NOTE*

INSTITUTIONALLY APPROPRIATE APPROACHES TO PRIVACY: STRIKING A BALANCE BETWEEN JUDICIAL AND ADMINISTRATIVE ENFORCEMENT OF PRIVACY LAW

I. INTRODUCTION

Americans are sharing more personal information than ever before. A majority of U.S. adults bank online[1] and use social networking.[2] A growing minority of Americans share their political views via social media.[3] A significant minority of Americans share images and videos that they produce themselves.[4] Some even track their health information using technology.[5] Despite this trend, studies show little or no change in American attitudes about the importance of data privacy.[6] Americans think data privacy is of great import and worry about its continued protection in the digital age.[7] Studies show a pattern of powerlessness of the average online American to achieve her preferred level of privacy, due to a combination of ignorance of

---

[1] Susannah Fox, *51% of U.S. Adults Bank Online*, PEW RES. CTR. (Aug. 7, 2013), http://www.pewinternet.org/Reports/2013/Online-banking/Findings.aspx, *archived at* http://perma.cc/0ahZL2ZwJcb/.

[2] Joanna Brenner & Aaron Smith, *72% of Online Adults are Social Networking Site Users*, PEW RES. CTR. (Aug. 5, 2013), http://www.pewinternet.org/Reports/2013/social-networking-sites.aspx, *archived at* http://perma.cc/0AKm6n4vB72.

[3] Aaron Smith, *Civic Engagement in the Digital Age*, PEW RES. CTR. (Apr. 25, 2013) ("17% of all adults posted links to political stories or articles on social networking sites, and 19% posted other types of political content. That is a six-fold increase from the 3% of adults who posted political stories or links on these sites in 2008."), http://www.pewinternet.org/Reports/2013/Civic-Engagement.aspx, *archived at* http://perma.cc/091i5tY8BHR. Furthermore, those who share political content have outsized influence. During the 2012 election season, fifty-two percent of registered voters reported that other people had suggested political videos for them to view, with social media playing an important role in the distribution of videos. Aaron Smith & Maeve Duggan, *Online Political Videos and Campaign 2012*, PEW RES. CTR. (Nov. 2, 2012), http://www.pewinternet.org/Reports/2012/Election-2012-Video.aspx, *archived at* http://perma.cc/0tJuAi2vgcq/.

[4] Lee Rainie, Joanna Brenner & Kristen Purcell, *Photos and Videos as Social Currency Online*, PEW RES. CTR. (Sep. 13, 2012), http://www.pewinternet.org/Reports/2012/Online-Pictures.aspx, *archived at* http://perma.cc/0uctGBwKBYd/.

[5] Susannah Fox & Maeve Duggan, *Tracking for Health*, PEW RES. CTR. (Jan. 28, 2013), http://www.pewinternet.org/Reports/2013/Tracking-for-Health.aspx, *archived at* http://perma.cc/0RLpD1UswHS/.

[6] *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 83 (2010) (citing studies from the past twenty years in which consumers affirm that privacy is important to them).

[7] *See* Lee Rainie et al., *Anonymity, Privacy, and Security Online*, PEW RES. CTR. 2 (Sept. 5, 2013), http://www.pewinternet.org/~/media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf, *archived at* http://perma.cc/0kgnC5VNUnq/.

the scope of data revelation and a lack of tools available to protect her privacy meaningfully.

Americans are likely to think that social media companies offer more data privacy protections than they actually do.[8] Young adults are particularly likely to be so mistaken.[9] Americans' confusion may result from how data privacy policies are marketed. Companies often summarize their data privacy policy as a series of services for the user's benefit without making clear what value the company is getting from the consumer's personal information. For example, Twitter's privacy policy states, "Our Services are primarily designed to help you share information with the world."[10] Google's privacy policy states, "We collect information to provide better services to all of our users . . . ."[11] These statements probably mislead users into assuming companies offer protections that do not, in fact, exist.

Americans feel discomfort with industry practices despite continued market engagement with products that tend to expose more user data to companies and to the general public, but have been frustrated in their efforts to protect their data privacy. Users act upon their privacy concerns in large numbers. Eighty-six percent of adults have taken steps to avoid surveillance when using the Internet.[12] In spite of these precautions, twenty-one percent of adult internet users have had personal email or social media accounts compromised and eleven percent have had sensitive data, such as Social Security numbers and financial information, stolen.[13] For these and other reasons, sixty-eight percent of Americans think that current laws fail to protect individuals' online privacy adequately.[14]

Commentators have suggested that the market undersupplies data privacy protections.[15] Consumers cannot accurately value their personal information when they do not understand the terms by which they exchange it for services. In George Akerlof's classic analysis of the market for used cars,[16]

---

[8] Chris Jay Hoofnagle et al., *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?* 20 (Apr. 14, 2010) ("We suggest, then, that young-adult Americans have an aspiration for increased privacy even while they participate in an online reality that is optimized to increase their revelation of personal data."), http://www.ftc.gov/os/comments/privacyroundtable/544506-00125.pdf, *archived at* http://perma.cc/0i1FKegWC1D.

[9] *Id.* at 18 ("We found that while young adults tend to be similar to older adults in attitudes, practices, and policy preferences regarding information privacy, they are quite more likely than older adults to be wrong in judging whether the legal environment protects them.").

[10] TWITTER PRIVACY POLICY, https://twitter.com/privacy (last visited Oct. 23, 2013), *archived at* http://perma.cc/0cKnBjZmqpy?type=image.

[11] GOOGLE POLICIES & PRINCIPLES, https://www.google.com/intl/en/policies/privacy/, *archived at* http://perma.cc/0m7YvgJyWJW/ (last visited Oct. 23, 2013).

[12] Rainie et al., *supra* note 7, at 2.

[13] *Id.*

[14] *Id.*

[15] *E.g.*, Pamela Samuelson, *Privacy As Intellectual Property?*, 52 Stan. L. Rev. 1125, 1127 (2000) (rehearsing a similar argument to the one this paper makes to illustrate the utilitarian argument for greater privacy protection).

[16] *See generally* George Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q. J. of Econ. 488 (1970).

he observed that where possible, sellers conceal unflattering information about products from buyers, causing the buyers to overvalue flawed products. This practice removes the competitive advantage in creating products without the hidden flaw.[17] As a result, no seller will have the incentive to place non-flawed products on the market.[18] Akerlof's theoretical outline corresponds with the actual industry tendency to sugarcoat or even misrepresent data privacy policies. The data-gathering company has an incentive to conceal or deemphasize its personal information collection practices, which otherwise may discourage consumers from providing personal data.

Typically, consumers cannot differentiate between a product or business practice that has strong data security and privacy provisions from one lacking such provisions.[19] Consumers who desire greater privacy protections thus will be unable to select and pay more for a product that is better in that respect.[20] Therefore, market actors do not have an incentive to provide such products. In this way, products and business practices with stronger privacy protections are driven from the market. These considerations offer a utilitarian ground to doubt the theory that the relative lack of privacy-protecting products and business models indicates public indifference to privacy and shows that the public would benefit from stronger enforcement of privacy protections at law.[21]

---

[17] *Id.* at 495.

[18] *Id.*

[19] *See* Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RES., no. 2, June 2011, at 254 (showing that privacy information about online applications is often invisible to consumers, but "when privacy information is made more salient and accessible," some consumers would be willing to pay higher prices to purchase from websites that better protected their privacy), *available at* http://guanotronic.com/~serge/papers/isr10.pdf, *archived at* http://perma.cc/0VrhFZkb2zD/. The low popularity of more secure social networking options such as Diaspora and Identi.ca suggest that information about privacy protections accorded by social media platforms remains unknown to all but the most savvy of consumers. *See* April Glaser & Libby Reinish, *How to Block the NSA from Your Friends List*, SLATE, (June 17, 2013, 11:12 AM) (estimating use of Identi.ca at about 1.5 million, compared to Facebook's 1 billion), http://www.slate.com/blogs/future_tense/2013/06/17/identi_ca_diaspora_and_friendica_are_more_secure_alternatives_to_facebook.html, *archived at* http://perma.cc/0LBqcRNt77T/. Fifty-nine percent of Internet users are resigned to the view that it is not possible to be completely anonymous online. *See* Rainie et al., *supra* note 7, at 2. The latter attitude reduces consumers' incentives to aggressively seek out services that protect privacy.

[20] *Cf.* Riccardo Bonazzi et al., *Business Model Considerations for Privacy Protection in a Mobile Location Based Context* (Fourteenth Int'l Conf. on Intellig. in Next Generation Networks, 2010) (discussing privacy protection as a main value proposition, with business models based on monetizing privacy contingent on consumer knowledge of privacy controls), *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5640885, *archived at* http://perma.cc/0LaWH1LozqT/.

[21] *But see* Marshall Kirkpatrick, *Facebook's Zuckerberg Says the Age of Privacy is Over*, READWRITE (Jan. 9, 2010) (recapping Facebook founder Mark Zuckerberg's argument that because of changing social norms and consumer demand to share, Facebook is trending toward less options for privacy), http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov#awesm=~om56538dIc3y3q, *archived at* http://perma.cc/09qenVngCX2?type=live.

It would be a difficult task to craft regulations to correct the pervasive information asymmetries in the market for data privacy. That is not the project of this paper. Instead, I argue for a distribution of enforcement authority between the courts and the Federal Trade Commission ("FTC" or "the Agency") that would more vigorously and predictably protect a scope of personal privacy defined by law. The FTC should be the forum where corporate data privacy practices are balanced against the general public interest in data privacy, with a view toward striking the balance that maximizes overall societal utility. At the same time, courts should take a more active role in resolving disputes that concern whether one person has infringed the right of another, with the support of state administrative agencies specifically tasked with resolving these types of disputes.

In Part II, I summarize the current shape of the privacy torts at common law, and illustrate the promise of adjudicative reasoning for handling data privacy cases. I will suggest that ossified privacy torts used in most states are unable to address modern problems of data privacy.

Part III describes the source of the FTC's authority to regulate unfair and deceptive trade practices and summarizes the history of the FTC's enforcement of privacy matters. I then argue that holding companies responsible for transacting personal information with consumers in a way that accords with their reasonable expectations underlies the FTC's three recent consent orders with major companies Facebook, Google, and Twitter. Like the determinations of the scope of reasonable expectations and consent at common law, the FTC's judgments are guided by judgments about what distribution of rights would be best for society at large.

Part IV argues that the FTC's enforcement approach is best suited for matters that tend to balance the interest of a class of people in having control over personal information against others who wish to provide some other service using the private data. Adjudicative proceedings, by contrast, are best suited to approaches to privacy involving determinations of whether one party has a duty to respect the other's privacy claim. The article then proposes that states broaden the scope of data privacy claims and create agencies to assist state courts in adjudicating those claims. The section goes on to discuss some implications and further issues presented by the argument.

II. Privacy at Common Law

In this section, I trace the development of the four privacy torts and illustrate the unique advantages of common law adjudicative reasoning for resolving two-party disputes. The hallmark of judicial reasoning is operating on the basis of rules of consistent application, and applying those rules to the facts of particular cases.[22]

---

[22] Prentis v. Atl. Coast Line Co., 211 U.S. 210, 226 (1908) ("A judicial inquiry investigates, declares, and enforces liabilities as they stand on present or past facts and under laws

Louis Brandeis and Samuel Warren provided the first modern restatement of privacy common law in their famous article *The Right to Privacy*.[23] Brandeis and Warren described privacy, the "right to be let alone," as a broad, unitary right stemming from a person's "inviolate personality."[24] They stressed the importance of a flexible common law standard to meet the needs of changing technology.[25] Warren and Brandeis did not purport to define the privacy tort for every circumstance. Rather, the authors noted that courts had started to deem the viewing and use of others' space and data as tortious.[26] They presumed that courts could continue resolving spatial and data privacy disputes on a case-by-case basis.

Writing half a century later, William Prosser sought to limit the privacy tort and provide clear, bright-line standards.[27] Prosser disclaimed privacy as a single, broad, ideal in favor of four relatively distinct causes of action: "1. Intrusion upon . . . seclusion or solitude, or . . . private affairs. 2. Public disclosure of embarrassing private facts . . . . 3. Publicity which places [a person] in a false light . . . . 4. Appropriation, for the defendant's advantage, of . . . name or likeness."[28] Prosser purposely tied the elements of the torts to specific common facts in the privacy cases up to 1960. These four privacy torts have been included in the Restatement of Torts and are the law in many jurisdictions.[29]

Edward Bloustein, a contemporary critic of Prosser, argued that the specific and separate character of the four privacy torts would hamper the ability of privacy tort law to respond in an agile fashion to technological change.[30] Without a central, animating principle, the case law would struggle to evolve beyond the facts of the disputes Prosser recounted in his article. By contrast, Bloustein argued that the core value motivating privacy protections at common law was human dignity.[31]

Contemporary scholars continue to critique the four privacy torts for being insufficiently responsive to changes in societal and cultural circum-

---

supposed already to exist. . . . Legislation . . . looks to the future and changes existing conditions by making a new rule, to be applied thereafter to . . . those subject to its power.").

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

[24] *Id.* at 193–95, 205.

[25] *Id.* at 193. ("Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.").

[26] *Id.* at 195, 198–200.

[27] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 423 (1960). ("[I]t is high time that we realize what we are doing, and give some consideration to the question of where, if anywhere, we are to call a halt [in expanding the domain of privacy law].").

[28] *Id.* at 389 ("The law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff . . . .").

[29] RESTATEMENT (SECOND) OF TORTS §§ 652B–652E (1977); *see, e.g.*, Machon v. Pa. Dep't of Pub. Welfare, 847 F. Supp. 2d 734, 750 (E.D. Pa. 2012) (noting that Pennsylvania courts have adopted the Restatement's four invasion of privacy torts).

[30] Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 1004–07 (1964).

[31] *Id.* at 974 (breaches of privacy wreak "a blow to human dignity, an assault on human personality").

stances. New technologies that enable corporations, government, and even individuals to obtain and use personal data easily are chief among these changed circumstances that the current privacy tort framework lacks the plasticity to take into account. According to Neil Richards and Daniel Solove, Prosser's work ossified privacy at common law,[32] thereby limiting privacy tort doctrine's ability to respond to changing times. In fact, as Lior Strahilevitz argues, modern courts have replaced the four privacy torts with a less structured balancing approach:

> [T]here have been many opportunities presented for judges to address [data privacy] problems via tort rules . . . . [I]n the majority of cases, the courts have understood themselves to be junior partners to legislators and regulators in dealing with new privacy challenges. The possibility that legislators might want to legislate has convinced the courts to stop innovating through common law. And the unwillingness of judges to modernize tort protections to deal with new challenges has prompted legislators in turn to legislate in ad hoc, often incoherent ways.[33]

In the past two decades, a handful of cases have exemplified common law courts' handling of data privacy cases in the digital age. In these cases, courts constructed the harm stemming from commercial uses of personal data to which consumers did not consent in a highly constricted way.[34] Courts also went out of their way to observe that damages would be limited in data privacy actions.[35] These cases suggest that the litigant's likelihood of success in a data privacy tort action is low and that even successful data privacy litigants would likely win minimal damages. These decisions were

---

[32] Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1890 (2010).

[33] Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 CALIF. L. REV. 2007, 2034 (2010).

[34] *E.g.*, Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995) (holding that the use of consumer data to target third parties did not violate the intrusion upon seclusion or appropriation privacy torts because the defendants were not disclosing particular cardholders' financial information, and finding that "a single, random cardholder's name has little or no intrinsic value to defendants").

[35] *See, e.g.*, *In re* Jet Blue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005) (rejecting a hypothetical claim for damages based on "the loss of the economic value of their information" because "[plaintiffs] had no reason to expect that they would be compensated for the 'value' of their personal information . . . [and there is] no support for the proposition that an individual passenger's personal information has or had any compensable value in the economy at large."). Although this holding involved plaintiffs' breach of contract action, the court's rationale applies for limiting the availability of damages in privacy tort matters. A recent Third Circuit case also illustrated data privacy plaintiffs' limited ability to state a claim for injunctive relief or punitive damages. *See* Boring v. Google, Inc., 362 F. App'x 273, 279 (3d. Cir. 2010). Google eventually settled for one dollar with the plaintiffs, who had sued the company after discovering that a Google Street View camera car had been on their private driveway to photograph their home's exterior. Chris Davies, *Google Pays $1 Compensation in Street View Privacy Case*, SLASHGEAR (Dec. 3, 2010), http://www.slashgear.com/google-pays-1-compensation-in-street-view-privacy-case-03117450/, *archived at* http://perma.cc/0hnxYaP5qhR.

built on quite assailable analysis, but provide courts with precedent for staying out of the thicket of striking a balance between privacy claimants and corporations.[36]

III. Privacy and the FTC

In this section, I will first explain the scope of the FTC's authority. Then, I will describe how privacy enforcement actions have evolved over the past two decades. During the late 1990s, the FTC based its enforcement actions on a formalistic conception of notice. The FTC's recent consent orders with Facebook, Google, and Twitter represent a move towards considering a variety of factors in its enforcement actions that reflect the agency's judgments about what distribution of rights would be best for society. In the data privacy context, the competing interests of consumers and companies constitute a classic polycentric conflict. That is, the FTC's consent orders necessarily have a cascading impact on stakeholders besides the company that the consent order binds.[37] Lon Fuller argued that actors that can engage in managerial direction are particularly well-suited to handling polycentric disputes.[38] This is because the decision involves creating a principle in the first instance and has web-like ramifications for private and governmental actors. I argue here that the FTC's consent orders with companies in the area of data privacy more effectively address polycentric disputes.

A. The Source of the FTC's General Authority

The FTC derives its authority to prosecute companies for data privacy violations and issue enforcement guidelines from the Federal Trade Commission Act ("FTCA"). Congress "empowered and directed [the FTC] to prevent persons, partnerships, or corporations . . . from using unfair methods of competition . . . and unfair or deceptive acts or practices . . . ."[39] The statute's language thus confers upon the FTC broad authority to define unfair and deceptive trade practices and take enforcement actions against violators.

---

[36] *See, e.g.*, Andrew J. McClurg, *A Thousand Words Are Worth A Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 Nw. U. L. Rev. 63, 118 (2003) (discussing issues in the context of damages in data privacy cases, noting that "the value of the data profile of any particular individual is small and difficult to quantify . . . [and thus] requiring victims of consumer profiling to prove a specific monetary loss unwarrantedly prejudices their claims."); Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 Fordham L. Rev. 1305, 1318–19 (2001) (noting that court decisions could have extended privacy doctrines to cover modern data privacy infringements, but have mostly declined to extend privacy doctrines to cover those types of cases).

[37] *See* Lon L. Fuller, *The Forms and Limits of Adjudication*, 92 Harv. L. Rev. 353, 394–98 (1978) (defining polycentric tasks).

[38] *Id.* at 398.

[39] 15 U.S.C. § 45(a)(2) (2012).

In *Federal Trade Commission v. Sperry & Hutchinson Trading Stamp Co.*, the Supreme Court upheld a broad reach for the FTC's discretion.[40] The Court held that the FTC has the power to define unfair competitive practices and that the commission is empowered to "proscribe practices as unfair or deceptive in their effect upon consumers regardless of their nature or quality as competitive practices or their effect on competition."[41] The Court noted that at the time of writing the FTCA, Congress expressly chose "unfair and deceptive" over more specific language and cited a Senate Committee Report endorsing the view that "there were too many unfair practices to define, and after writing 20 of them into the law it would be quite possible to invent others."[42] Congress thus delegated broad authority to the FTC to decide what counted as unfair or deceptive. The Court also noted that, after the Supreme Court had interpreted the FTCA to be limited to contexts where competition was implicated, Congress adopted the Wheeler-Lea Amendment, which changed the language of the FTCA to "unfair or deceptive acts or practices" so it would clearly protect both consumers and competitors.[43] Congress thus reaffirmed its intent for the FTC to have broad discretion to define business practices that were unfair or deceptive, even if they had no effect on competition.

Finally the *Sperry* court held that Congress empowered the FTC to use the "elusive, but congressionally mandated standard of fairness . . . like a court of equity" considering "public values beyond simply those enshrined in the letter or encompassed in the spirit of the antitrust laws."[44]

The FTC primarily exerts its authority through adjudication.[45] When the FTC has "reason to believe" that the law is being violated by a company, the agency may issue a complaint setting forth its charges to the company.[46] The FTC occasionally uses rule-making, especially when tasked by a specific statute, such as the privacy rules promulgated in response to Congress's specific mandate in the Gramm-Leach-Bliley Act.[47]

Many FTC enforcement actions end in consent orders.[48] The consent agreement only formally binds the companies involved, but other industry

---

[40] FTC v. Sperry & Hutchinson Co., 405 U.S. 233 (1972).

[41] *Id.* at 239.

[42] *Id.* at 240 (quoting S. REP. NO. 63-597, at 13 (1914)).

[43] *Id.* at 244.

[44] *Id.*

[45] FED. TRADE COMM'N, A BRIEF OVERVIEW OF THE FEDERAL TRADE COMMISSION'S INVESTIGATIVE AND LAW ENFORCEMENT AUTHORITY (2008), *available at* http://www.ftc.gov/ogc/brfovrvw.shtm, *archived at* http://perma.cc/0HUhbxSnAsP/.

[46] *Id.*

[47] 16 C.F.R. § 313 (2013) (implementing privacy rules pursuant to the Gramm-Leach-Bliley Act).

[48] *See Legal Resources,* FED. TRADE COMM'N (listing data privacy and security FTC matters, most of which ended with consent orders), http://business.ftc.gov/legal-resources/48/35 (last visited Nov. 4, 2013), *archived at*, http://perma.cc/0UVXkZXituP.

players frequently observe consent agreements with great interest.[49] Thus, consent orders share common features with regulation, because industry responds to consent orders by seeking to avoid conduct too close to the facts that spurred the enforcement action. An agency's conduct must be in line with its previous actions unless it explains its change in policy.[50] If the FTC thus deviates from a pattern of conduct without a clear statement for its policy shift, a reviewing court may deem the agency's enforcement action arbitrary and capricious, because the party was insufficiently able to use the FTC's previous norms to guide its conduct.[51]

The FTC also issues enforcement guidelines as a method of carrying out its statutory duties. An enforcement guidelines document is "an agency statement of general applicability and future effect, other than a regulatory action, that sets forth a policy on a statutory, regulatory, or technical issue or an interpretation of a statutory or regulatory issue."[52] FTC enforcement guidelines indicate when the FTC is likely to find a "reason to believe" the law is being violated.[53] Enforcement guidelines thus give companies advance notice as to what conduct is likely to draw a complaint from the FTC, and allows them the opportunity to conform without being drawn into an enforcement action. The FTC has used enforcement guidelines to great effect in the context of antitrust enforcement actions. The FTC Horizontal Merger Guidelines, for instance, are widely referenced by antitrust lawyers in advising clients on how to shape their operations and employed by courts as persuasive authority in determining what activity is anticompetitive.[54]

B. Evolution of the FTC's Enforcement of Data Privacy

Using its broad authority under the FTCA, the FTC has initiated enforcement actions for deceptive and unfair trade practices in the context of data privacy. This section traces the evolution of the FTC's criteria for initiating enforcement actions over the past two decades.

---

[49] *See* Altria Group, Inc. v. Good, 555 U.S. 70, 89 n.13 (2008); *see also In re* Google, Inc., No. 1023136, F.T.C. (2011) (statement of Rosch, Comm'r, concurring), *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzzstatement.pdf, *archived at* http://perma.cc/05AMrUdWFnk.

[50] *See* Shaw's Supermarkets, Inc. v. N.L.R.B., 884 F.2d 34, 36 (1st Cir. 1989) (Breyer, J.) (citations omitted) ("Whatever [the agency's] ground for departure from prior norms . . . it must be clearly set forth so that the reviewing court may understand the basis of the agency's action and so may judge the consistency of that action with the agency's mandate.").

[51] *Id.*

[52] Exec. Order No. 13,422 § 3(g), 72 Fed. Reg. 2,763 (Jan. 23, 2007).

[53] *See* 15 USC § 45(b) (2012).

[54] *See, e.g.*, Bradley C. Weber, *DOJ and FTC Issue New Horizontal Merger Guidelines*, A.B.A. HEALTH ESOURCE (Sept. 2010) ("And while they do not carry any legal weight, it is likely that [the Horizontal Merger Guidelines] will influence judges and assist the courts in developing an appropriate framework for interpreting and applying the antitrust laws to horizontal mergers."), https://www.americanbar.org/newsletter/publications/aba_health_esource_home/weber.html, *archived at* http://perma.cc/0sHe7yAYFJD.

When the FTC first announced to Congress that it would pursue enforcement actions in this area, it delineated a multi-factor approach. The FTC first elaborated its approach to data privacy in a 1998 report entitled *Privacy Online: A Report to Congress*, which all sitting Commissioners signed without any concurring or dissenting statements.[55] In this report, the FTC stated its intent to incorporate the Fair Information Practice Principles ("FIPPs") into its approach to data privacy. The FIPPs are: "Notice/Awareness; Choice/Consent; Access/Participation; Integrity/Security; and Enforcement/Redress."[56] The FTC defined these principles as follows: (1) Notice: companies to disclose their information practices before collecting personal information from consumers;[57] (2) Choice: companies to provide consumers with options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided;[58] (3) Access: companies allow consumers to view and contest the accuracy and completeness of data collected about them;[59] (4) Security: companies take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.[60] The report also addressed enforcement, a mechanism for imposing sanctions for noncompliance, as a critical ingredient in any governmental or self-regulatory program to ensure privacy online.[61]

The FTC's practices for initiating enforcement actions in the context of data privacy have evolved over the past two decades. As the following sections will show, the agency has moved from focusing mostly on whether there was notice, to taking into account both notice and harm, to its current consideration of a variety of factors in pursuit of developing fair rules of play in the personal information industry.[62] Put another way, the FTC's practices have come to match their theoretical explanation of how they would use their authority to Congress in 1998.

1. In Re Geocities (1998): Notice as the Determinative Factor

In re GeoCities was the FTC's first data privacy matter. GeoCities, the FTC alleged, had misrepresented the purposes for which it was collecting

---

[55] FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf, *archived at* http://perma.cc/08jQ4mvCMKX.

[56] *Id.* at 7.

[57] *Id.* at 7–8

[58] *Id.* at 8–9.

[59] *Id.* at 9.

[60] *Id.* at 10.

[61] *Id.* at 10–11.

[62] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 2–3 (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf, *archived at* http://perma.cc/0BKGwc1auYQ.

data about its customers.[63] The FTC alleged that GeoCities had stated to its consumers that it would not sell or rent the information consumers gave it to any third parties, when in fact, GeoCities had sold information consumers submitted to third parties.[64] In a press release following the consent order, the FTC stated that GeoCities must prominently post a privacy notice on its home page.[65] For adults, this notice was thought to be enough. For children, however, the FTC required a series of age verification requirements to ensure that the user was older than twelve years of age.[66] The idea was that notice was all that was necessary for adults to make an informed choice as to whether to surrender their information to GeoCities.

Two years later, Commissioners Leary and Swindle suggested that notice be the primary emphasis of the FTC's inquiry.[67] But this view has never been endorsed by a majority of Commissioners or endorsed by Congress. *In re GeoCities* represents the high mark for notice as the key ground for FTC enforcement actions. With more experience handling data privacy matters, the FTC moved closer to employing the multi-factor balancing test recommended by the FIPPs.

2. 1998-2007: Increasingly Broad Definitions of Notice and Harm

In re Geocities focused exclusively on, and took a highly formal approach to, consumer notice. However, through experience over the following ten years, the FTC discovered the pure notice-based rationale for intervention failed to include many instances in which the FTC found it necessary to intervene. From 1998 to 2008 The FTC relied upon two dominant rationales for intervention: notice and harm.[68] While FTC's rationales for action remained formally within the paradigms of notice and harm, cases began to define notice and harm in a broad enough way to take into account the FIPPs. This section will examine how the FTC expanded notice and harm in turn.

---

[63] GeoCities, 127 F.T.C. 94, 96–99, 121–33 (1999) (consent order) (settling charges that website had misrepresented the purposes for which it was collecting personally identifiable information from children and adults).

[64] *Id.* at 96–99.

[65] Press Release, Fed. Trade Comm'n, Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case (Aug. 13, 1998), *available at* http://www.ftc.gov/opa/1998/08/geocitie.shtm, *archived at* http://perma.cc/0Sqk1UnoVhF/.

[66] *Id.*

[67] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, DISSENTING STATEMENT OF COMMISSIONER ORSON SWINDLE 26-27 (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf, *archived at* http://perma.cc/05XEVhUNP1U; FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, STATEMENT OF COMMISSIONER THOMAS B. LEARY, CONCURRING IN PART AND DISSENTING IN PART 12 (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf, *archived at* http://perma.cc/05XEVhUNP1U.

[68] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 62, at 2 (distinguishing notice- and harm-based cases).

a. Notice

Enforcement actions against Gateway and Vision I Properties LLC illustrate the evolution of the FTC's construction of notice from formal notice to functional notice.[69] In *In re Gateway*, the FTC alleged that it was unfair or deceptive for Gateway to change its privacy policies without notifying its consumers of the change.[70] Gateway, the FTC alleged, had shared consumers' information with third parties after changing its policy to allow Gateway to share the information with third parties without notifying customers of the change.[71] This was the FTC's first case "to challenge deceptive and unfair practices in connection with a company's material change to its privacy policy."[72] Notably, the remedy agreed upon in the settlement was that users had to opt in to have their data used in this way in the future. This suggests that the FTC found that an opt-in mechanism is a way of ensuring that a consumer receives adequate notice. The remedy also included a provision that Gateway pay the Treasury the value it earned from renting the consumer's information. In Gateway's case, it was a paltry $4,608. However, a company whose primary livelihood is sale of consumer information would do well not to run afoul of this precedent. Howard Beales, Director of the FTC's Bureau of Consumer Protection, identifies consent as the crux of the case: "It's simple—if you collect information and promise not to share, you can't share unless the consumer agrees . . . . You can change the rules but not after the game has been played."[73]

Similar concerns were at play in a 2005 action against CartManager, a business that provides online shopping carts for several Internet merchants. The FTC alleged that CartManager "rented personal information about merchants' customers to marketers, knowing that such disclosure contradicted merchant privacy policies."[74] Prior to the FTC's enforcement action, a customer would browse products on a merchant's website, but when it came time to access the cart and pay for the items, the customer would be accessing CartManger's servers and thus would be subject to CartManger's privacy policy. This would be so despite the website having the look and feel of the merchant's website. The FTC reasoned that the consumers could not have had notice of CartManager's privacy's policies. Even if they had duti-

---

[69] Press Release, Fed. Trade Comm'n, Gateway Learning Settles FTC Privacy Charges (July 7, 2004), *available at* http://www.ftc.gov/opa/2004/07/gateway.shtm, *archived at* http://perma.cc/0z4uwPYq9et.

[70] Complaint, In the Matter of Gateway Learning Corp., A Corp., No. 042-3047, 2004 WL 1632833 (F.T.C. July 7, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/040707cmp0423047.pdf, *archived at* http://perma.cc/0cfStKZimiu/.

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] Press Release, Fed. Trade Comm'n, Internet Service Provider Settles FTC Privacy Charges (Mar. 10, 2005), *available at* http://www.ftc.gov/opa/2005/03/cartmanager.shtm, *archived at* http://perma.cc/025D7TsZ4Fa/.

fully read the privacy policies of the website at which they chose to shop, they could not have known that CartManager would have substantially different privacy policies than the merchant. The FTC alleged that consumers were not "adequately inform[ed]" of the discrepancy in privacy policy.[75] The FTC thus considered more factors than simply formal notice in the CartManager enforcement action. The FTC relied on the language used to convey the language and the time when the company conveyed its privacy policy.

This case indicates that the FTC finds there to be a limit to the amount of background research consumers can reasonably be expected to perform about privacy policies. After all, it was theoretically possible for users to discover Cartmanager's privacy policy. The FTC decided, however, that it would put too much of a burden on consumers to do that.

The transition from Gateway to Cartmanager shows that the FTC's understanding of constructive notice is broad enough to account for the limited time and energy consumers have to decipher privacy policies. This evolution reflects a policy decision that when notice is merely formal, that is no notice at all. It prevents consumers from making informed decisions about their personal information, and thus distorts the market for privacy protections.

b. Harm

The decade following *In re GeoCities* brought a similar broadening and re-defining of what harm to consumers was sufficient to trigger enforcement action by the FTC. "Harm" has evolved to include problematic results from consumer information rendered without consumers having a reasonable opportunity to decide whether to yield it.

In *In re ReverseAuction*, the FTC alleged that ReverseAuction "violated consumers' privacy by harvesting consumers' personal information from a competitor's site and then sending deceptive spam to those consumers soliciting their business."[76] ReverseAuction had registered on eBay, obtained the contact information of eBay users, and emailed them ReverseAuction ads averring that the users' eBay accounts were about to expire. The majority stated that the use of the FTC's unfairness authority was proper because there was substantial harm.[77] As Commissioner Mozelle W. Thompson noted, the harm accrued because ReverseAuction's conduct

---

[75] *Id.*

[76] Press Release, Fed. Trade Comm'n, Online Auction Site Settles FTC Privacy Charges (Jan. 6, 2000), *available at* http://www.ftc.gov/opa/2000/01/reverse4.shtm, *archived at* http://perma.cc/0qLFN7tWX48/.

[77] *See generally* Fed. Trade Comm'n v. ReverseAuction.com, Inc., No. 00 0032, 2000 U.S. Dist. LEXIS 20761 (D.D.C. Jan. 10, 2000) (settling charges that an online auction site allegedly obtained consumers' personal identifying information from a competitor site and then sent deceptive, unsolicited email messages to those consumers seeking their business).

> not only breached the privacy expectation of each and every eBay Member, it also undermined consumer confidence in eBay and diminishes the electronic marketplace for all its participants. This injury is exacerbated because consumer concern about privacy and confidence in the electronic marketplace are such critical issues at this time.[78]

This definition of harm is broad enough to encompass many cases when the company's presentation of its privacy policies results in the reasonable consumer not being informed of the gravity of the choice to surrender her information at the time of transfer. This broadness of the harm-based standard did not go unnoticed by the Commissioners who dissented,[79] but as this section will show, the majority has carried the day in the FTC's subsequent enforcement actions. In the wake of the consent order, the FTC Chairman reaffirmed the significance of choice in the news release, mentioning that "[c]onfidence that privacy will be protected is an important element in consumers' decisions where to shop on the Internet."[80] The FTC also reaffirmed its role in encouraging industry self-regulation.[81]

The FTC expanded upon *In re ReverseAuction* in its rationale for pursing an enforcement action against BJ's in 2005.[82] In *In re BJ*'s, the FTC ruled that a company may be subject to an enforcement action if it failed to provide reasonable security for consumers' data, even if it had not made an express statement about privacy.[83] This enforcement action extended the definition of harm past ReverseAuction's because in BJ's case, unlike in ReverseAuction, nothing had happened to the insecure data; the data was merely more vulnerable than the consumers might expect. This made clear that the FTC employs a broad notion of harm that balances consumers' and companies' interests. It is less costly for society as a whole if companies are spurred to have at least adequate data security practices rather than waiting for a data breach to take place. In short, having the FTC take action in cases like BJ's redounds to the overall higher welfare of society.

The FTC has employed an increasingly broad standard for what constitutes harm to justify its intervention in privacy matters. In *In re BJ's* it even embraced an increased risk of loss as a cognizable harm. The evolution of

---

[78] Fed. Trade Comm'n v. ReverseAuction.com, Inc., No. 0023046, F.T.C. (Jan. 6, 2000) (statement of Thompson, Comm'r), *available at* http://www.ftc.gov/os/2000/01/reversemt.htm, *archived at* http://perma.cc/0yZCRFfPdpy.

[79] Fed. Trade Comm'n v. ReverseAuction.com, Inc., No. 0023046, F.T.C. (Jan. 6, 2000) (statement of Swindle & Leary, Comm'rs, concurring in part, dissenting in part), *available at* http://www.ftc.gov/os/2000/01/reversesl.htm, *archived at* http://perma.cc/0334JoRDcWP.

[80] Press Release, Fed. Trade Comm'n, Online Auction Site Settles FTC Privacy Charges, *supra* note 76.

[81] *Id.*

[82] Press Release, Fed. Trade Comm'n, BJ'S [sic] Wholesale Club Settles FTC Charges (June 16, 2005), *available at* http://www.ftc.gov/opa/2005/06/bjswholesale.shtm, *archived at* http://perma.cc/03cTNByALkJ.

[83] *Id.*

the definition of both harm and notice appears to be motivated by the FTC's increasing sense of itself as a balancer of interests in the context of the information privacy trade. The FTC took on this role more directly, I argue, in later enforcement actions.

3. Recent cases (2008–present): Consideration of all of the FIPPs in determining enforcement action choice and terms of consent orders

The past five years have reflected a sea change in the FTC's justifications for data-privacy-related enforcement actions. Welfarist balancing based on a diverse menu of factors including notice, choice, access, and security has become increasingly prominent in the FTC's discussion of data privacy matters. The FTC has returned to considering the broad range of factors included in its initial description to Congress of the authority it planned to exert in the area of online privacy. By taking many concerns into account in evaluating consumer's reasonable expectations, the FTC accomplishes a welfarist analysis of which privacy interests businesses may invade without cost.

In re Sears heralded the FTC's increased willingness to rely on a welfarist assessment of balancing consumers' and industry's interests, with the relevant factors grounded in the FIPPs.[84] Three enforcement actions involving the internet's leading social media companies, rooted in similar reasoning, indicate that firms should expect the FTC to apply this model.

In *In re Sears*, the FTC alleged that it was deceptive to place information at a time in the transaction when a reasonable consumer is unlikely to be paying attention.[85] The FTC alleged that Sears had violated FTCA by deceiving consumers about the extent to which it tracked their online activities. According to the FTC, Sears paid customers in exchange for visiting its websites and downloading research software that would track browsing history confidentially.[86] Sears only disclosed the full extent of the data the software tracked in the middle of a lengthy license agreement made available at the end of a multi-step process.[87] The FTC considered the context of when information is presented to be relevant to the reasonable consumer's understanding of the conditions of information transfer.[88] The proceeding, however, stands for the proposition that firms must avoid the appearance of

---

[84] *See In re* Sears Holdings Mgmt. Corp., No. C-4264, F.T.C. (Aug. 31, 2009) (decision and order), *available at* http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf, *archived at* http://perma.cc/0vyWkDvyzq8.

[85] *Id.*

[86] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change, *supra* note 62, at 12.

[87] *Id.* at 13.

[88] *See id.* at 19–20.

purposively deemphasizing information about privacy terms in a transaction for information.

As the FTC's recent Twitter, Facebook, and Google Buzz consent orders illustrate, the agency has increasingly concerned itself with ensuring that actual data privacy protections accord with consumers' reasonable expectations.[89] In making this assessment, the FTC has utilized the FIPPs, which suggest consideration of notice, choice, access, and security.

In the Twitter enforcement action, the FTC emphasized the importance of consumers' reasonable expectations when they designated information as private.[90] The FTC alleged that "serious lapses in the company's data security allowed hackers to obtain unauthorized administrative control of Twitter, including access to non-public user information, tweets that consumers had designated as private, and the ability to send out phony tweets from any account."[91] In the wake of the case, David Vladeck, Director of the FTC's Bureau of Consumer Protection stated:

> [A] company that allows consumers to designate their information as private must use reasonable security to uphold such designations. Consumers who use social networking sites may choose to share some information with others, but they still have a right to expect that their personal information will be kept private and secure.[92]

This statement suggested that the FTC would take notice when a consumer chooses to designate her information as private and would consider action if the company's conduct does not accord with the consumer's designation. This enforcement action provided guidance as to the extent to which the FTC will hold companies to data privacy standards commensurate with consumer expectations, as elucidated in *BJ's*, in the social media context. As in *In Re Sears*, the reasoning is freed from the moorings of references to harm and notice in the main statements of rationale. Rather, the FTC seems to be taking into account all relevant factors in coming to an agreement with the company to resolve the enforcement action.

The FTC's action against Google following its launch of Google Buzz also reflected the agency's concern with assuring consumers' reasonably in-

---

[89] Press Release, Fed. Trade Comm'n, Twitter Settles Charges that It Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program (June 24, 2010), *available at* http://www.ftc.gov/opa/2010/06/twitter.shtm, *archived at* http://perma.cc/0FShc8ViQHn [hereinafter Twitter]; Press Release, Fed. Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), *available at* http://www.ftc.gov/opa/2011/03/google.shtm, *archived at* http://perma.cc/0qtfHHqvByb [hereinafter Google]; Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises (Nov. 29, 2011), *available at* http://www.ftc.gov/opa/2011/11/privacysettlement.shtm, *archived at* http://perma.cc/0ui4ksZCGqX [hereinafter Facebook].

[90] *See* Twitter, *supra* note 89.

[91] *Id.*

[92] *Id.*

formed choice in transacting information. According to the FTC's complaint, on the day of Google Buzz's launch, Gmail users received a message announcing the new service offering two options: "Sweet! Check out Buzz," or "Nah, go to my inbox."[93] The FTC alleged that Google nonetheless enrolled some Gmail users who declined the service. The FTC also alleged that Google failed to inform adequately some users who accepted the service that the individuals they emailed most frequently would be identified publically by default.[94] Moreover, Google's "turn off the buzz" feature did not fully remove the user from the network.[95] The FTC also alleged that Google utilized customers' information provided for Gmail for social networking purposes in violation of the company's privacy policies.[96]

The Google Buzz consent order contained an important first. The FTC required Google to implement a "comprehensive privacy program," and required audits conducted by independent third parties every two years to assess its privacy.[97] The consent order, more specifically, required Google to develop a terms of use page that "clearly and prominently disclose[s]: (1) that the Google user's information will be disclosed to one or more third parties, (2) the identity or specific categories of such third parties, and (3) the purpose(s) for respondent's sharing . . . ."[98] The consent order also required that Google obtain affirmative consent from users before going through with changes to Google's privacy policy.[99]

In the Google matter, the FTC exerted broad authority to impose substantial limitations on Google in the consent order. Both the rationale for action and the remedies show concern with setting the limits of what information consumers must have to make a choice regarding their personal information. Concurring, Commissioner Rosch noted that the agency was concerned that Google was accepting the terms as leverage that "hurt other competitors as much or more than the terms will hurt [Google]."[100] This concurrence underscores the practical policy import of these consent orders, regardless of the fact that they are technically non-binding on non-parties.

The Facebook enforcement action followed the Google Buzz action, and its consent order shared many features with Google's. The Facebook enforcement action alleged that Facebook used user data in ways not allowed by its stated privacy policy. The FTC alleged that Facebook "deceived con-

---

[93] Google, *supra* note 89.
[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *Id.*
[98] *In re* Google, Inc., No. 102 3136, F.T.C. (2011) (agreement containing consent order), *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf, *archived at* http://perma.cc/0rQPFV6Zkfj.
[99] *Id.*
[100] *In re* Google, Inc., No. 1023136, F.T.C. (2011) (statement of Rosch, Comm'r, concurring), *supra* note 49.

sumers by telling them they could keep their information on Facebook private, and then repeatedly allowing it to be shared and made public."[101]

Facebook's consent order entailed similar remedies to Google's. The remedies are centered on giving a reasonably attentive user the resources to know to what she is consenting when she turns her information over to the companies. Facebook must also create a comprehensive privacy security program. Notably, the consent order requires Facebook "to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences."[102]

The terms of this Facebook consent order apply to matters beyond those at issue when the complaint first arose. Facebook is required to obtain users' consent before changing the visibility of user data.[103]

These recent consent orders represent the FTC's shift toward enforcement actions meant to protect consumers from bearing an unfair or unknowing burden in the market for personal information. The FTC has warned industry with these consent orders that mere formal notice to consumers will not be enough to avoid enforcement actions. Building choice into the user interface, allowing customers to opt into the company's uses of their personal information, and simplifying consumer choice are three methods that the FTC has flagged as suggested policies, and may be ways of avoiding enforcement actions.[104]

The FTC's approach in its most recent consent orders balances businesses' commercial interests with consumers' interests in data privacy, using the FIPPs as guidance. The FTC is well suited to handle data privacy conflicts that involve balancing the interests of many stakeholders because of its expertise in data privacy, ability to do independent research and adapt quickly to changing customs and technology, and custom of providing tailored solutions through consent orders.

IV. Toward an Institutionally-Appropriate Approach to Avenues for Vindicating the Privacy Interest

The FTC has the authority under FTCA § 5 to engage in data privacy enforcement actions. Its increasingly activist role has been noted and analyzed by several scholars. The increasing influence and consistency in approach of the FTC in the context of privacy has led Daniel Solove and Woodrow Hartzog to deem the FTC's statements on privacy to be "the new

---

[101] Facebook, *supra* note 89.

[102] *Id.*

[103] *In re* Facebook, Inc., No. 092 3184, F.T.C. (2011) (agreement containing consent order), *available at*, http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.

[104] *See* Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change, *supra* note 62, at 22-30, 35–48, 57.

common law of privacy."[105] The multi-factor approach adopted by the FTC since 2008 employing the FIPPs is a pragmatic approach well-suited to resolving polycentric data privacy disputes with basis in existing agency practice and law.

By contrast, courts lack the institutional capacity to conduct broad, forward-looking balancing of society's interests with respect to technology, speech, and privacy in resolving particular matters. *Dwyer v. American Express Co.*, *In re JetBlue Airways Corp Privacy Litigation*, and *Boring* exemplify courts' failure to engage critically with the type of harm that constant surveillance or data misappropriation can present to an individual in the digital age.[106]

Nonetheless, adjudicative reasoning has important advantages and should play a significant role in the continuing development of data privacy law. While many forward-looking policy questions should find their resolution in FTC action or congressional action, common law courts provide the best forum for handling disputes between parties over particular facts, particularly in smaller claims. Courts' institutional strengths include drawing lines and determining relevant factors for distinguishing between fact patterns. Courts are uniquely well-suited to determining whether a particular company has gone "too far" in making use of consumer data and are best at defining the proper scope of damages. In making these fact-specific determinations, courts would seek to define when the duty to respect individuals' interest in data privacy overrides the privilege to speak, express oneself and engage in commerce.[107]

First, this section will outline a form state proposal that would implement this framework by increasing the scope of privacy state law and creating state administrative agencies to handle individual privacy claims. Then, it will discuss what this framework brings to existing literature regarding how the right to privacy should be enforced.

A. Implementing an institutionally appropriate privacy regime

My proposed new state administrative agencies would adjudicate state law data privacy conflicts cost-effectively and efficiently. These state administrative agencies could also be in communication with the FTC about patterns in matters that they see coming before them. In this way, they could

---

[105] Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 COLUM. L. REV. (forthcoming 2014).

[106] *See Boring*, 362 F. App'x at 279; *Jet Blue*, 379 F. Supp. 2d at 299; *Dwyer*, 652 N.E.2d at 1351.

[107] I have suggested elsewhere a framework in which certain relationships and actions trigger a relational right to exclude others from access to or use of information. This approach treats privacy as quasi-property. Lauren Henry, Privacy as Quasi-Property 24 (Apr. 30, 2013) (unpublished manuscript) (on file with author).

refer matters more appropriate for the investigative, policy-driven approach the FTC takes.

I propose a two-pronged approach to obtain institutionally appropriate enforcement of privacy law. On the state level, legislatures should pass laws that (1) create administrative agencies to be a forum for individuals to litigate privacy claims under state law, and (2) maximize the value of common law review of privacy law by broadening the scope of the intrusion upon seclusion privacy tort.

First, states should pass laws creating administrative agencies to adjudicate privacy claims based on state statutory and common law in the areas of privacy, data security, and identity theft. The judgments of the administrative agencies would be subject to appeal to state courts. These laws would also encourage the state privacy agency to refer matters or questions to the FTC where they find that that a privacy matter presents a substantial polycentric conflict and would benefit from the investigative capacity of the FTC. This would allow the FTC to be apprised of matters in which its expertise would be useful. But the FTC would not be required to examine further any matter referred by the state administrative agency.

The cooperative approach that the Equal Employment Opportunity Commission (EEOC) takes with state Fair Employment Practices Agencies (FEPAs), state agencies that enforce state anti-discrimination laws, could provide a blueprint for the relationship state privacy agencies could have with the FTC.[108] The EEOC makes individualized agreements for sharing work with state agencies, including authorizing the state agency to handle matters that fall within the EEOC's jurisdiction (on top of the state agency's organic authority to handle appropriate state law discrimination claims).

Second, states should reform state privacy law to expand the common law cause of action. The four Restatement privacy torts heavily constrain courts' ability to recognize harms to privacy given the quick pace of technological development.[109] Therefore, states could expand the intrusion upon seclusion tort in the following way. If a plaintiff can develop a strong case that the context, relationship between parties, and manner of access or use of the personal information warrants the right to exclude, it should be considered an infringement of privacy. This standard provides a broader canvass for common law courts to develop virtual private spaces beyond the eye of society in the digital age. Appropriately, it is a standard that would be able to change substantively over time because of the nature of common law adjudication.

While both components of this proposal rely upon state action, federal action could facilitate this proposal's adoption at the state level. Congress

---

[108] *Fair Employment Practices Agencies (FEPAs) and Dual Filing*, EQUAL EMP'T OPPORTUNITY COMM'N, http://www.eeoc.gov/employees/fepa.cfm (last visited Sept. 28, 2013), *archived at* http://perma.cc/08R4P4zwrkU.

[109] *See supra* Section II.

could tie the passage of the state legislation proposed above to important federal funding.[110] An example of this arrangement is the National Minimum Legal Drinking Act, which withholds ten percent of all federal highway construction funds from states that refuse to enforce a minimum legal drinking age of 21.[111]

The Supreme Court's recent decision in *Nat'l Fed'n of Indep. Bus. v. Sebelius* may limit Congress's ability to influence states.[112] This case involved a federal statute that conditioned states' pre-existing federal Medicaid funding on implementing Congress's proposed Medicaid expansion program.[113] Although that provision was upheld, no view carried a majority of the court. Chief Justice Roberts, joined by Justices Breyer and Kagan, would have ruled that the Medicaid expansion could survive, but that states must be given the right to opt out of the expansion without losing their pre-existing Medicaid funding.[114] Justices Scalia, Kennedy, Thomas, and Alito would have struck down the Medicaid expansion completely.[115] If opponents of a federal statute encouraging states to create data privacy agencies could persuasively argue that Congress has tied the adoption of a data privacy state agency to pre-existing funding, a federal court could strike down the incentive that statute gave to states to create such an agency. To avoid this, it may be wise to condition future funding rather than existing funding as the incentive to adopt this policy on the state level.

This proposal is attractive because it makes adjudication available for small matters less likely to be brought to state courts in the first instance because of the time and expense of non-administrative litigation. The proposal also enables the FTC to choose enforcement actions more effectively due to communication between the FTC and state administrative agencies.

Critics might contend that the second proposal accords courts too much discretion. However, this is an appropriate step to take because over the past fifty years since the development of the four Restatement privacy torts, the courts' enforcement of privacy has ossified and become rigidly devoted to the formal requirements for the four torts. Introducing more flexibility in what courts may enforce would take advantage of the special expertise common law courts have in distinguishing between cases. Moreover, if state courts take up too much authority, they are subject to curtailment by both state legislatures and Congress.

State administrative agencies can substantially ease the burden of handling the bulk of privacy cases and can draw out the difficult factual matters

---

[110] Any such federal legislation would specify that it does not seek to preempt substantive state privacy law.

[111] 23 U.S.C. § 158 (2012).

[112] 132 S.Ct. 2566 (2012).

[113] *Id.* at 2577.

[114] *Id.* at 2601–08 (opinion of Roberts, C.J.).

[115] *Id.* at 2656–68 (dissenting opinion).

on which many modern privacy matters turn, leaving only fine legal distinctions to be determined by state courts.

B. Relationship to Literature on Reforms to Data Privacy Law

In this section, I compare my approach to existing proposed reforms of data privacy law. These other proposals can be divided into three categories: (1) judge-initiated strengthening of common law privacy torts, (2) creation of new data privacy claims through omnibus federal legislation, and (3) self-regulation.

Many scholars have identified broad principles that should underlie any change in approach.[116] A few have outlined more specific approaches, identifying the institution that should act to more accurately assess and weigh Americans' privacy concerns. One commentator has argued that courts should extend the common law privacy causes of action to cover the disclosure and commercialization of personal information contrary to users' wishes.[117] Another commentator has agreed that courts should resolve privacy controversies, and also has proposed new omnibus federal Internet privacy legislation that establishes privacy causes of action.[118] Another scholar has disagreed with the focus on court action and instead has stressed the need for a new federal administrative agency with a broad mandate to define and prosecute privacy infringements.[119] Still another scholar has insisted that industry self-regulation is the preferable path in this area, which implicates rapidly developing technology.[120] In another variation of the self-regulatory approach, another commentator has suggested a system where each person tags their information with standard labels indicating permissible uses of their data.[121]

Early in its data privacy watchdog career, the FTC emphasized self-regulation as a solution to growing privacy concerns in the nascent informa-

---

[116] *See, e.g.*, NISSENBAUM, *supra* note 6, at 107 (outlining a theory of contextual integrity, which defines privacy as a right to a flow of personal information in accordance with entrenched, context-relative informational norms); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1416–18, 1421 (2000) (arguing that privacy is a constitutive element of a democratic civil society because it enables and nurtures individual autonomy).

[117] *See* Connie Davis Powell, *"You Already Have Zero Privacy. Get Over It!" Would Warren and Brandeis Argue for Privacy for Social Networking?*, 31 PACE L. REV. 146, 179–81 (2011).

[118] *See* Jonathan D. Frieden et al., *Putting the Genie Back in the Bottle: Leveraging Private Enforcement to Improve Internet Privacy*, 37 WM. MITCHELL L. REV. 1674, 1722–25 (2011).

[119] *See* FREDERICK S. LANE, AMERICAN PRIVACY: THE 400-YEAR HISTORY OF OUR MOST CONTESTED RIGHT 258 (2011).

[120] *See* Catherine Schmierer, Note, *Better Late than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Legislation*, 17 RICH. J.L. & TECH., no. 4, 2011, at 1, 56–57.

[121] Lauren Gelman, *Privacy, Free Speech, and "Blurry Edged" Social Networks*, 50 B.C. L. REV. 1315, 1342 (2009).

tion age.[122] However, the persistence of data privacy enforcement actions (including many recapped in part III), casts doubt on self-regulation's ability to provide any meaningful safeguard for a substantial privacy interest without some type of a check on corporate conduct from government.[123] In a recent guidance document, the FTC flagged the concerns of many commenters about the effectiveness of self-regulations and has acknowledged the limits of self-regulation to protect data privacy without support from legal institutions.[124] The calls for self-regulation in data privacy have gone mostly unanswered, and what little self-regulation has occurred has been thin.[125] This suggests self-regulation without further guidance is not an adequate option. Self-regulation may play an important role in any privacy regime, but it is not adequate protection on its own to guard against the economic incentive companies have to obtain and use personal information in a way that hurts consumers.

My proposal is compatible with expanding the common law to include a broader type of data privacy injury (in fact, that is part of my proposal), and with expanding federal law to create more data privacy claims. I supplement this proposal with institutions and clear procedural directives. The state administrative agencies could act as adjuncts to state courts in enforcing expanded data privacy laws that would allow many small data privacy claims a hearing. State administrative agencies, which would deal with these small claims on the ground, would inform the FTC of patterns or individual cases that the FTC would be well-suited to act upon. The referral system would also help courts avoid handling polycentric disputes better handled by the FTC's forward-looking, regulatory approach.

Each of the alternative proposals—self-regulation, common law data privacy claim expansion, and federal law data privacy claims—do not address the difficulties courts face in analyzing problems from the polycentric perspective that a quick moving issue with many stakeholders like privacy requires. Dividing the work of regulating privacy between the courts and the FTC would reduce the burden on courts to rule in ways that decide prospectively for large numbers of companies and people, a role unfit for courts. The FTC has rulemaking, adjudicative, and investigatory capacities that could enable it to deal with significant, problematic conduct first at the agency level, potentially precluding action in front of a system of non-uniform courts. The courts could then focus on defining the circumstances where people have a right to exclude others from their personal information, a task for which courts are eminently well suited.

---

[122] *See generally,* FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS (1999), *available at* http://www.ftc.gov/os/1999/07/privacy99.pdf, *archived at* http://perma.cc/0qqY3s4bUzy.

[123] *See supra* Section III.

[124] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, *supra* note 62, at 11 ("In most areas . . . there has been little self-regulation.").

[125] *Id.*

V. Conclusion

Privacy has a long history of protection under American common law, statutory law, and constitutional law. This paper presents a framework mindful of institutional competences for employing our existing legal principles for privacy in contexts that maximize their ability to serve the public interest and adapt with changing times.

* Lauren Henry, B.A., Yale College, 2009; J.D. Candidate, Harvard Law School, Class of 2014. The author is also grateful to Professors Yochai Benkler, Mark Tushnet, and Larry Yackle for invaluable comments on earlier versions of this note.