collecting the information).

62 *See e.g.*, Alex Kardon, *Damages Under the Privacy Act: Sovereign Immunity and a Call for Legislative Reform*, 34 HARV. J.L. & PUB. POL'Y 705, 767 (2011) (explaining the difficulties of recovering for so-called "nonpecuniary damages" under judicial interpretation of the term "actual damages" in the Privacy Act).

statutory exceptions and judicial interpretations that narrow the statute's applicability to claims of noncompliance.[63] The Privacy Act requires federal agencies to: 1) ask the private individual for written consent to disclose personal information; 2) allow the private individual to review and correct the information; 3) regulate and restrict the collection, use, and dissemination of information; and 4) waive sovereign immunity.[64]

However, there are a dozen exceptions to the first requirement, the broadest of which, the "routine use" exception, allows for nonconsensual disclosure if the purpose for disclosure aligns with the purpose of collection.[65] Use of this exception is claimed to have "led to the over collection of information" because agencies "fail[ ] to assess the relevance or need of such information."[66] The Supreme Court held that the Privacy Act sufficiently protected against unwarranted dissemination,[67] but, as one critic argues, that holding "ignore[s] the reality that abuse of the 'routine use' exemption is all too common."[68] In fact, it was reported that 18% of "routine use" disclosures were not even reviewed to validate the exception.[69]

But that clear noncompliance faces little consequence based on the Supreme Court's interpretation of the Privacy Act's liability provisions. The Privacy Act states that when an agency violates the Privacy Act "in a manner which was intentional or willful," the affected individual may recover for the sum of "actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of $1,000" and "the costs of the action together with reasonable attorney fees as determined by the court."[70] The Supreme Court held, however, that the $1,000 statutory minimum is only available where the plaintiff sustained actual damages totaling less than $1,000.[71] Moreover, in a later case, the Court held that emotional distress damages were not "actual damages" within the meaning of the statute and only economic damages sufficed.[72]

---

63 *Id.*

64 Schilling, *supra* note 60, at 833.

65 *See* 5 U.S.C. § 552a(b)(3) (2018).

66 Schilling, *supra* note 60, at 834.

67 *See* NASA v. Nelson, 562 U.S. 134, 136–37 (2011).

68 Schilling, *supra* note 60, at 835.

69 *Id.*

70 5 U.S.C. § 552a(g)(4) (2018).

71 Doe v. Chao, 540 U.S. 614, 616 (2004).

72 FAA v. Cooper, 566 U.S. 284, 304 (2012).

These narrow interpretations combined effectively declaw the Privacy Act by limiting the situations that result in negative consequences for noncompliance. Not only would a plaintiff have to prove that the agency's noncompliance was intentional or willful, but the plaintiff must also prove that they suffered actual, economic damages as a result of the noncompliance. As a result, there is little incentive to comply with the Privacy Act because the agencies face few to no penalties. Ultimately, this statute, designed to protect against the disclosure of personal information, instead allows for excessive disclosure, overcollection, and little enforcement.

C. Tort Regime—A Private Solution to Protecting Privacy?

As an alternative to constitutional and statutory regimes to protect privacy, one common solution is to employ a tort regime to bring about optimal solutions. The advantage is that the tort regime can create private markets to lead to optimal investments in privacy protections by incentivizing either limited collection or increased cybersecurity investments. The potential impacts of tort regimes on private and public collectors of data are different, however, and are modeled separately in the discussion below.

The need for tort liability in privacy protection rests on the assumption that the recipients of personal information do not have the same incentives to protect that information as do the providers of personal information. For example, make the plausible assumption that the California Department of Education in *Morgan Hill* is not motivated to protect student information to the degree many parents would protect it.[73] The problem is a common one—the benefits (or costs) of the decision maker are not aligned with the benefits (or costs) of all those affected by the decisions. In the privacy context, this means that the recipient of information is not as incentivized to provide privacy protections—vigorous legal defense to discovery or cybersecurity investment against hacking—as the information provider may desire. This misalignment of incentives means that the information recipient may make decisions for which it does not suffer negative consequences. The result is

---

73 Press Release, Cal. Dep't of Educ., Schools Chief Tom Torlakson Applauds Federal Court Order Strengthening Student Privacy Protections in *Morgan Hill* Case (Mar. 4, 2016), https://www.cde.ca.gov/nr/ne/yr16/yr16rel18.asp [https://perma.cc/U48Y-JWBZ] (stating that a "large number of objections to the potential release of student data" were submitted by parents to keep the CDE from disclosing it).

that the information recipient may underinvest in protection and defense of that information.

To align the incentives of the information recipient and the information provider, the economic response is to internalize the externality.[74] In this instance, the information recipient must somehow bear the negative consequences of under protection. A typical method is to impose tort liability and award monetary damages. However, the problem with tort law in this particular instance is twofold. First, a tort regime designed to protect the privacy interests of a population with highly diverse privacy concerns will inevitably overprotect some individuals and underprotect others. Second, a private tort system is limited against public (government) collectors of information. The latter point is particularly important and is discussed at greater length below. In general, due to the coercive nature of government collection of data, privacy concerns are heightened because an individual has a limited ability to self-protect his or her privacy by opting out of information mandates.

Nevertheless, the theory behind tort law is simple: if a victim suffers an injury due to the negligent behavior of the tortfeasor, then the tortfeasor must compensate the victim.[75] The compensation may include direct damages (such as medical expenses for a physical injury), consequential damages (that flow from the injury, such as lost wages) and punitive damages (meant to punish).[76] The damage calculation is intended not only to put the victim in the position he or she would have been in but for the negligence, but also to incentivize the tortfeasor and potential tortfeasors to exercise greater care in similar future situations.[77] Industry participants that may face potential liability invest in procedures to minimize tort exposure.[78] In the case of privacy it would mean that the information recipient would perhaps invest in legal and cyber defense to protect the information if the release would lead to penalty.

---

74 *See* N. GREGORY MANKIW, ESSENTIALS OF ECONOMICS 196 (8th ed. 2016) ("Instead of regulating behavior in response to an externality, the government can use market-based policies to align private incentives with social efficiency. For instance, . . . the government can internalize the externality by taxing activities that have negative externalities . . . .").

75 *See* RESTATEMENT (SECOND) OF TORTS § 901 (AM. LAW INST. 1979).

76 *See id.* at §§ 903–909.

77 *See id.* at § 901.

78 *See generally* Gary T. Schwartz, *The Ethics and the Economics of Tort Liability Insurance*, 75 CORNELL L. REV. 313, 314 (1990) (noting the increasing adoption of negligence insurance policies).

As a corollary, the tort regime may encourage the development of private insurance markets to protect the insured against potential liabilities. Not only does such a market benefit victims by providing funding in the face of loss, the secondary benefits are the salutary effects of insurance premiums, deductibles, and contractual obligations of care imposed by the private market. These costs, if properly set, may further incentivize protection investments. The development of such markets takes time. Insurance markets develop to counter known risks; the greater the uncertainty of the risks, the less likely insurance will be available at reasonable rates. Even without insurance markets, a company may decide to self-insure against uncertain tort liability.[79] This self-insurance may convey similar benefits to consumers as do private insurance markets.

The optimal insurance regime is difficult to create in any market. The first step is to set the tort liability optimally in order to inspire sufficient self-insurance and insurance market development. The second step is for the self-insurer or insurance market to translate that risk into the desired protection of the privacy interests. To illustrate, let x be an individual with high regard for the privacy interest and y be a person with low concern for the privacy interest. Let Θ represent likelihood of entry into a privacy exchanging transaction. Assume also that an increase in overall transactions is a societal "good" and that tort liability leads to insurance markets and is represented by ø.

1. *Privacy Tort Regimes—Private Sector Transactions*

Scenario 1: Voluntary Transactions without Tort Liability.

(a) Transaction bears no privacy revelation risk.

$x\,\Theta = y\,\Theta$

x and y are equally likely to enter the transaction. No tort liability is necessary and no insurance or investment is needed to increase the number of transactions.

(b) Transaction bears slight to medium privacy revelation risk.

$x\,\Theta < y\,\Theta$

---

79 *See* Mark W. Flory & Angela Lui Walsh, *Know Thy Self-Insurance (And Thy Primary and Excess Insurance)*, 36 TORT & INS. L.J. 1005, 1010 (2001).

x's enthusiasm for the transaction is less than y's enthusiasm for the transaction. x would be less likely to enter the transaction than y.

Scenario 2: Voluntary Transactions with Tort Liability

As evidenced in Scenario 1, increased investment in protections or a lower information requirement would help x enter the transaction. An increase in tort liability might incentivize such investment. However, the existence of tort liability may also discourage a transaction offering in the first instance, thus decreasing the number of transactions. The preferable societal solution is therefore ambiguous. It will depend on whether x's decision to self-protect by opting out is better for society than trying to encourage x's entry by a tort regime. There are two possible outcomes:

(a) $(x\ \Theta < y\ \Theta) < (x\ \Theta\ \emptyset = y\ \Theta)$ Tort regime maximizes transactions.

(b) $(x\ \Theta < y\ \Theta) > (x\ \Theta\ \emptyset = y\ \Theta)$ Tort regime does not maximize (may decrease) transactions.

Again, whether the intervention of a tort regime will result in greater transactions will depend on (1) how many individuals would opt out of the transaction without a tort regime in place as opposed to (2) the decrease in offered transactions because the tort regime has increased costs. In this theoretical example, it follows that a tort regime would be more effective in increasing transactions when the risks of revelation (or potential damage from revelation) are high.

Importantly, private collectors of information may have an incentive to protect collected information even in the absence of tort law. Many companies invest tremendous sums in their brand or reputation, which may be at risk if an unwanted disclosure of private information occurs.[80] If the company is susceptible to "brand risk" in the area of privacy, they may already have private insurance or privacy policies that incen-

---

80 My thanks to Professor Thomas W. Hazlett, the Hugh H. Macaulay Endowed Professor of Economics at Clemson University and Director of the Information Economy Project, for suggesting the exploration of this issue. *See* Pat Conroy, et al., *Building Consumer Trust: Protecting Personal Data in the Consumer Product Industry*, DELOITTE U. PRESS (Nov. 13, 2014), https://www2.deloitte.com/insights/us/en/topics/risk-management/consumer-data-privacy-strategies.html [https://perma.cc/T7N5-JBAG] ("The results of a recent survey of consumers and executives show that consumers have a keen sense of awareness of the risks surrounding data security and privacy, and that many consumer product executives are likely overestimating the extent to which they are meeting consumer expectations related to data privacy and security.").

tivize protections of client data.[81] Such brand risk may not apply to all collectors equally, but there is evidence that even data collectors that do not have a direct relationship with consumers may experience drops in their stock value if consumer information is not protected properly.[82] The importance of brand risk cannot be underestimated. Unlike tort law which is costly, imperfect, and necessitates articulating an actual harm—difficult in privacy invasion cases—brand risk is felt immediately in stock value loss and decreases in demand. Brand risk is also much more responsive to changes in consumer privacy preferences than is tort law, since the latter may change only with new legislation or the development of case law.

2. *Privacy Tort Regimes—Public Sector Transactions*

As a starting observation, public sector transactions are not necessarily "voluntary" in the classic, common law sense of that word. For example, even a privacy-conscious individual cannot "opt out" of filing financial information with the IRS. Given the asymmetry of bargaining power between an individual and a monopolistic (or relatively monopolistic) government entity, most individuals are captive to the privacy selection made by the government. Under a liberal framework, however, reasonable freedom depends on "the presence of alternatives, between which one may choose."[83] Therefore, while the supposed contract between the government and individuals may be voluntary in the most technical of circumstances, the problem is that there is no bargained-for exchange, and essentially no freedom to negotiate or reveal preferences by exercising alternatives.

To expand further, it may be argued that at least in some cases, individual x can opt out by simply choosing not to par-

---

81 There is evidence of considerable corporate costs related to a company's missteps on consumer privacy issues. Corporations that have experienced such costs include ChoicePoint, Google and Facebook. *See* Jessica Rich, FTC, PRIVACY TODAY AND THE FTC'S 2014 PRIVACY AGENCY 3–4 (2013) https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-today-ftcs-2014-privacy-agency/131206privacytodayjrich.pdf [https://perma.cc/D5PL-H2NK].

82 *See id.* (noting that ChoicePoint lost value in the market even though it was a third-party data seller). *See generally* Dirk Bergemann & Alessandro Bonatti, *Selling Cookies*, 7 AM. ECON. J.: MICROECONOMICS 259, 259 (2015), http://www.mit.edu/~bonatti/selling_cookies.pdf [https://perma.cc/ZL5U-3QVJ] (modeling the price of data).

83 George Kateb, *Foreword to* JUDITH N. SHKLAR, POLITICAL THOUGHT & POLITICAL THINKERS, at xvii (Stanley Hoffmann ed., U. Chi. Press, 1998); *see* Judith N. Shklar, *The Liberalism of Fear*, *reprinted in* SHKLAR, *supra*, at 3–20.

ticipate in a government benefit if it would pose an unacceptable exposure of private information. For example, x could enroll her school-aged children in a private school that protects information more vigorously than does a public school. There are of course many obvious problems with viewing such an action as "voluntary" or "socially optimal." To encourage taxpayers to forgo public benefits to protect privacy interests seems extreme. It is at a minimum highly inefficient, but also raises equity issues as such an "opt out" is generally available only to the wealthy. In short, the absence of a viable opt-out option limits the ability of privacy-conscious individuals to self-protect by declining to engage in the transaction. The result will be overparticipation in public sector transactions that carry a high risk to privacy.

Scenario 3: Involuntary Transactions without Tort Liability.

(a) Transaction bears zero privacy revelation risk.

$x\,\Theta = y\,\Theta$

(b) Transaction bears low to medium privacy revelation risk.

$x\,\Theta = y\,\Theta$

(c) Transaction bears medium to high privacy revelation risk.

$x\,\Theta = y\,\Theta$

In Scenario 3, by government mandate, x and y must enter the transaction; opting out (self-protection) is not an option. Unless privacy exposure risk is zero, that means that x is entering into a transaction that under private circumstances she would not have entered. Hence, in this Scenario 3, the number of transactions is *greater than* the privacy-protecting social optimum. The most privacy-concerned individuals are forced to engage in the transaction even when they would normally opt out or require additional protections to voluntarily opt in. This is a quintessential contract of coercion so that privacy preferences are unrevealed. The result is that government entities are not properly incentivized to gather the least amount of information necessary, nor are they incentivized to invest in privacy protection regimes or vigorously defend against discovery requests. The entire cost of privacy loss is borne by the individual information providers, even unwilling providers.

In this scenario, the presence of a tort regime will not increase transaction participation. Here, the social goal must be defined distinctly from that in the private sector (voluntary)

transaction context—the internalization of third-party interests should lead to a decrease of transactions.

Scenario 4: Involuntary Transactions with Tort Regimes

$(x \Theta = y \Theta) < (x \Theta \text{ ø} = y \Theta)$ Tort regime minimizes unnecessary transactions.

As discussed next, tort regimes in the public context are extremely complex. And there is no brand risk in the public context that in the absence of tort liability will still encourage privacy protection investment.

3. *Tort Liability for Government Entities*

The path to suing the government, whether federal or state, is littered with obstacles. The first obstacle, the doctrine of sovereign immunity, can eliminate a plaintiff's tort claims. Under the doctrine, "[t]he United States, as sovereign, is immune from suit [unless] it consents to be sued . . . ."[84] Federal sovereign immunity is derived not from the Constitution but from our English ancestry and its extensive history in English law.[85] Sovereign immunity extends to the states through the Eleventh Amendment to the United States Constitution.[86] Accordingly, in order to sue a government entity, that entity (federal or state) must waive its sovereign immunity.[87]

The federal government waived its sovereign immunity to tort claims in the Federal Tort Claims Act (FTCA).[88] However, that waiver is not absolute and is subject to many exceptions.[89] "The most sweeping of these exceptions bars claims 'based upon the exercise or performance [of] or the failure to exercise or perform a *discretionary* function or duty.'"[90] Courts nonetheless recognize that a plaintiff can sue for the wrongful dis-

84 United States v. Sherwood, 312 U.S. 584, 586 (1941).

85 *See* United States v. Lee, 106 U.S. 196, 205–06 (1882).

86 *See* U.S. CONST. amend. XI (providing that citizens of one state cannot sue another state).

87 *See Lee*, 106 U.S. at 227.

88 *See* 28 U.S.C. § 1346(b)(1) (2018).

89 *See* 28 U.S.C. § 2680 (2018); Jonathan R. Bruno, *Immunity for "Discretionary" Functions: A Proposal to Amend the Federal Tort Claims Act*, 49 HARV. J. ON LEGIS. 411, 411–12 (2012).

90 Bruno, *supra* note 89, at 412 (alteration in original) (emphasis added).

closure of private information[91] despite the broad "discretionary" exception.[92]

Although the law is clear that a private plaintiff is allowed to sue the federal government for wrongful disclosure, a potential claimant faces other legal roadblocks. In order to sue under the FTCA, the plaintiff must first exhaust administrative remedies with the appropriate agency.[93] The request for administrative relief must include: (1) a written statement of the injury and (2) a "sum-certain damages claim."[94] Then, the plaintiff can only bring a lawsuit in court if the agency denies the claim for relief or if the agency fails to respond to the claim within six months of its submission.[95]

Yet another hurdle lies on the path to a tort suit: the statute of limitations. In fact, there are two statutes of limitations relevant to a federal tort claim. First, a tort claim needs to be filed with the appropriate agency within two years of the claim's accrual.[96] Second, once an agency has formally denied a claim, the plaintiff has six months from notice of that denial to file the action in court.[97] If either of these time limitations expires, the plaintiff is forever barred from pursuing the claim.[98] With these obstacles, few plaintiffs actually have their day in court against a government agency under the FTCA.

It is worth noting that the FTCA is not the only statute that allows a private citizen to file suit against the government for negligent disclosure. As discussed in Part I, the Privacy Act of

---

91 *See, e.g.*, Johnson v. Sawyer, 47 F.3d 716, 722–24 (5th Cir. 1995) (United States sued for disclosing tax information); Boyd v. United States, 932 F. Supp. 2d 830 (S.D. Ohio 2013) (Veterans Affairs sued for disclosing medical information); Martin v. Locke, 659 F. Supp. 2d 140, 143 (D.D.C. 2009) (officers of the Secretary of Commerce sued for disclosing "private facts").

92 *See* Jerome Stevens Pharm., Inc. v. FDA, 402 F.3d 1249, 1252–53 (D.C. Cir. 2005) (explaining that the discretionary function exception only applies if the action being challenged passes a two-part test).

93 *See Martin*, 659 F. Supp. 2d at 151–52.

94 *Id.*

95 *See* McCallister v. United States, 925 F.2d 841, 843–44 (5th Cir. 1991). *Cf.* 28 U.S.C. § 2401(b) (2018) ("A tort claim against the United States shall be forever barred unless . . . action is begun within six months after the date of mailing . . . of notice of final denial of the claim by the agency to which it was presented.").

96 *See* 28 U.S.C. § 2401(b) (2018); *see also* Myszkowski v. United States Gov't, 553 F. Supp. 66, 67–68 (N.D. Ill. 1982).

97 *Myszkowski*, 553 F. Supp. at 68. ("In our view, § 2401(b) provides that tort claimants filing suit against the United States can be barred by the statute of limitations in two ways: (1) they can be barred if they do not file a claim with the appropriate federal agency within two years; or (2) they can be barred even if they do file a timely administrative claim, but fail to file a suit in district court within six months after final notice of the agency's action on their claim.").

98 28 U.S.C. § 2401(b) (2018).

1974 also provides a private cause of action to people who have had their information wrongfully disclosed. Unlike the FTCA, the Privacy Act does not require a plaintiff to exhaust administrative remedies with an agency.[99] Instead, a plaintiff can file suit in a district court immediately. However, the Privacy Act has its own broad list of exceptions,[100] and the Supreme Court has limited a plaintiff's recovery in cases of intentional wrong to "actual damages,"[101] thereby preventing a plaintiff from recovering non-economic damages. On the other hand, the FTCA allows a plaintiff to recover the same types of damages from the government that would be recovered from a private defendant—including emotional distress and punitive damages.[102]

It is arguably harder for a plaintiff to sue a state government. Because this Article uses *Morgan Hill* as a cautionary tale for the privacy-concerned, this Article focuses on a plaintiff's ability to sue the State of California. Like the federal government, California has sovereign immunity unless a statute expressly abrogates its sovereign immunity.[103] California Government Code section 815.6 extends tort liability to a public entity "[w]here [the] public entity is under a *mandatory* duty imposed by an enactment that is designed to protect against the risk of a particular kind of injury[.]"[104] This section is basically a parallel to the FTCA's "discretionary function" exception. The duty must be imposed by statute, and whether it is mandatory or discretionary is a question of law.[105] Accordingly, the plaintiff must first prove that the public entity's duty is mandatory before proceeding to prove their primary cause of action.

In the context of *Morgan Hill*, a private third party would have to first determine whether the California Department of Education (DOE) had a mandatory duty to protect the third party's education records.[106] Arguably, California Education

---

99 *See generally* 5 U.S.C. § 552a(g)(1) (2018) (providing that individuals may bring a civil action against the offending agency).

100 5 U.S.C. § 552a(b)(1)–(12) (2018).

101 FAA v. Cooper, 566 U.S. 284, 287 (2012).

102 *See* 28 U.S.C. § 1346 (2018).

103 *See* Tuthill v. City of San Buenaventura, 167 Cal. Rptr. 3d 820, 827 (Cal. Ct. App. 2014); Cochran v. Herzog Engraving Co., 205 Cal. Rptr. 1, 3 (Cal. Ct. App. 1984); *see also* CAL. GOV'T CODE § 815 (West 2016) (providing that a public entity is not liable for injury unless a statute provides otherwise).

104 GOV'T § 815.6 (emphasis added).

105 *See Tuthill*, 167 Cal. Rptr. 3d at 828 (quoting Haggis v. City of Los Angeles, 93 Cal. Rptr. 2d 327, 333 (Cal. 2000)).

106 *Cf.* Nunn v. State of California, 35 Cal. 3d 616, 624 (1984) (requiring a plaintiff to prove a mandatory duty as a threshold inquiry).

Code § 49076 provides such a duty.[107] According to the statute, "[a] school district *shall not* permit access to pupil records to a person without written parental consent or under judicial order" unless an exception applies.[108] Alternatively, although FERPA does not provide a private cause of action, it imposes a similar mandatory duty and may also serve as a basis for tort liability under § 815.6.[109]

Next, the third party would have to determine whether the DOE breached that mandatory duty. This is where the third party runs into an impenetrable obstacle: the DOE is protected by a judicial order exception under both statutes.[110] Because the DOE disclosure of the approximately ten million student records is pursuant to a judicial order, it cannot be claimed that the DOE breached its duty to any of those students, and none of those students would have a viable claim under section 815.6.[111]

4. *Judicial Orders and Tort Regime Goals*

The question of this Article remains: given that judicial orders may provide legal cover for those who disclose third party information, can a tort regime incentivize socially optimal protections for the privacy-concerned in the face of a judicial order? The quick answer is, unlikely. Again, the definition of socially optimal in this context may vary between the private and government context but only slightly. In the private context, the socially optimal level of privacy protection would be a legal defense that limits discovery and risk of revelation to the degree necessary to maximize transactions.

Tort exposure, however, is arguably less effective in this context than brand risk. Tort liability is limited when the proximate cause of liability flows from a judicial order. As a practical matter, to the extent that the judicial order may reduce transactions (and profit), opportunists may seek out privacy-sensitive industries and threaten lawsuit. The higher the potential loss (via brand risk or tort liability) the more likely the industry is to opt for a settlement even in the face of a frivolous lawsuit.[112] Such settlements can increase industry costs and

---

107 CAL. EDUC. CODE § 49076 (West 2016).

108 *Id.* (emphasis added).

109 *See* GOV'T § 815.6 (discussing a public entity's mandatory duty to protect against certain injuries).

110 *See* 20 U.S.C. 1232g(b) (2018); EDUC. § 49076(a).

111 *See* EDUC. § 49076 (providing for a judicial order exception).

112 *See generally* G. Nicholas Herman, *How to Value a Case for Negotiation and Settlement*, 31 MONT. LAW. 5, 22 (2005) ("The foregoing methods of valuation

reduce transactions.[113] To the extent, however, that the judiciary functions as an active gatekeeper of discovery decisions, the court can minimize these costs and by extension increase socially desirable transactions.

The problem is exacerbated in the government entity context, where there is no brand risk and only limited tort liability to incentivize protection of third-party interests. In such contexts, the judiciary serves an essential gatekeeper role that cannot be abrogated—there is no party, no law, and no alternative incentivizing regime that can fill that role. It is precisely this type of scenario that the judicial advisory committee arguably anticipated in its revision of Rule 26 of the Federal Rules of Civil Procedure.[114]

II
PROTECTING THE PRIVACY INTEREST

Even in a perfect, privacy-protected world (i.e. the privacy right is legislatively articulated and tort liability is optimal), the judicial order exemption in such statutes makes the role of the judiciary as gatekeeper and protector of the privacy interest irreplaceable.[115] As set forth below, the rules of procedure and the judicial protective order are but two means by which courts have protected the privacy interest. It is time, however, for the courts to fully employ the discretion afforded them in Rule 26 and to adopt greater protections for the privacy interest than the traditional protective order.

A. Rules of Discovery—Then and Now

The privacy interest is not a new concept to the American judiciary. Indeed, for more than eighty years, courts have recognized the burden imposed on private parties when their personal, private information is disclosed as part of a discovery request.[116] As has long been the case, litigants file motions for

---

largely assume that the client's decision to settle or go to trial will be made solely on the basis of which course of action will yield the best result from a rote economic standpoint. However, choosing between settlement and trial is not purely an economic process.").

113 *See* Eliot Martin Blake, *Rumors of Crisis: Considering the Insurance Crisis and Tort Reform in an Information Vacuum*, 37 EMORY L.J. 401, 408 (1988).

114 *See* FED. R. CIV. P. 26(g) advisory committee's note to the 1983 amendment ("Concern about discovery abuse has led to widespread recognition that there is a need for more aggressive judicial control and supervision.").

115 *See supra* notes 10–13.

116 *See, e.g.*, Wiesenberger v. W.E. Hutton & Co., 35 F.R.D. 556, 557 (S.D.N.Y. 1964) (limiting the disclosure of personal income tax returns unless "clearly required in the interests of justice"); Conn. Importing Co. v. Cont'l Distilling Corp., 1

discovery—plaintiffs specify the class of documents and information they believe will assist, directly or indirectly, in proving or disproving an element of their case.[117] It is relatively costless for plaintiffs to request more than they might need for two reasons: (1) the information might unexpectedly prove useful or (2) the cost or risk of producing the information might force the defendant to settle. The courts have the discretionary authority to limit the request if, for example, the invasion of third-party privacy outweighs the evidentiary benefit to the plaintiff.[118] Although courts have always had the authority, in practice, courts rarely limit discovery on privacy grounds on their own motion, especially when a litigant (the defendant) bears the privacy burden—that is, when the information requested is the defendant's own personal information.[119] Courts rationalize (correctly) that the motions for discovery put the defendant on notice of the desired information, which gives the defendant the opportunity to object to its disclosure.[120] If the defendant (the information provider in this example) does not object to the discovery request, then the court will not object either.[121] Even when a party does object to the discovery request, courts are reluctant to grant the objection and impose limitations.[122]

As a result, under the early iterations of Rule 26 of the Federal Rules of Civil Procedure, parties could request and be granted access to extensive data as there was a plausible (even if tenuous) connection between the information requested and an element at issue in the case.[123] After several decades of broad discovery orders, the legal community, focusing not on

---

F.R.D. 190, 193 (D. Conn. 1940) (recognizing that the court has discretion to limit discovery requests to avoid an undue invasion of privacy).

117 *See* FED. R. CIV. P. 26(b) advisory committee's note to 1946 amendment (clarifying that discoverable information covered "not only evidence for use at the trial but also inquiry into matters in themselves inadmissible as evidence but which will lead to the discovery of such evidence").

118 *See* Stark v. American Dredging Co., 3 F.R.D. 300, 302 (E.D. Pa. 1943) (citing *Conn. Importing Co.*, 1 F.R.D. at 193).

119 *See Conn. Importing Co.*, 1 F.R.D. at 193 ("[T]he plaintiff on a noticed hearing has had opportunity to protest against any oppressive invasion of its privacy. No such protest has been made . . . . Thus it is scarcely entitled to the protection . . . .").

120 *See id.*

121 *See id.*

122 *See, e.g.*, Apco Oil Corp. v. Certified Transp., Inc., 46 F.R.D. 428, 432 (W.D. Mo. 1969) (denying the objection to the discovery request and ordering the plaintiff to answer all of the interrogatories).

123 *See* Hickman v. Taylor, 329 U.S. 495, 507–08 (1947) (affording "broad and liberal treatment" to discovery rules as long as the information requested is relevant and non-privileged).

privacy but on the economic burden associated with these requests, demanded reform.[124] In 1983, the Federal Rules of Civil Procedure imposed a proportionality standard to limit discovery requests.[125] Rule 26 was amended to include a list of factors—buried in subsection (b)(2)(C)(iii)—for courts to balance when evaluating the proportionality of a discovery request to the needs of the case.[126] Despite the courts' preexisting authority to limit discovery based on privacy concerns, the word "privacy" was curiously absent from this new list of factors.[127] Furthermore, courts rarely applied the amended proportionality factors,[128] and when they did, they emphasized the economic burdens of discovery as the primary limiting factor.[129]

As judicial discovery requests intersected with technological advancements and the beginnings of the new "Big Data" era, the legal community cried out again for discovery reform, citing unreasonably broad discovery requests and mountainous expenses associated with producing the desired discovery.[130] In response, the Federal Rules of Civil Procedure were amended several more times to further empower the courts to

---

124 *See* Milton Pollack, *Discovery—Its Abuse and Correction*, 80 F.R.D. 219, 221 (1978) (arguing for discovery reform because the contemporary rules gave "the parties virtually unlimited management over discovery . . . limited only by privilege and relevancy standards."); *see also* FED. R. CIV. P. 26(b) advisory committee's note to 1983 amendment (justifying the amendment because the contemporary discovery abuse resulted in "excessively costly and time-consuming activities that are disproportionate to the nature of the case, the amount involved, or the issues or values at stake").

125 FED. R. CIV. P. 26(b) advisory committee's note to 1983 amendment.

126 *Id.* The amendment "encourage[d] attorneys to be sensitive to the comparative costs of different methods of securing information" and determined proportionality by evaluating "[the lawsuit's] nature and complexity, the importance of the issues at stake in a case seeking damages, the limitations on a financially weak litigant to withstand extensive opposition to a discovery program or to respond to discovery requests, and the significance of the substantive issues."

127 *See* Seattle Times Co. v. Rhinehart, 467 U.S. 20, 30 (1984) ("The Rules do not differentiate between information that is private or intimate and that to which no privacy interests attach. . . . Thus, the Rules often allow extensive intrusion into the affairs of both litigants and third parties." (footnote omitted)).

128 *See* Agnieszka A. McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, 64 U. KAN. L. REV. 235, 252 (2015) ("Despite the Committee's express intent to make proportionality a limit on discovery, courts seemed to under-utilize the proportionality factors."); FED. R. CIV. P. 26(b) advisory committee's note to 2015 amendment.

129 *See* McPeak, *supra* note 128, at 253 and accompanying text.

130 *See* FED. R. CIV. P. 26(b) advisory committee's note to 1993 amendment ("The information explosion of recent decades has greatly increased both the potential cost of wide-ranging discovery and the potential for discovery to be used as an instrument for delay or oppression."). *See also id.* at advisory committee's note to 2000 amendment.

restrict discovery and emphasize the proportionality factors.[131] Then, in 2015, the proportionality standard and the guiding factors moved to the forefront of Rule 26(b),[132] indicating a desire to refocus the courts and litigants on limiting discovery.[133] In fact, Chief Justice Roberts specifically recognized the need for the legal community to heed the 2015 amendments and implement the proportionality test as a best practice for case management and the pursuit of efficient justice.[134] Implementation and compliance is a two-way street. On the one hand, "[j]udges must be willing to take on a stewardship role, managing their cases from the outset rather than allowing parties alone to dictate the scope of discovery and the pace of litigation."[135] On the other hand,

> lawyers must size and shape their discovery requests to the requisites of a case. Specifically, the pretrial process must provide parties with efficient access to what is needed to prove a claim or defense, but eliminate unnecessary or wasteful discovery. *The key here is careful and realistic assessment of actual need.*[136]

During the same time frame that the Federal Rules of Civil Procedure were first amended to limit discovery requests, Congress passed laws to protect certain sensitive information.[137]

---

131 In 1993, Rule 26(b) was amended to "enable the court to keep tighter rein on the extent of discovery." In 2000, Rule 26(b)(1) was amended to further limit party-controlled discovery only to the information that is relevant to the "claim or defense" of either litigant rather than all information that was relevant to the "subject matter" of the action. Nonetheless, the court has the power to order discovery of all information relevant to the subject matter of the action for good cause. In 2006, Rule 26 was amended yet again to address issues of cost and size associated with the production of electronically stored information, especially when that information is not reasonably accessible. Finally, in 2015, Rule 26(b) was reorganized to place the proportionality test at the beginning of the rule, signaling a desire for the courts to actually follow the rule and apply the test.

132 The factors were unearthed from the multi-layered subsections of Rule 26(b)(2)(C)(iii) and reorganized into Rule 26(b)(1). FED. R. CIV. P. 26(b)(1)

133 *See* FED. R. CIV. P. 26(b) advisory committee's note to 2015 amendment.

134 *See* Roberts, *supra* note 16, at 6–7.

135 *Id.* at 10.

136 *Id.* at 7 (emphasis added).

137 To give a few examples, Congress passed the Family Educational Rights and Privacy Act (FERPA) in 1974 to protect the disclosure of student records. 20 U.S.C. § 1232g(b)(2)(B) (2018). *See also Legislative History of Major FERPA Provisions*, U.S. DEP'T OF EDUC. [hereinafter *Legislative History*], http://www2.ed.gov/policy/gen/guid/fpco/ferpa/leg-history.html [https://perma.cc/CD6M-N4A7] (last modified Feb. 11, 2004).

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in part to protect patients' privacy by keeping their medical records confidential. 42 U.S.C. § 1320d–6 (2018).

The Children's Online Privacy Protection Act was passed in 1998 to protect children's privacy online while under the age of thirteen. 15 U.S.C. § 6501 (2018).

These laws impose negative consequences for the disclosure of protected information in the absence of consent or a court order.[138] The procedural requirements associated with seeking a court order essentially imposed a mandatory threshold issue for the litigants to argue and the courts to consider: whether the information is more important to the needs of the case than the privacy protection it currently enjoys. Understandably, sometimes the benefit of the information does justify its disclosure—indeed, that is why the judicial order exceptions exist in the first place—but the legal community has recognized the importance of reducing that information's exposure to irrelevant parties.[139]

B. The Protective Order

As set forth above, the primary means by which a court can protect the privacy interest is to limit discovery in the first instance. Once discovery is granted, however, judges often employ a secondary method to protect the privacy interest—the protective order.[140] Generally, protective orders require that the information be used only for the case in which it is requested and be accessed only by the requesting party.[141] Protective orders can also be narrowly tailored to limit the scope of the information requested,[142] require the redaction of personal identifying information,[143] and order the return or destruction of the information once the case closes.[144] In the case of

138 *See generally Legislative History, supra* note 137 (discussing FERPA, HIPAA, and the Children's Online Privacy Protection Act as examples of laws that penalize illegal disclosure of protected information).

139 Upon motion and a showing of good cause, the court can impose a protective order on the desired information with various parameters specifying the use and scope of the information. *See* FED. R. CIV. P. 26(c). In cases involving especially technical discovery, courts can appoint a special master to facilitate the conveyance of information between parties in a reasonably controlled, protected medium. *See* FED. R. CIV. P. 53.

140 *See* Haghayeghi v. Guess?, Inc., 168 F. Supp. 3d 1277, 1281 (S.D. Cal. 2016); Hinsdale v. City of Liberal, Kan., 961 F. Supp. 1490 (D. Kan. 1997), *aff'd*, 981 F. Supp. 1378 (D. Kan. 1997); United States v. Smith, 602 F. Supp. 388 (M.D. Pa. 1985), *aff'd*, 776 F.2d 1104 (3d Cir. 1985); Britt v. Superior Court, 574 P.2d 766 (Cal. 1978); Alch v. Superior Court, 82 Cal. Rptr. 3d 470 (Cal. Ct. App. 2008).

141 *See* Ragusa v. Malverne Union Free Sch. Dist., 549 F. Supp. 2d 288, 294–95 (E.D.N.Y. 2008).

142 *See id.*

143 *See* Music Grp. Macao Commercial Offshore Ltd. v. Foote, No. 14-cv-03078-JSC, 2015 WL 2170121, at *3 (N.D. Cal. May 8, 2015).

144 *See In re* C.F., Nos. H12CP08012016A, H12CP08012017A, 2009 WL 455922, at *12 (Conn. Super. Ct. Jan. 26, 2009). Additionally, destroying documents is easier said than done in the digital age. Before e-discovery, documents could be destroyed by shredding or burning and there would be no backup disk or flash drive to reverse the destruction. Presently, digital documents can be re-

e-discovery, the protective order even tries to provide some cybersecurity. These orders are not foolproof, however, and cannot replace the initial gatekeeper role of the judge in granting discovery in the first instance.

Moreover, protective orders are effective only when the signatories comply with their parameters, and even then information can be misplaced or disclosed inadvertently.[145] The fairly modern *Zyprexa* case exemplifies this limitation.[146] About thirty thousand personal injury suits were filed against Eli Lilly & Company for side effects caused by the pharmaceutical company's schizophrenia medication Zyprexa.[147] In connection with those lawsuits, the court issued a protective order that placed millions of documents under seal to prevent them from being disclosed to the public.[148] However, a reporter, an expert witness for the plaintiffs, and an outside attorney unrelated to the *Zyprexa* lawsuits conspired to disseminate and publish the documents.[149] The protective order provided an exception to the otherwise prohibited disclosure of any of the documents; the documents could be turned over if they were subpoenaed and proper procedures were followed.[150] The reporter hatched the plan, the outside attorney subpoenaed the documents on false pretenses, and the expert witness transferred the documents to the attorney. Millions of confidential, sealed documents then found their way into the hands of various organizations and individuals, including the New York Times, who then disseminated the documents to the public at large.[151] Once the court and the *Zyprexa* litigants heard of the breach, the court ordered any disseminated documents to be returned to the special master, but the damage could not be undone.[152]

---

stored from external hard drives, flash drives, a cloud storage service, and built-in backup tools that modern operating systems come equipped with.

145 Indeed, the Federal Rules of Civil Procedure address issues of inadvertent disclosure. *See* FED. R. CIV. P. 26(b)(5)(B).

146 *See* Childs *supra* note 34, at 579; *In re* Zyprexa Injunction, 474 F. Supp. 2d 385, 423–25 (E.D.N.Y. 2007).

147 *See Zyprexa Injunction*, 474 F. Supp. at 391.

148 *See* Childs, *supra* note 34, at 579–80.

149 *See Zyprexa Injunction*, 474 F. Supp. at 392 ("To carry out the scheme for obtaining and disseminating the protected documents, [the attorney] intervened in a state case in Alaska wholly unrelated to Zyprexa. In that case, he then subpoenaed from [the expert witness] confidential documents he knew to be under the protective order which bore no relevance to the Alaska litigation. The subpoenaed documents were sent by [the expert witness to the attorney] pursuant to an expedited amended subpoena about which Lilly was deliberately kept in the dark so that it would be unable to make a timely objection.").

150 *Id.* at 398.

151 *Id.* at 392–93.

152 *Id.* at 393; *see also* Childs, *supra* note 34, at 593.

Many of the recipients refused to return the documents, while others had already published them online or in newspapers, effectively immortalizing the confidential information in the public domain.[153]

The protective order was a great security feature in theory, but its effectiveness was nullified by a nefarious trio, only one of whom had permission to access the information.[154] This example serves as a cautionary tale of the damage that can be caused when sensitive information falls into the wrong hands.

Intentional dissemination and inadvertent disclosure were less of a problem before modern technology when discovery requests were fulfilled with reams of paper and other tangible items. As a practical matter, it was just more difficult to copy and distribute physical documents before the digital age. Correcting inadvertent disclosure was as easy as "clawing back" improperly disclosed documents,[155] and protected material could be inventoried upon return once the case closed. But digital storage—despite its intangible nature, firewalls, and passwords—undermines the primitive, yet more tractable court protections applied to a ream of paper in a locked filing cabinet.

The Federal Rules of Civil Procedure acknowledge the technicalities associated with the disclosure of electronically stored information.[156] But even highly detailed, technical discovery plans cannot protect private information with absolute certainty. In this day and age, technology has made information

---

153 *See* Childs, *supra* note 34, at 593 ("[T]he litigants . . . and the court were making significant efforts to retrieve the documents—efforts which were . . . largely futile.").

154 This case exemplifies the difficulty of drafting and enforcing a protective order. The attorney who disseminated the information was not disciplined or fined for his action because he was not actually bound by the order. The attorney received the documents from an expert witness who violated the protective order. The court did order the attorney to return or destroy any documents he had. *See Zyprexa Injunction*, 474 F. Supp. 2d at 429–30. The lack of penalty for the actual information disseminator demonstrates the limited power of the protective order.

155 *See* FED. R. CIV. P. 26(b)(5)(B) (explaining when information is inadvertently disclosed to the opposing party, the recipient must return the information to the disclosing party). It is much easier to return pieces of paper that have been reproduced a finite number of times than it is to return a digital document that may be stored on a recovery drive, forgotten in a trash bin, or hidden in a download folder.

156 FED. R. CIV. P. 26(f)(3)(C) (requiring the parties to meet and confer to establish a discovery plan that addresses "any issues about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced"). *See also* FED. R. CIV. P. 26 advisory committee's note to 2006 amendment.

increasingly accessible,[157] more difficult to destroy,[158] and easier to reproduce.[159] Furthermore, any entity that houses large electronic sets of sensitive data is a target for hackers.[160] Several law firms have recently been victims of cyberattacks because of their collections of personal identifying information, trade secrets, and insider knowledge for advantageous stock market trades.[161] To shore up the protective order for modern day realities, courts must first acknowledge that they cannot rely solely on the protective order of old to limit the inadvertent disclosure of sensitive information. A means to assure protection is to consider and weigh the affected parties' privacy interest at every step of the discovery process.

III
PROMOTING CYBERSECURITY

Cybersecurity is a battle that everyone seems to be losing. Headlines scream out of cyberattacks on private and governmental data sets, and even of government surveillance of digital troves thought to be private and secure. It is far beyond the scope of this Article to discuss the intricate engineering strate-

---

157 An e-mail address can be accessed from any computer or smart phone with an internet connection, digital documents can be stored in the cloud or some other popular storage server like Dropbox, and every time that information is transmitted from one location to another the sender, recipient, and the intermediary service all have access to that information.

158 *See* Joan E. Feldman & Larry G. Johnson, *Lost? No. Found? Yes. Those Computer Tapes and E-mails are Evidence*, BUS. L. TODAY, May/June 1999, at 18–22 (discussing various ways to protect data from destruction and how to recover data that has been destroyed).

159 *Id.*

160 Banks, hospitals, social media outlets, and government agencies are among some of the various entities that have been victims of cyber attacks in the past year alone. *See* Sy Mukherjee, *Hackers Have Crippled Another Major Hospital Chain with a Cyberattack*, FORTUNE (Mar. 29, 2016, 1:18 PM), http://fortune.com/2016/03/29/hackers-medstar-cyber-attack [https://perma.cc/4CJ5-APZQ] (discussing a cyberattack on MedStar, which operates 10 hospitals in the Washington, D.C. area); Riley Walters, *Continued Federal Cyber Breaches in 2015*, HERITAGE FOUND. (Nov. 19, 2015), https://www.heritage.org/cybersecurity/report/continued-federal-cyber-breaches-2015 [https://perma.cc/S7WX-T5BY] (discussing government agencies that were breached in 2014 and 2015); *How Cybercriminals Target Social Media Accounts*, MCAFEE, https://www.mcafee.com/us/security-awareness/articles/how-cybercriminals-target-social-media-accounts.aspx [https://perma.cc/NUH3-9NRY] (last visited Jun. 27, 2016) (discussing how and why social media platforms such as Facebook, Twitter, Instagram, and LinkedIn are hacked).

161 *See* Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016, 9:14 PM), https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504 [https://perma.cc/K3LN-CTC2] (discussing recent cyberattacks on prominent law firms).

gies to keep data truly secure. It is also beyond the scope of a generalist jurist hearing yet another discovery request on a busy day in court. Therefore, this section examines not engineering and encryption, but the judicial practice of appointing a special master to handle the more technical intricacies of e-discovery.

Under the current Federal Rules of Civil Procedure, special masters enjoy relatively expansive authority that allows them to handle various duties determined and consented to by the parties, hold trial proceedings and make or recommend findings of fact (especially when there is a complex issue regarding accounting or damages computation), and address certain pretrial and posttrial matters that would not be handled effectively and efficiently by a district court judge.[162] However, their authority has evolved considerably over time from humble, narrow beginnings as issues became more technical and as civil dockets became congested with ever-increasing mounds of discovery requests.[163]

In its initial iteration, Rule 53 allowed special masters to hear trial testimony and report recommended findings of fact to the jury when the issues were too complicated for a jury to digest alone or, where non-jury matters are concerned, when "exceptional conditions" required the appointment of a special master.[164] Issues were rarely too complex for a jury to address without the help of a special master, and the Supreme Court construed "exceptional conditions" narrowly.[165] Without describing a condition that was "exceptional," the Supreme Court recognized several conditions that *were not* exceptional enough to condone the appointment of a special master.[166] Notably, docket congestion, complex litigation issues, and trial duration were insufficient circumstances to pass the "exceptional" analysis.[167] Accordingly, special masters were seldom used when Rule 53 was newly drafted.

In 2003, Rule 53 was amended to its current language, thus drastically expanding both the circumstances in which a special master may be appointed and his or her authority in

---

162 FED. R. CIV. P. 53(a).

163 *See* Shira A. Scheindlin and Jonathan M. Redgrave, *Special Masters and E-Discovery: The Intersection of Two Recent Revisions to the Federal Rules of Civil Procedure*, 30 CARDOZO L. REV. 347, 348–51 (2008).

164 *Id.* at 348 n.2 and accompanying text.

165 *Id.* at 349 n.12 and accompanying text.

166 *See* La Buy v. Howes Leather Co., Inc., 352 U.S. 249, 259 (1957).

167 *Id.*

such a circumstance.[168] Arguably the most expansive of the added provisions allows for the appointment of a special master to "perform duties consented to by the parties."[169] As long as both parties agree to the appointment and scope of the special master's duty then the special master may perform those duties.[170] The rule no longer requires the issue to be too complex for a jury and no longer requires an "exceptional condition" for the appointment of a special master. As a result, special masters have become increasingly prevalent throughout all types and stages of litigation.[171]

In this Article, the use of special masters for discovery management is strongly encouraged. Courts often consider appointing a special master when large, electronic data sets are to be accessed or transferred. In the *Morgan Hill* case, for example, the court took care to select a special master with cybersecurity credentials—no doubt because of the size and sensitivity of the data at issue. But as set forth below, a cybersecurity or industry specialist is not necessarily a privacy interest expert. This Article encourages judges to be particularly sensitive to that fact. So much so that, under specific circumstances, the court may want to appoint an additional special master to specifically monitor and protect the privacy interests of underrepresented parties.[172]

---

168 FED. R. CIV. P. 53(a).

169 FED. R. CIV. P. 53(a)(1)(A).

170 *Id.*; *see also* Scheindlin & Redgrave, *supra* note 163, at 352 n.26–27 and accompanying text.

171 *See* David Ferleger, *Judicial Adjuncts in Disability Rights Litigation*, FED. LAW., Dec. 2012, at 44 (noting that special masters are used more often since the 2003 amendment in "constitutional, commercial, disabilities, mass tort, and other litigation for assistance at all stages in the adjudication process"). For example, in *Morgan Hill*, the parties agreed to the appointment of a special master to facilitate "the parties' development of an electronic discovery protocol." Order at 2:4–9, Morgan Hill Concerned Parents Ass'n v. Cal. Dept. of Educ., No. 2:11-cv-03471-KJM-AC (E.D. Cal. July 2, 2015), ECF No. 116. The special master proposed an e-discovery protocol that addressed which databases would be available to the plaintiffs, which platform e-mails and other network files would be uploaded so that the plaintiffs may have access to view and search them, how to sort privileged documents from non-privileged documents, notification of the disclosure of student records pursuant to FERPA, and various safeguards to be implemented to further protect the sensitive information from disclosure. Order at 1–14, *Morgan Hill*, No. 2:11-cv-03471-KJM-AC (Nov. 3, 2015), ECF No. 127-1.

172 *See* FED. R. CIV. P. 53(a).

IV
A NEW DISCOVERY FRAMEWORK: PROTECT, PROMOTE, THEN PERMIT

One may ask, however, if a judge orders that private data be handed over, does it not mean the plaintiff needs the data for its case? This is an excellent question, and one contemplated by the Federal Rules of Civil Procedure. There are limits to how permissive a court should be in allowing plaintiffs to gather evidence. The discovery granted must be "proportional to the needs of the case."[173] In essence, a plaintiff's "need" is a term of art that must be balanced against a defendant's "costs" in providing information[174]—these costs arguably include the burden to third parties such as parents of California school children.[175] This balancing act has long been the law, but the language of the statute was recently changed to greater strengthen the limits judges should place on discovery—in no event more than needed by the case.[176]

In particular, third-party interests are difficult to defend in a court of law because of the cost of intervening in a court

---

173 FED. R. CIV. P. 26(b)(1) ("Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case . . . .").

174 *See id.* In determining proportionality, the parties and the court need to consider the following factors: "the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit." *Id.*

175 Historically, courts have considered the financial burden of producing the requested discovery, but with the abundance of private, sensitive data being stored in the digital world, some scholars have encouraged the courts to consider the privacy burden as well. *See* McPeak, *supra* note 128, at 235, 288–91. Indeed, some courts have started to do just that. *See* Appler v. Mead Johnson & Co., No. 3:14–cv–166–RLY–WGH, 2015 WL 5615038, at *4 (S.D. Ind. Sept. 24, 2015); *see also* Bd. of Trs. v. Cut Bank Pioneer Press, 160 P.3d 482, 487 (Mont. 2007) (finding FERPA does not prohibit "the public release of redacted records regarding board disciplinary actions which contain no personally identifiable information").

176 *See* FED. R. CIV. P. 26 advisory committee's note to 2015 amendment. Limiting discovery based on the proportional needs of the case was an idea adopted back in 1983. *Id.* However, over the years, the proportionality requirement got buried within the subsections of Rule 26(b) and "the Committee had been told repeatedly that courts were not using [the] limitations as originally intended." *Id.* The 2015 Amendment put proportionality and the factors that determine proportionality at the forefront of the rule to emphasize their significance and ensure compliance. *Id.* The 1983 Committee Note recognized the need for "greater judicial involvement in the discovery process," while the 1993 Committee Note sagaciously observed that "[t]he information explosion of recent decades has greatly increased . . . the potential cost of wide-ranging discovery . . . ." *Id.* The 1993 Committee's words ring even more true today in the era of e-discovery.

case.[177] The judge, of course, is in the most efficient position to protect third-party interests and eliminate the need for third parties to incur legal costs. After all, in some circumstances, third-party information is at risk only because of the unique prerogative of the judiciary to compel discovery. Thus, judges abdicating their gatekeeper role on privacy issues would impose a monitoring cost and litigation cost on third parties to the litigation that could be handled directly by special masters and judges. As discussed above, defendants do not always have an incentive to protect third-party privacy interests.[178] Therefore, a general pattern of judicial acquiescence to litigants' discovery requests will neither encourage plaintiffs to self-limit discovery requests nor encourage defendants to invest in privacy protections. A passive judiciary in the face of third-party privacy issues would serve only to increase demand in legal services by third parties innocently scooped up in the litigation process of others.

The good news is that the judiciary is beginning to exercise extreme caution in the face of large, sensitive datasets.[179] But as the *Morgan Hill* case shows, there is uneven consideration of the privacy interest in discovery.

A. A Judicial Strategy to Protect Privacy Interests

Presented below is a simple three-step, judicial strategy to protect the privacy interests of third parties. The first step is a

---

177 Although it varies by jurisdiction, the filing fee *alone* for a motion to intervene could cost hundreds of dollars. *See, e.g.*, *Superior Court Filing Fees*, MASS. CT. SYS., https://www.mass.gov/service-details/superior-court-filing-fees [https://perma.cc/45JY-MVFH] (indicating that it costs $240 to file a Motion to Intervene as Plaintiff plus a $20 security fee, plus a $15 surcharge). Beyond that, attorneys charge hundreds of dollars *per hour* to represent someone in litigation. *See* David Goguen, *How, and How Much, Do Lawyers Charge?*, LAWYERS.COM, https://www.lawyers.com/legal-info/research/how-and-how-much-do-lawyers-charge.html [https://perma.cc/JB49-2NHE] (last visited Mar. 4, 2016) ("In rural areas and small towns, lawyers tend to charge less, and fees in the range of $100 to $200 an hour for an experienced attorney are probably the norm. In major metropolitan areas, the norm is probably closer to $200 to $400 an hour.").

178 *See supra* subpart I.C.

179 *See, e.g.*, Music Grp. Macao Commercial Offshore Ltd. v. Foote, No. 14-cv-03078-JSC, 2015 WL 2170121, at *3 (N.D. Cal. May 8, 2015) (recognizing the defendant's need for the requested documents, but ordering that the requested documents be disclosed with personally identifying information redacted); Ragusa v. Malverne Union Free Sch. Dist., 549 F. Supp. 2d 288, 294–95 (E.D.N.Y. 2008) (limiting the disclosure to a select group of math students and further limiting the disclosure by redacting all personally identifiable information); *see also* Order, Easton Area Sch. Dist. v. Express Times, No. C-0048-cv-2011-4775 (Pa. Commw. Ct. April 27, 2011), 2011 WL 8478250 (ordering the disclosure of the requested emails but ordering that those emails be redacted to exclude information protected under FERPA).

threshold privacy screen to alert judges to cases where the privacy interests may need the greatest judicial protection. When a judge is balancing the privacy interest against disclosure, the need to protect the privacy interest is particularly acute when third parties cannot self-protect (opt out of the transaction) and cannot pursue tort remedies in the event of disclosure. As a threshold analysis, therefore, a judge should intervene to protect privacy interests in discovery when certain elements exist because they indicate circumstances when such rights are least likely to be otherwise protected.[180]

In addition, the judge should identify which data should be deemed "personal" or "sensitive."[181] Not all data are equal. Some data are particularly sensitive so heightened protections are justified.[182] In this first step it is particularly important to protect data that is of a highly sensitive nature—data that is simply too-hot-to-handle. Some too-hot-to-handle data is easy to identify. For example, it is broadly accepted that social security data, trade secrets, and certain financial data may fall into the highly sensitive category. Over time, a court might establish a standard list of the types of third-party information that would require special treatment and affirmative permission by a judge (or a special master) to compel.[183]

The fact that Congress[184] itself has decided by statute that certain data is highly sensitive is a clear indicator that the courts should narrowly construe the judicial order exception

---

180 As suggested *infra* subpart IV.C., under certain circumstances, a judge may wish to appoint a second special master tasked specifically to monitor privacy matters.

181 Courts have long experienced dealing with "confidential" information. Some are well-categorized and protected such as those that enjoy attorney-client privilege, the spousal privilege, and others. As used here, "private data" may include these categories but is much broader in scope.

182 *See* McPeak, *supra* note 128, at 260 (highlighting federal statutes that specifically protect certain financial information, personal information of minors, *school records*, video rental information, information recorded by web service providers, limiting telemarketing, and medical information).

183 Special thanks to Professor Steven J. Eagle of the Antonin Scalia Law School at George Mason University for his insights on this point.

184 Congress is not the only body who recognizes the data being asked for is of a special nature; the Federal Trade Commission—an agency with extensive privacy and cybersecurity expertise—has express warnings to parents to safeguard their children's information. Indeed, the FTC warning encourages parents to hold their school districts' feet to the fire on data gathering and protection. *See Protecting Your Child's Personal Information at School*, FED. TRADE COMM'N (Aug. 2012), http://educationnewyork.com/files/alt056.pdf [https://perma.cc/M299-YDG7] (encouraging parents to ask for a copy of the school's policy on surveys, directory information policy, and to ask who has access to the child's personal information, and also encouraging parents to file a complaint with the Department of Education when a breach has occurred). Congress has also directed the FTC to require

provided in these statutes by asking one simple question: not only can, but s*hould*, the court compel the requested data to be handed over?

1. Step One—The Privacy Screen
   a. Third-party privacy interests are implicated;
   b. The privacy interests at stake are identified as a concern by common law principles or by state or federal statute (e.g. FERPA); or
   c. The defendant (the information collector) is a government entity.

If the privacy screen indicates that third-party privacy interests are potentially threatened, the judge may weigh more heavily the privacy concerns set forth in Steps Two and Three below. As an alternative, the judge may wish to appoint a second special master tasked specifically to monitor privacy issues throughout the discovery process. This "privacy master" can then advise the judge or the case's primary special master on privacy considerations at each stage of discovery and help balance privacy protections in judicial orders. The summary of Steps Two and Three below is followed by more in-depth analyses of each step.

2. Step Two—Protecting the Privacy Interest
   a. Demand that data be redacted and/or aggregated to remove individual identifiers;
   b. Determine the least amount of data access that is "proportional to the needs of the case;"[185] and
   c. Provide affected individuals an "opt-out" option.
3. Step Three—Promoting Cybersecurity
   a. Assign a special master as needed;
   b. Limit the number of people with access to the data;
   c. Keep data under defendants' security controls; limit the electronic transfer and storage of data; and
   d. Place data transfers "under seal" and apply protective orders liberally, but rely on them as warnings rather than cybersecurity protections.

B. Step Two—Protecting Privacy

The privacy interest considered in Step Two should not be confused with the cybersecurity concerns discussed in Step

---

that financial institutions protect consumers' personal financial information. *See* 15 U.S.C. §§ 6801–09, 6821–27 (2018).

185 Of course this will not eliminate the possibility that determined hackers can reverse engineer even limited data by matching it to complementary data in the hackers' possession.

Three. In general, the cybersecurity interest is more concerned with the inadvertent exposure of data to unauthorized parties (for example, computer hackers).[186] A party's or third-party's privacy interest, in contrast, applies even to the legitimate exposure of data to the requesting party. For example, in the *Morgan Hill* case, third parties have rightfully noted that particular privacy interest—they question why the plaintiff should see such detailed information as home addresses, social security numbers, and disciplinary records.[187] Consideration of these privacy interests is not only part of a well-crafted judicial order, but is also well within the judicial wheelhouse.[188]

Most courts realize the sensitivity of information that can be disclosed only through judicial order, subpoena, or parental consent, and seek to limit the scope of the disclosure as much as possible.[189] Many have followed Step Two by placing thoughtful limits to data disclosures.[190] Still, as proved by the

---

186 Of course the privacy interest and cybersecurity interests are often so intertwined it is difficult to separate the two. For example, protecting the privacy interest in Step One—limiting the data exposed—is the best way to protect data in the first place. However, this Article speaks of the privacy interest and cybersecurity interests separately here to focus and simplify the process for the judiciary.

187 *See* Letter from Patrick A. Chabot, Superintendent, Sonora Union High School District, to Kimberly J. Mueller, Morgan Hill Concerned Parents Ass'n v. Cal. Dep't of Educ., No. 2:11-cv-03471 (E.D. Cal. Apr. 11, 2016), No. 173-1.

188 *See infra* note 189 and accompanying text. Ordering for information redaction seems to be a relatively simple way to assuage those concerns.

189 *See, e.g.*, Music Grp. Macao Commercial Offshore Ltd. v. Foote, No. 14-cv-03078, 2015 WL 2170121, at *3 (N.D. Cal. May 8, 2015) (recognizing the defendant's need for the requested documents, but ordering that the requested documents be disclosed with personally identifying information redacted); Ragusa v. Malverne Union Free Sch. Dist., 549 F. Supp. 2d 288, 294–95 (E.D.N.Y. 2008) (limiting the disclosure to a select group of math students and further limiting the disclosure by redacting all personally identifiable information); Easton Area Sch. Dist. v. Express Times, No. C-0048-cv-2011-4775, 2011 WL 8478250 (Pa. Commw. Ct. Apr. 27, 2011), *aff'd*, 41 A.3d 977 (Pa. Commw. Ct. 2012) (ordering the disclosure of the requested emails but ordering that those emails be redacted to exclude information protected under FERPA).

190 *See, e.g.*, Davids v. Cedar Falls Cmty. Schs., No. C96-2071, 1998 WL 34112767, at *3 (N.D. Iowa 1998) (finding that after conducting a balancing test in which the privacy interest of the student is weighed against the genuine need of the party requesting disclosure, disclosure will be ordered when the need for disclosure outweighs the student's privacy interest); *In re* C.F., No. H12CP08012016A, H12CP08012017A, 2009 WL 455922, at *2 (Conn. Super. Ct. Jan. 26, 2009) (suggesting that the attorneys retained by the third parties, whose privacy rights could potentially be affected by the outcome of a discovery request, could be heard on the disclosure issues relative to the proceedings conducted by the court); Board of Trs. v. Cut Bank Pioneer Press, 160 P.3d 482, 487 (Mont. 2007) (finding that student disciplinary records that have personally identifiable information redacted would not violate FERPA because they would not be "educational records" anymore as defined by FERPA).

breathtaking scope[191] and slim regard of third-party privacy interests[192] in the *Morgan Hill* order, the need to emphasize the importance of the privacy interest remains.

1. *Redact and/or Aggregate Identifying Information*

When data must be transferred to the plaintiff, one way to limit inadvertent, individual exposure is to remove identifying information. This is often accomplished by courts ordering that data be redacted or aggregated.[193] This tried and true brand of judicial protection is still a valuable strategy in today's digital world. However, the court should not be overly confident in its effectiveness as bits and pieces of information can be re-aggregated and combined over different data sources to the ultimate detriment of privacy rights.[194] An additional drawback is that redacting or aggregating information can be time consuming and cost prohibitive. But high costs of redaction or aggregation should not immediately lead the court to favor release of unredacted or disaggregated data. Rather, the balanc-

---

191 *See* Notice of Disclosure of Student Records, Morgan Hill Concerned Parents Ass'n v. Cal. Dep't of Educ., No. 2:11-cv-03471 (E.D. Cal. Mar. 29, 2013), 2013 WL 1326301 ("Examples of information that is stored on CDE's databases and network drives includes *name, social security number,* home address, demographics, course information, statewide assessment results, teacher demographics, program information, behavior and discipline information, progress reports, special education assessment plans, special education assessments/evaluations, Individualized Education Programs (IEPs), records pertaining to health, mental health and medical information, student statewide identifiers (SSID), attendance statistics, information on suspensions and expulsions, and results on state tests.") (emphasis added).

192 *See* Order at 5:25-6:7, Morgan Hill Concerned Parents Ass'n v. Cal. Dep't of Educ., No. 2:11-cv-03471 (E.D. Cal. Mar. 1, 2016), ECF No. 164.

193 *See generally supra* note 189.

194 *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1139 (2002) ("States maintain records spanning an individual's life from birth to death, including records of births, marriages, divorces, professional licenses, voting information, worker's compensation, personnel files (for public employees), property ownership, arrests, victims of crime, criminal and civil court proceedings, and scores of other information. Federal agencies maintain records pertaining to immigration, bankruptcy, social security, military personnel, and so on. These records contain personal information including a person's physical description (age, photograph, height, weight, eye color); race, nationality, and gender; family life (children, marital history, divorces, and even intimate details about one's marital relationship); residence, location, and contact information (address, telephone number, value and type of property owned, description of one's home); political activity (political party affiliation, contributions to political groups, frequency of voting); financial condition (bankruptcies, financial information, salary, debts); employment (place of employment, job position, salary, sick leave); criminal history (arrests, convictions, traffic citations); health and medical condition (doctors' reports, psychiatrists' notes, drug prescriptions, diseases and other disorders); and identifying information (mother's maiden name, Social Security number).").

ing of the privacy interest (and other considerations) must still be made against the needs of the case. High costs for redaction may lead a court to order that less data be released, no data be released, or another privacy protection option be employed.

2. *Order the Least Amount of Data Necessary*

Perhaps the most underused tool for judges is to demand that the requesting party demonstrate how data will be used. In other words, the court can ask for an expert to explain: why this data? Would less (fewer details or a smaller dataset) do? Would a less sensitive proxy suffice? For example, in the *Morgan Hill* case, the total population of school children data for a set time period was ordered for release—an estimated ten million records.[195] By "total population" it meant each and every student that fell in that category. However, rarely do empiricists have all the data they want. Therefore, empiricists have spent decades designing strong, reliable empirical models that produce reliable results using just a sampling of the total population. To be sure, in general, data is like chocolate, more is better than less. However, there are competing interests that must be weighed. Highly sensitive data can and should be released "proportionate to the needs of the case." It is incumbent on the requesting party to show they *need*—not merely desire—the requested data. This permits a judge the option to compel a subset of a large, sensitive dataset. Although this may fail to protect the data of those who fall into the "sample," it will at least protect the privacy interest of those outside the sample. It also may reduce the costs of redaction so that even the "sample" is better protected.

3. *Provide Affected Individuals an "Opt-Out" Option*

When third-party privacy interests are implicated, a judge may consider providing third parties an opt-out option. The benefit of the "opt-out" is that individuals vary greatly as to the importance they ascribe to personal privacy.[196] An opt-out permits the privacy-concerned individual to self-identify this preference.[197] The opt-out also permits a judge to adjust a

---

195 *See* discussion *infra* Part V.

196 In the case of children, it is even more pronounced as a child lacks the legal capacity to consent and parents must make the privacy choice on the child's behalf.

197 Opt-out regimes may be complex and expensive, and a deciding judge who herself is privacy-unconcerned may not see the need (or benefit) in requiring this option. To bring the issue home to a privacy-unconcerned judge, one commentator suggests that the judge be required to reveal her own data (including it in the

discovery order if a greater privacy interest is revealed than the judge had anticipated. Judges themselves have privacy preferences and, left to their own internal gauge, may grossly miscalculate the privacy interests at stake. Perhaps the most intuitive way for parents to protect their child's information would be to "opt-out" of the judicial order—to declare that their own child's records cannot be released. Interestingly, the opt-out option was not in place for affected students in the *Morgan Hill* case.[198]

However, the opt-out is a suboptimal solution at best. First, there are costs and administrative difficulties that may prevent truly effective notice to all potentially affected third parties. Second, asking individuals to self-identify in order to opt-out may, in and of itself, reveal identifying information to the court that the truly privacy-concerned would hesitate to send.[199] Finally, an opt-out may not even be an option if the data requested is "proportionate to the case."

---

order) when she permits discovery of others' data. To be sure, this may be an effective means of stressing the importance of the privacy interest. However, a tenured (Article III) judge whose job will not suffer with the exposure of personal information may not fully appreciate the impact such a release might have on the common citizen.

198 *See* Theresa Harrington, *Ability to Opt Out Uncertain in Lawsuit Requiring Student Data Release*, EDSOURCE (Feb. 18, 2016), https://edsource.org/2016/ability-to-opt-out-uncertain-in-lawsuit-requiring-student-data-release/95043 [https://perma.cc/GH8S-CBCM] ("The way we're interpreting it is: 'Get your paperwork in now and the court is going to decide whether that is an opt-out or not,' . . . . 'So, we strongly encourage everyone to get their paperwork in because the judge will make that determination.'") (quoting Robert Oakes, spokesman for the California Department of Education).

Compare supra note 24 *with* note 198. The objection form in the first source allows those who file it to preserve their privacy rights and enforce them in the event their files are disclosed unlawfully, but it is no guarantee that the files will not be disclosed. In fact, the court has denied a petition to stay disclosure of the students' records despite the pending litigation regarding the legality of that ordered disclosure. If it is determined that the order is overbroad and therefore invalid, only those who filed the objection form may have the ability to bring a civil action to assert their breached privacy right.

199 Again, as an example of a policy antithetical to individuals' privacy interest, the *Morgan Hill* judge did not give an "opt-out" option but rather set up a "complaint" system. To file a complaint, the name of the child, name of parent or guardian, school district and years of attendance had to be entered. The court required it to be mailed which is inconvenient, yes, but not a bad, low-tech means of protecting data (if the hard copy is managed well, under seal, etc.). However, so many complaints were filed that the judge urged other judges to set up an electronic filing—this may be problematic if not properly guarded.

C. Step Three—Promote Cybersecurity

In recent months, hackers are hitting well-known law firms[200]—a reminder that a protective order does not protect data from outside threats. A judge should enter each judicial order with the mindset that the data compelled will be data at risk. Data can be compromised by high-tech hacker attacks in the cloud or by the low-tech loss of a laptop or flash drive. A judge cannot, and should not, however, try to become a cybersecurity guru.

In addition to limiting the exposure of data in the first place,[201] a few additional, threshold cybersecurity strategies for judicial orders are needed. These may include a combination of the following: (a) assign a special master; (b) limit the number of people with access to the data; (c) keep data under the defendant's security protections; limit the electronic transfer and storage of data; and (d) use "under seal" and protective orders liberally but rely on them as warnings rather than effective cyber protections.

1. *Assign a Special Master*

As discussed above, assigning a special master to supervise the discovery process is well-known to judges and may be of particular importance when a large, sensitive dataset is at stake. In choosing a special master, technological expertise is as important in such a case as is legal acumen—arguably more so. But a special master of a large case may not be best suited to protect, or even see, the privacy issues at stake. Therefore, the judge may wish to provide strict guidance on privacy matters or appoint a "privacy master" tasked with protecting unrepresented third-party privacy interests. In particular, any special master should apprise the judge of difficulties in protecting the privacy interests outlined by the judge in Steps One and Two. For example, if redaction as ordered becomes problematic, the judge may have to rebalance the original order.

---

200 *See* Hong & Sidel, *supra* note 161, at 2.

201 The first strategy, limit the data exposed, is of course just an application of Step One set forth above. It is the most effective of cybersecurity strategies, if the court does not order the data disclosed, then the court has no cybersecurity interest in it. Of course the data may be unsecure as held by the non-requesting party. That is a problem between the data holder and the data owner. That is irrelevant to this calculus. As a defender of the public trust and the status it is granted, the court has a heightened obligation to consider the interests of nonconsenting parties.

2. *Limit the People with Data Access*

Limiting the number of people with access to the data is also important. Certain people have the right to access data—the requesting party being the obvious rightsholder. However, it might be useful to limit access by non-essential people. For example, the requesting party may be working with a law firm but the entire law firm does not need blanket access to the data.

3. *Keep Data Under Producing Party's Security Controls; Limit the Electronic Transfer and Storage of Data*

Part of the problem with the electronic transfer and storage of data is that multiple copies and potential points of access and leakage are created. As a practical matter, data need not have a "location" in the simple sense of the word. In fact, engineers may design redundant systems that separate data (even individual data) and store them in various locations. A rough analogy would be ripping a page of information in half and storing each half in a different location; to retrieve data, a decryption code can be used to bring together the two halves for a full picture.[202]

Arguably, defendant and plaintiff may have different storage locations and different security measures. If defendant is a private sector entity, then it can be reasonably assumed that individuals voluntarily gave their information to the defendant knowing (or trusting) the security measures defendant employed. Keeping these security measures at the status quo would mean that the individual's privacy protections are no less than those which he or she initially bargained for. A judge may therefore condition plaintiff's access to defendant's data to on-site access at the defendant's offices or other data access point. In the *Morgan Hill* case, for example, plaintiffs were wisely limited to data queries, rather than full data access. Plaintiffs presented the queries to defendant who then could run the query on defendant's own data systems.[203]

---

202 *See* Ariel Rabkin, *Data Need Not Have Location*, AEIDEAS (Mar. 2, 2017, 6:00 AM), http://www.aei.org/publication/data-need-location/ [http://perma.cc/3T4R-4PH3] (proposing that, in general, United States cybersecurity policy should focus on capabilities, not location) ("A good rule would say something like 'data should not be transferred in such a way that the recipient can extract the following particular private aspects' or 'data must be stored securely in such a way that unauthorized parties cannot learn the plaintext.'").

203 *See* Order at 6:16–24, Morgan Hill Concerned Parents Ass'n v. Cal. Dep't of Educ., No. 2:11-cv-03471 (E.D. Cal. Mar. 1, 2016), ECF No. 164.

To the extent this is not viable, the special master may carefully detail how data or data results be transferred, stored, and destroyed by secure methods for additional protection.

4. *Reliance on Filings "Under Seal" and Protective Orders as Warnings Only*

In the digital age, a court's protective order, or an order to place a filing "under seal," is not what it used to be. A court's sole reliance on a protective order to guard sensitive electronic data is, in fact, a dangerously outdated notion. Protective orders are an important legal device in the protection of data; they clarify the importance of handling sensitive information with care. But, for example, the *Morgan Hill* protective order states that all the records used by plaintiffs are to be "destroyed" when no longer needed,[204] demonstrating a lack of understanding of how digital data can rapidly spread to a multitude of platforms quickly, making it extraordinarily difficult to "destroy." Moreover, it is small comfort that "only the lawyers will have access" to data. First, this is not entirely accurate as a matter of law—plaintiffs, plaintiffs' lawyers, and plaintiffs' experts are all permitted access to data as may be required by the case. Second, if not properly controlled, data transfers from defendant to plaintiff potentially may be stored in several locations—the respective clouds used by each user, servers of various users, etc.—each independently susceptible to attack or inadvertent leak.

V
MORGAN HILL—A CAUTIONARY EXAMPLE

As a case study for judicial discovery orders of highly sensitive data, this Article examines the current, ongoing California case *Morgan Hill Concerned Parents Ass'n v. California Dep't of Educ.*[205] This particular case exemplifies the need for judges to actively limit the size and scope of discovery based on a proportionality standard. In this case, the judge took a more passive role and merely approved the litigants' discovery agreements.[206] As a result, the *Morgan Hill* judge has ordered an

---

204 *See* Order at 14:25–27, *Morgan Hill*, No. 2:11-cv-03471 (E.D. Cal. May 5, 2016), ECF No. 60 ("Within 60 days after the final disposition of this action . . . each Receiving Party must return all Protected Material to the Producing Party or destroy such material.").

205 Morgan Hill Concerned Parents Ass'n v. Cal. Dep't of Educ., No. 2:11-cv-03471, 2013 WL 1326301 (E.D. Cal. Mar. 29, 2013).

206 The plaintiffs and defendants had a dispute regarding the production of certain discovery requested by the plaintiffs, and the plaintiffs moved to compel

estimated ten million students' full records to be disclosed, relying more on the secondary protections of a protective order than the primary protections that only discovery limits can provide.[207]

More than a year later, the court issued another order regarding the disclosure of information in compliance with an agreement between the parties. In conjunction with that order, the court issued a notice of disclosure. The court acknowledged that:

> [e]xamples of information that is stored on CDE's databases and network drives includes name, social security number, home address, demographics, course information, statewide assessment results, teacher demographics, program information, behavior and discipline information, progress reports, special education assessment plans, special education assessments/evaluations, Individualized Education Programs (IEPs), records pertaining to health, mental health and medical information, student statewide identifiers (SSID), attendance statistics, information on suspensions and expulsions, and results on state tests.[208]

Still, despite the clearly sensitive nature of that information, the court did not exclude any of that information from the discovery request.[209] Instead, the court determined that the protective order was satisfactory to protect the privacy interest.[210] Specifically, the court found that the educational records "could be disclosed, in one form or another, as long as parents or students are notified of the disclosure by publica-

---

production of that discovery. *See* Order, *Morgan Hill*, No. 2:11-cv-03471-KJM-AC (E.D. Cal. Oct. 1, 2014), ECF No. 64. Although the court denied the plaintiffs' motion to compel, the record makes clear that the court was actually confirming an agreement made between the parties during the interim of the motion to compel and the court's ruling on that motion. Order at 2:16-3:19, *Morgan Hill*, No. 2:11-cv-03471-KJM-AC (E.D. Cal. Dec. 16, 2014), ECF No. 85. The parties agreed that the data would be produced "in a manner to allow plaintiffs to track students, to the maximum extent feasible, wherever they are identified throughout defendant's electronic databases." *Id.* at 2:17-19.

207 *Id.* at 1:20-27; *see also* Order at 7:7-9, *Morgan Hill*, No. 2:11-cv-03471-KJM-AC (E.D. Cal. July 2, 2015), ECF No. 116 ("Here, there is a protective order in place governing the disclosure of confidential information. (ECF No. 60.) That order is adequate to ensure the information disclosed is not disseminated to others.").

208 Notice of Disclosure of Student Records, *Morgan Hill*, No. 2:11-cv-03471-KJM-AC (E.D. Cal. Mar. 1, 2013), 2013 WL 1326301.

209 *See id.*

210 *See* Order, *Morgan Hill*, No. 2:11-cv-03471-KJM-AC (E.D. Cal. Mar. 1, 2016), ECF No. 164.

tion and a protective order restricts the use of the information to this litigation only."[211]

At the encouragement of her appointed special master, the Judge amended this part of the order to keep the most sensitive data set (CALPADS) on site with the defendant (the California Department of Education), provided that Defendant assist Plaintiff in running their requested data queries. This on-site query option is an improvement over a blanket data-transfer order and an option more consistent with the protective procedures set forth in this Article. It should be noted, however, that although the Judge later ordered that the CALPADS data stay on site with the California Department of Education,[212] there are still strong privacy and cybersecurity concerns left unaddressed.

The court in this case clearly considers the information sensitive enough to require a protective order and a special master, but seems not to appreciate that those protections are unlikely to adequately protect the privacy interests at stake. The privacy interest is best protected by narrowing the scope and redacting information, and protective orders and special masters should be used as a final layer of protection once the discovery request has been whittled down to the information reasonably essential to the case. Where, as here, the digital discovery is sensitive information concerning minors, the privacy interest deserves even greater consideration than the traditional use of protective orders and special masters.

Again, the court did not consider fully the privacy interest of affected parties—especially third-parties—when deciding to compel disclosure of private information in the first place. As set forth in subpart II.A of this Article, if the burden outweighs the benefit, then the discovery request should be denied in totality.[213] In turn, if the information is reasonably essential to the case, then the privacy interest should be reconsidered to limit the scope of the request only to the information that is required.[214] That was not done in this case and, as a result,

---

211 *Id.* at 4:23–25 (quoting ECF No. 116) (internal quotation marks omitted).

212 *Id.*

213 *See, e.g.*, Appler v. Mead Johnson & Co., LLC, No. 3:14–cv–166–RLY–WGH, 2015 WL 5615038, at *6 (S.D. Ind. Sept. 24, 2015) (declining to compel the production of entire categories of data from a Facebook profile due to the privacy burden outweighing the relevance to the case).

214 *See* Ragusa v. Malverne Union Free Sch. Dist., 549 F. Supp. 2d 288, 294–95 (E.D.N.Y. 2008) (narrowing the scope of the requested discovery to only those math students that Plaintiff taught during the time period at issue).

the most personal information of an entire generation of California children is unnecessarily vulnerable.[215]

VI
A PIGOVIAN TAX FOR GOVERNMENT COLLECTED DATA

Obviously, the best way for information recipients to protect sensitive data is to not collect sensitive data. For instance, in the *Morgan Hill* case, if the defendant, the California Department of Education, had insisted that school districts not report social security numbers of children (for example) in the first instance, then the data would not exist for the judge to compel in discovery.[216]

Ironically, the Eastern District of California follows a similar limiting principle. The Eastern District publishes its own rules for evidence that is to be filed to the court[217] and specifically requests that complete social security numbers are not filed with the court.[218] The court rightly identifies this information as too sensitive, and not sufficiently useful, for the court to hold.

But as discussed earlier, it is difficult to incentivize government entities to be circumspect in the collection of data.[219] Government entities are more difficult than private entities to sue in tort. Alternatively, government entities, unlike private entities, face no reputational effects (brand risk) to incent cautionary data collection and protection investments. To bolster privacy protections in government data collection, it would be useful to create a statutory right to information privacy.[220] For

---

215 *See* Order at 5:24–7:5, *Morgan Hill*, No. 2:11-cv-03471 (E.D. Cal. March 1, 2016), ECF No. 164.

216 This is a bit tricky as the social security numbers of special education students are used to coordinate data across several government agencies. This practice is now being corrected in recognition of the sensitivity of this data. *See* Cal. Assemb. A.B. 2097, 2015–2016 Reg. Sess. (Cal. 2016) (drafting an act to repeal the schools' authority to collect and solicit social security numbers and authorizing the schools to create individualized student identification numbers).

217 *See generally Local Rules of the United States District Court*, E.D. CAL. (effective Jan. 1, 2015), http://www.caed.uscourts.gov/caednew/assets/File/EDCA%20Local%20Rules%20Effective%201-1-15.pdf [https://perma.cc/H76N-5KRJ].

218 *Id.* at Rule 140 (requiring all but the last four digits of a social security number, all but the last four numbers of a financial account number, and all but the year in someone's birthdate to be redacted in documents filed with the court, and also requiring children's names to be abbreviated and home addresses to be limited depending on the type of action).

219 *Supra* subpart I.C.

220 As mentioned several times, in limited circumstances, some statutory protections already exist. However, even in these areas, adding a cause of action for

any such right to have a disciplining impact, the breach of it by a government agency must carry a penalty—a Pigovian tax on the overcollection and underprotection of data might be a good start.[221]

A good legal moment to exercise such a right is within the discovery context—to incentivize (or defray the costs for) interested third parties to intervene in a litigation and protect their own interests. The legal action might be "wrongful disclosure" and would carry a fixed fine if found valid.[222] Although full development of such a regime is beyond the scope of this Article, a bare-bones framework may include the following.

The goal of a wrongful disclosure claim would be two-fold: (1) to incentivize the government to invest in vigorous discovery defenses when they arise and (2) to invest in cybersecurity measures for the data collected. As a corollary, a "wrongful disclosure" claim might be effective in limiting government overcollection of data—whether actually disclosed or not. In the discovery context, an ancillary "overcollection" claim would be easy to add to a wrongful disclosure cause of action. For example, if the agency wrongfully disclosed the information but collected the least amount necessary to meet their mandated task, then the agency is liable for X damages. If, however, the agency wrongfully disclosed the information *and* collected more than was necessary to meet their mandated task, then the agency is liable for X + Y damages.[223]

Again, government collection of data is particularly problematic because of the coercive nature of such information requests. It is also problematic because of the unique disclosure obligations of government under the various sunshine acts. At the very least, incenting agencies to carefully match data requests with the entities' data needs would help reduce the

---

the breach of the statute and for any general overcollection of data would assist in the self-disciplining of government record collection.

221 A Pigovian tax is described in Wikipedia as "a tax on any market activity that generates negative externalities (costs not included in the market price). The tax is intended to correct an inefficient market outcome, and does so by being set equal to the social cost of the negative externalities." *Pigovian Tax*, WIKIPEDIA, https://en.wikipedia.org/wiki/Pigovian_tax [https://perma.cc/Q5X9-XNX7] (last modified Feb. 21, 2017).

222 To incent vigorous protection of third-party interest, a wrongful disclosure claim would include failure to properly limit the scope of disclosure of private information to plaintiffs. In other words, disclosure to the public at large would not be a necessary element to setting forth a valid claim.

223 It may also be desirable to hold the government strictly liable for overcollection of sensitive data as a standalone cause of action, but again, that is outside the scope of this Article.

number of involuntary transactions in which the privacy-conscious must participate.[224]

CONCLUSION

With each new privacy "crisis"—from the Snowden revelations to the FBI Apple tangle, and Facebook data exposures to whatever is next—the larger issue revealed is that privacy law is behind the technology curve. Information has never been more accessible, transferable, or vulnerable, and the law provides inadequate protection. The Supreme Court has not yet found a constitutional right to information privacy, the few statutes that seek to protect private information are riddled with exceptions, and the tort regime severely limits a plaintiff's ability to recover for wrongfully disclosed information, especially when the government is the defendant.

The revision of the Federal Rules of Civil Procedure has made strides to protect information from extraneous discovery, but to incentivize socially optimal levels of informational privacy, constitutional, statutory, and tort common law need to adapt. Judges play a privileged role in our society as exemplified by the incredible trust we grant them to compel disclosure of private information to another, hostile party. What is proposed here is a simple, practical process to help judges balance affected parties' privacy interests and cybersecurity concerns against the need for trial discovery.

To recap, Step One is a "privacy screen" to determine the weight a court should give the privacy interest by considering the type of information requested, statutory protections for it, and the status (private or public) of the litigating parties. Step Two is to protect affected parties' privacy interests by employing three tactics to limit the exposure of sensitive data: (a) demand that data be redacted and/or aggregated to remove individual identifiers; (b) determine the least amount of data access that is "proportional to the needs of the case;" and (c) provide affected individuals an "opt-out" option.

Step Three is to employ four strategies to protect affected parties' cybersecurity interest: (a) assign a special master; (b) limit the number of people with access to the data; (c) keep data at the data provider's location; limit the electronic transfer and storage of data; and (d) use "under seal" and protective orders liberally, but rely on them as warnings rather than effective cyber protections.

---

224 *See* discussion *supra* subpart I.C.

In particular, due to the unique nature of government-collected data, the analyses in this Article demonstrate the need for strong judicial intervention when personal, sensitive government-collected data is at issue. Presently, public entities have little to no incentive to limit data collection, invest in cybersecurity measures and defend against broad discovery requests. In addition to judicial engagement in discovery, this Article suggests a new cause of action: a type of Pigovian tax on public entities that may help align the privacy interests of individuals with the data needs of government entities.

The good news is that the United States has a highly professional judiciary that is well-suited to adapt to the changing demands and dangers posed by an interconnected world. But in the digital era, the courts' essential gatekeeper role is magnified as one judge acting alone can destroy the privacy interests of millions. Following the framework presented here will not guarantee against privacy losses nor will it prevent all data spills, but it will hopefully raise awareness and the protective diligence of all concerned parties. Moreover, there is no doubt that it is time to recalibrate our privacy regimes from a data protection emphasis to a data limitation emphasis. Hopefully the analyses presented in this Article will be of use in changing how we adjust statutory and judicial privacy protections to the modern realities of the Internet and era of big data.