I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Privacy Harms and the Effectiveness of the Notice and Choice Framework

JOEL R. REIDENBERG*
STANLEY D. AND NIKKI WAXBERG CHAIR AND PROFESSOR OF LAW, FORDHAM

N. CAMERON RUSSELL
EXECUTIVE DIRECTOR, FORDHAM CLIP

ALEXANDER J. CALLEN
RESEARCH FELLOW, FORDHAM CLIP

SOPHIA QASIR
RESEARCH FELLOW, FORDHAM CLIP

THOMAS B. NORTON
PRIVACY FELLOW, FORDHAM CLIP

Abstract: In the last fifteen years, the Federal Trade Commission and the White House have promoted notice and choice as the preferred mechanism for protecting consumers' privacy online. But law and policy scholars doubt the efficacy of this mechanism. Research shows that consumers rarely read website privacy policies, that such policies are often too

---

 The authors would like to thank the participants at the 42nd Research Conference on Communication, Information and Internet Policy, TPRC 2014, for comments on an earlier draft. Work on this article was supported by Grant CNS-1330214 from the National Science Foundation to the Center on Law and Information Policy at the Fordham University School of Law, New York, NY (Fordham CLIP) and by a Fordham Law School Faculty Summer Research Grant.

complex for users to understand, and that website policy statements do not match consumers' privacy expectations. Efforts to ameliorate these issues through technological tools, such as privacy filters and do-not-track codes, have been unsuccessful. Further, these tools do not address whether notice and choice theory aligns with the actual privacy harms that consumers experience.

This alignment remains unexplored. This article proposes to examine the relationship between the notice and choice theory and users' actual privacy concerns. The article takes a novel approach that examines federal privacy litigation and FTC enforcement actions. This focus on the wrongs litigated in the real world reveals the most important harms that consumers experience and provides a better understanding of the efficacy of the notice and choice framework.

The data set compiled to support the research for the article consists of all federal class action complaints alleging online privacy violations filed during the last ten years and the Federal Trade Commission complaints and settlements addressing online privacy. The article next addresses the roles that jurisdiction and competence play in framing claims, and identifies a typology of the wrongful acts experienced by consumers. The research shows that four types of claims appear in both private litigation and public enforcement with respect to personal information: (1) unauthorized disclosure, (2) surreptitious collection, (3) failure to secure, and (4) undue retention.

The article then applies this typology to map "zones of effectiveness" for the notice and choice regime. The article identifies which wrongs a proper notice and choice regime can and cannot address. The research demonstrates that while some wrongful practices might be avoided by the inclusion of specific statements in a notice, others will be incurable through notice. The latter set of wrongs is outside the "zone of effectiveness" of a notice and choice regime.

I. INTRODUCTION

The United States has historically considered two models for the protection of information privacy: targeted statutory rights such as the Fair Credit Reporting Act and market self-regulation based on

notice and choice.[1] In the last fifteen years, the Federal Trade Commission and the White House have promoted notice and choice as the preferred mechanism for protecting consumers' privacy online.[2] But law and policy scholars have doubted the practical efficacy of this mechanism.[3]

Technologists, however, have tried to address the efficacy and have sought to develop various tools that would facilitate use of notice and choice for online users.[4] At best, these tools have only achieved modest success.[5] More recently, serious efforts to develop automated machine learning tools, also known as natural language processing, have emerged to offer promise of greater effectiveness.[6] These tools

---

[1] *See e.g.*, DANIEL SOLOVE AND PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS (2013); Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315 (2000).

[2] *See e.g.*, *Consumer Privacy Bill of Rights*, THE WHITE HOUSE (2012) http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights; FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESS AND POLICY MAKERS (2012) http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[3] *See generally* Fred Cate, *Protecting Privacy in Health Research: The Limits of Individual Choice*, 98 CALIF. L. REV. 1765 (2011). *See also infra* Part II.A.2 and accompanying notes.

[4] Tools such as the Platform for Privacy Preferences ("P3P"), privacy seals, and browser plug-ins have not succeeded in achieving wide adoption.

[5] Research shows that users rarely read website privacy policies, that such policies are often too complex for users to understand, and that website policy statements do not match consumers' privacy expectations. *See infra* Part II.A.2 and accompanying notes. Efforts to ameliorate theses issues through technological tools, such as privacy filters and do-not-track codes, have been unsuccessful. *See, e.g.*, Joel R. Reidenberg, et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. (forthcoming 2015) (describing research on privacy policy usability and technical tools for usability improvement).

[6] For example, research for this paper was funded through a $3.4 million National Science Foundation collaborative grant to Carnegie Mellon University, Fordham University, and Stanford University to explore natural language tools and crowd sourcing as means to help users understand web privacy policies. *See* Norman Sadeh et al., *Towards Usable Privacy Policies: Semi-automatically Extracting Data Practices From Websites' Privacy Policies* (Poster), ACM SYMP. ON USABLE SECURITY AND PRIVACY (SOUPS 2014); N. Sadeh et al., *The Usable Privacy Policy Project: Combining Crowdsourcing, Machine Learning and Natural Language Processing to Semi-Automatically Answer Those Privacy Questions Users Care About*, CARNEGIE MELLON UNIVERSITY, SCHOOL OF COMPUTER SCI., INST. SOFTWARE RES. TECHNICAL REP., CMU-ISR-13-119 (2013); Steve Bellovin and Sebastian Zimmeck, *Machine Learning Analysis of Privacy Policies*, U. MICH. TELECOMM. L. REV. (forthcoming); Sebastian Zimmeck and Steven M. Bellovin, *Privee: An Architecture for*

would seek to use automated, computer processing to decipher the meaning of website privacy policies and then present users with meaningful indications of a site's information practices. The success of these technologies will depend on the clarity of website privacy policies and whether the policies actually address the harms that users experience. Even the most promising natural language processing tools to improve the function of notice and choice do not address whether notice and choice theory aligns with the actual privacy harms that consumers experience.

This Article proposes to examine the relationship between the notice and choice theory and users' actual privacy concerns. The Article takes a novel empirical approach that examines both federal privacy litigation and FTC enforcement actions.[7] This focus on the wrongs litigated in the real world reveals the most important privacy harms that consumers experience and provides a better understanding of the areas where the notice and choice framework may or may not be effective.[8]

The Article begins with a discussion of the background on notice and choice and users' protections (Part II). Next, the Article explains the method for collecting data about privacy events and harms, and examines the roles that jurisdiction and competence play in framing claims (Part III). The following part extrapolates from that data the typology of harms or wrongful acts that users perceive (Part IV). The analysis of the data reveals that four types of claims appear in both private litigation and public enforcement with respect to personal information: (1) unauthorized disclosure, (2) surreptitious collection, (3) failure to secure, and (4) undue retention. Based on this typology, Part V maps the "zones" where notice and choice may be effective and where it will be ineffective as a framework to protect user privacy. In essence, this part identifies those wrongs that a notice and choice framework can and cannot address. The research demonstrates that

---

Automatically Analyzing Web Privacy Policies, PROC. OF 23RD USENIX SECURITY SYMP., AUGUST 2014, USENIX ASS'N, https://www.usenix.org/conference/ usenixsecurity14/ technicalsessions/presentation/zimmeck.

[7] Other studies have addressed issues either with respect to the FTC or with respect to specific litigation, but none have provided a full picture. *See, e.g.*, Sasha Romanosky, David A. Hoffman, & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, J. EMPIRICAL LEGAL STUD., (forthcoming), *available at* http://ssrn.com/ abstract=1986461 (analyzing breach litigation); Woodrow Hartzog & Daniel J. Solove, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014) (discussing FTC cases).

[8] This approach focuses on practices that become known to consumers. If consumers are unaware of data practices, then consumers would not perceive a harm and there would be no litigation even though privacy invasions might be taking place.

while some wrongful practices might be avoided by the inclusion of specific statements in a notice, others will be incurable through notice. The latter set of wrongs is, thus, outside the "zone of effectiveness" of a notice and choice regime. The Article concludes with a discussion of the policy implications of the findings.

II. THE BACKGROUND FOR NOTICE AND CHOICE AND USER PROTECTIONS

This Part provides background on issues surrounding the efficacy of notice and choice and then sets out the goal for our empirical research—exploring user concerns through litigation events to better understand the mechanism's effectiveness as a privacy protection.

A. The Efficacy of the Notice and Choice Regime

The FTC has identified notice as "[t]he most fundamental principle" in online privacy.[9] While some commentators and policymakers commend notice and choice, the mechanism has also been widely criticized.

1. *Commendations of Notice and Choice*

The notice and choice mechanism is designed to put individuals in charge of the collection and use of their personal information. In theory, the regime preserves user autonomy by putting the individual in charge of decisions about the collection and use of personal information.[10] Notice and choice is asserted as a substitute for regulation because it is thought to be more flexible, inexpensive to implement, and easy to enforce.[11] Additionally, notice and choice can legitimize an information practice, whatever it may be, by obtaining

---

[9] FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (June 1998), *available at* www.ftc.gov/reports/privacy3/priv-23a.pdf.

[10] *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1049 (2012) (*citing* Paula J. Dalley, *The Use and Misuse of Disclosure as a Regulatory System*, 34 FLA. ST. U. L. REV. 1089, 1093 (2007) ("[D]isclosure schemes comport with the prevailing political philosophy in that disclosure preserves individual choice while avoiding direct governmental interference.").

[11] *See* Calo, *supra* note 10, at 1048; *see also* Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 682 (noting that notice "looks cheap" and "looks easy").

an individual's consent.[12] Individual privacy preferences vary, and people who place a low value on privacy should be able to exchange it for goods, services, or information that they value more highly.[13] The mechanism prevents the setting of an arbitrary floor or ceiling for privacy.[14]

Partly as a result, notice and choice avoids the overregulation of legitimate business interests.[15] "[R]igid restrictions" resulting from overregulation can stifle innovation and competition, but the mechanism's emphasis on user autonomy prevents this.[16] In other words, notice and choice is seen as an alternative to statutory and administrative regulation.

2. *Criticisms of Notice and Choice*

Despite its claimed advantages, the notice and choice system faces many criticisms. Most of these criticisms focus on the mechanism's tendency to mis- or under-inform, its impracticality (in terms of costliness and scope), the extent to which users' cognitive hurdles limit its effectiveness, and the effect of creating undesirable externalities.

---

[12] Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 ISJLP 425, 440 (2011) (*citing* M. Ryan Calo, *A Hybrid Conception of Privacy Harm* (Draft) PRIVACY LAW SCHOLARS CONF., 28 (2010).

[13] *See* Calo, *supra* note 10 (*citing* James P. Nehf, *Shopping for Privacy Online: Consumer Decision Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J.L. TECH. & POL'Y 1, 14–17 (2007)).

[14] *See* Calo, *supra* note 10; *see also infra* note 15.

[15] *See* Calo, *supra* note 10, at 1049-50; *see also* Kenneth A. Bamberg & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 303 (2011) ("The shortcomings of command-and-control governance…are well recognized."); Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn From Environmental Law*, 41 GA. L. REV. 1, 9–11, 33–37 (2006) (arguing that "command-and-control type regulations would not be a good fit for the highly diverse and dynamic digital economy" due to the expense and threat to innovation.").

[16] *See* Calo, *supra* note 10, Calo argues that notice may be "more palatable to regulated industry." *Id.* As he puts it: "Mandated notice can and does face opposition, but opposition tends to be less fierce than do top-down dictates regarding what a company can and cannot do. Regulators, eager to do something to help consumers, but lacking the political capital or will to limit or curtail the activities of a given industry, may opt for notice as a means at least to improve the context of online privacy for some consumers." *Id.*

a. *Inadequate Information*

The notice and choice mechanism is often criticized for leaving users uninformed—or misinformed, as people rarely see, read, or understand privacy policies.[17] Critics argue that users who do not read privacy policies become uninformed consumers who can neither "protect[ ] themselves [n]or polic[e] the market."[18] And even if people do read the policies, they are unlikely to understand them, as policies are often long and filled with legal jargon.[19] Thus, policy readers often make "woefully incorrect assumptions" about how websites protect their privacy.[20]

---

[17] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1885 (2013) (*citing* Jon Leibowitz, Fed. Trade Comm'n, So Private, So Public: Individuals, the Internet & the Paradox of Behavioral Marketing, Remarks at the FTC Town Hall Meeting on Behavioral Advertising: Tracking, Targeting, & Technology (Nov. 1, 2007) (transcript available at http://www.ftc.gov/ speeches/ leibowitz/ 071031ehavior/ pdf). Paul Ohm refers to these issues as "information-quality problems." *See* Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907, 930 (2013). Daniel J. Solove refers to this as "the problem of the uninformed individual." *See* Solove, *supra* note 17.

[18] *See* Calo, *supra* note 10; *see also* Sarah Gordon, Symantec Security Response, Privacy at 12 (2003), *available at* http://www.symantec.com/avcenter/reference/privacy. attitudes .behaviors.pdf (noting that only three people out of a sixty-three-member study reported reading a privacy policy); Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 671 (2011) (noting that readership of boilerplate language "is effectively zero"). Additionally, a 2002 Yahoo report suggested that fewer than 1% of the website's visitors read its privacy policy. *See* MacCarthy, *supra* note 12, at 436; *see also* Fred H. Cate, The Failure of Fair Information Practice Principles, *in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 361 (Jane K. Winn ed., 2006)).

[19] *See* Bianca Bosker, *Facebook Privacy Policy Explained: It's Longer than the Constitution*, HUFFINGTON POST (Apr. 8, 2014 12:47 PM), http://www.huffingtonpost.com / 2010/05/12/facebook-privacy-policys_n_ 574389.html; *see also* Guilbert Gates, *Facebook Privacy: A Bewildering Tangle of Options*, N.Y. TIMES (Apr. 8, 2014 12:50 PM), http://www.nytimes.com/interactive/ 2010/05/12/ business/facebook-privacy.html?ref= personaltech (providing an infographic representing the webpages and subpages of Facebook and the privacy settings associated with each, as well as the word counts of other popular websites' privacy policies, as of May 21, 2010).

[20] *See* Solove, *supra* note 17, at 1886. Solove cites two studies revealing gross misinformation on the part of users. In one, people correctly answered questions about the privacy of their online transactions only 30% of the time. *See* Joseph Turow et al., Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It, 20-21 (Sept. 29, 2009) (unpublished manuscript) (available at http://ssrn.com/paper=1478214.). In another, "64% [of the people surveyed] do not know that a supermarket is allowed to sell other companies information about what they buy." *See* JOSEPH TUROW, LAUREN FELDMAN & KIMBERLY MELTZER, OPEN TO EXPLOITATION: AMERICAN SHOPPERS ONLINE AND OFFLINE (Univ. of Pa., Annenberg Pub. Policy Ctr. 2005), *available at* http://www.annenbergpublicpolicycenter.org/ downloads/information_and_ society/turow_appc_report_web_final.pdf. That same study revealed that 75% of study

b. *Impracticality*

The notice and choice mechanism is impractical. To start, there are simply too many privacy policies to keep track of, given the potentially hundreds of websites a user might visit on any given day.[21] To read all of these privacy policies would be extremely time consuming[22] and extremely costly.[23]

To complicate matters, users' multiple online interactions make it nearly impossible for users to control the online flow of data about them. Typically, websites contract with third parties who collect, track, or analyze visitor data. Such an arrangement makes it difficult for visitors to know or control what happens to their data.[24] Additionally, websites' privacy policies do not govern other connected third party websites, so first party websites cannot inform users as to

---

respondents incorrectly believed that the existence of a privacy policy meant that the website would not disclose user information with other entities. *See id.*

[21] *See* Ohm, *supra* note 17; Ben-Shahar & Schneider, *supra* note 18 (describing the "overload effect" in online disclosure). Daniel Solove refers to this as "the problem of scale." *See* Solove, *supra* note 17,at 1888-89. He puts it this way:

> "The problem is reminiscent of the beleaguered student whose professors collectively assign too much reading each night. From the perspective of each professor, the reading is a reasonable amount for an evening. But when five or six simultaneously assign a night's worth of reading, the amount collectively becomes too much. Thus, even if all companies provided notice and adequate choices, this data management problem would persist; the average person just does not have enough time or resources to manage all the entities that hold her data."

Solove, *supra* note 17, at 1889.

[22] Lorrie Cranor estimates that it would take a user an average of 244 hours per year to read the privacy policy of every website she visited. *See* Lorrie Faith Cranor, *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. TELECOMM. & HIGH TECH. L. 273, 274 (2012). This translates to about 54 billion hours per year for every U.S. consumer to read all the privacy policies he or she encountered. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP 543, 563 (2008).

[23] A Carnegie Mellon study estimated that it would cost $781 billion if every U.S. worker read each privacy policy he or she encountered. *See* McDonald and Cranor, *supra* note 22 at 564–65.

[24] *See* Cranor, *supra* note 22; *see also* MacCarthy, supra note 12, at 436–37 ("Privacy policies for the first-party websites that users interact with are difficult enough for users to understand, but when third-party sites enter the mix, the notion of effective privacy notice becomes completely untenable."); Solove, *supra* note 17 (referring to "the problem of scale").

how third parties use the data they collect from visitors.[25] The notice and choice framework does not obtain user consent for such secondary information use.[26] Accordingly, this "potentially unending chain of actors" means that "there is a degree to which the tracking, analysis, and use (current and future) of data is not only difficult to grasp, but unknowable."[27]

Related to the problem of data control is the problem of aggregation.[28] Though people might make reasonable decisions about revealing pieces of information based on the contents of one privacy policy, they may not realize that, in the future, these bits could be aggregated into a bigger picture that reveals sensitive information.[29] Because users have difficulty understanding the effects of future aggregation, they have difficulty assessing future harm and are thus

---

[25] *See* Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, PROC. OF THE ENGAGING DATA FORUM: THE FIRST INT'L FORUM ON THE APPLICATION AND MGMT. OF PERSONAL ELECTRONIC INFO. (Oct. 2009), *available at* http://www.nyu.edu/projects/nissenbaum/main_cv.html#pub. The authors note that, for example, as of July 27, 2009, NYTimes.com lists 14 common user-tracking advertising services not governed by the website's privacy policy. *See id.* at 5. The result of this structure is that users cannot "fathom" five points that are crucial for making an informed choice: "(1) Which actors have access [...]; (2) What information they have access to [...]; (3) What they do or may do with [the] information; (4) Whether the information remains with the publisher or is directly or indirectly conveyed to third parties; and (5) What privacy policies apply to the publisher compared to [ ] all the third parties, assuming these are even known to the users." *Id.*

[26] MacCarthy, *supra* note 12, at 436 (*citing* Fred H. Cate, The Failure of Fair Information Practice Principles, in CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY. 361 (Jane K. Winn ed., 2006)).

[27] *See* Barocas & Nissenbaum, *supra* note 25.

[28] *See* Solove, *supra* note 17, at 1889–90 (2013). Solove explains:

> "Suppose a person gives out an innocuous piece of data at one point in time, thinking that he or she is not revealing anything sensitive. At other points in time, the person reveals equally nonsensitive data. Unexpectedly, this data might be combined and analyzed to reveal sensitive facts about the person. The person never disclosed these facts nor anticipated that they would be uncovered. The problem was that the person gave away too many clues. Modern data analytics...can deduce extensive information about a person from these clues. In other words, little bits of innocuous data can say a lot in combination."

Id.

[29] *See* Solove, *supra* note 17, at 1889–90.

unable to engage in an analysis of the long-term costs and benefits associated with divulging information.[30]

Another criticism is that website privacy policies often give websites the right to change their policies and relationships with third parties at any time.[31] Here, the implication is that users will be expected to constantly re-check a website's privacy policy (and the policies of affiliated third parties, too) to keep abreast of a site's current privacy practices.[32] In reality, to do this would prove immensely burdensome in terms of time and money.[33] Such malleability for websites reveals how "flimsy" privacy commitments can be,[34] "even if [a user] were to vigilantly follow the privacy policies of the relevant actors, [she] may find that prior commitments no longer apply retroactively."[35]

c. *Cognitive Hurdles*

One scholar claims that the notice and choice mechanism is ineffective because humans suffer from "bounded rationality and cognitive biases."[36] This is illustrated by another study that reported survey participants erroneously believed that the mere existence of a website privacy policy meant the company promised not to share personal information.[37] Other studies suggest that the way a company

---

[30] Solove, *supra* note 17, at 1891. Solove explains that this occurs because privacy harms are "cumulative in nature," and that "harmful effects may only emerge from the downstream uses of the combination of data." *Id.*

[31] *See* Barocas & Nissenbaum, *supra* note 25.

[32] *See* Barocas & Nissenbaum, *supra* note 25; *see also* Solove, *supra* note 17, at 1888–89 ("And many entities frequently modify their privacy policies, so reading them all just once is not enough.").

[33] See *supra* notes 21 and 22 (discussing the amount of time and cost in dollars it would take for website visitors to read privacy policies).

[34] *See* Barocas & Nissenbaum, *supra* note 25.

[35] *See* Barocas & Nissenbaum, *supra* note 25.

[36] *See* Ohm, *supra* note 17, at 931.

[37] *See* Ohm, *supra* note 17, at 931; *see also* Joseph Turow, et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 ISJLP 723, 730–32 (2008).

expresses privacy terms (often in vague or uncertain language) has an effect on whether users accept those terms.[38]

d. *Negative Externalities*

The notice and choice mechanism is also criticized for creating "negative privacy externalities."[39] For example, one person's disclosure of information may reveal information about other parties, possibly to their detriment.[40] In this regard, notice and choice's focus on individual consent dooms the mechanism to "fail[ ] to account for the social impacts of individual privacy decisions."[41]

---

[38] *See* Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES § 18.3.2, at 370 (Alessandro Acquisti et al. eds., 2008). For example, consumers trust the privacy policies of aesthetically pleasing websites. *See id.* at 371. Additionally, prospect theory, the endowment effect, and hyperbolic discounting help explain people's failures when assessing privacy risks. *See id.* at §§ 18.3.2, 18.3.3, at 371–72. Prospect theory is the framework that "provides an interpretation of how individuals evaluate and compare uncertain gains and losses." *Id.* at 371. The endowment effect is the phenomenon whereby individuals value a good in their possession more highly than they would value the same good if it were not in their possession. *See id.* at 372. Hyperbolic discounting is the "idea that people do not discount distant and close events in a consistent way." *Id.*

[39] *See* MacCarthy, *supra* note 12, at 428–29.

[40] *See* MacCarthy, *supra* note 12, at 428–29. MacCarthy provides a few illustrative examples. For instance, an analysis of a person's social network friends may reveal details about his or her sexual orientation. *See id.* at 429 (*citing* Matthew Moore, *Gay Men 'Can Be Identified by Their Facebook Friends'*, THE TELEGRAPH (Sept. 21, 2009), http://www.telegraph.co.uk/technology/facebook/6213590/Gay-men-can-be-identified-by-their-Facebook-friends.html). Negative privacy externalities also arise in the context of "eligibility decisions, where those with a favored characteristic have an incentive to disclose, thereby outing those who remain silent." *Id.* For example, people who do not smoke will reveal so much to their health insurance companies, who then might be able to identify smokers based on their lack of such a disclosure. *Id.*

[41] *See* Solove, *supra* note 17, at 1892 ("Individual privacy has a variety of social functions."). *See also* Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1221 (2002) ("[I]nformation privacy should be conceptualized as a norm constitutive of a democratic society."); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 882–83 (2003) ("Society as a whole has an important stake in the contours of the protection of personal information."); Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 709 (1987) ("[P]rivacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone."); Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 959 (arguing that the tort of invasion of privacy "does not simply uphold the interests of individuals against the demands of community, but instead safeguards rules of civility that in some significant measure constitute both individuals and community."); Paul M. Schwartz, *Privacy and Democracy*

e. *FTC Response to Notice and Choice Issues*

The intent of a notice and choice regime is to enable users to make meaningful, informed decisions regarding their privacy. For a user to have control over his or her privacy, he or she must be able to both understand the consequences and control the disclosure of his or her personal information.[42] The reality, however, is that "individuals often lack complete information about the consequences of information disclosure as well as mechanisms for ensuring that their information is disclosed only in the ways they desire."[43]

Accordingly, in 2010, the FTC staff noted that the "notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand," and recommended that "[p]rivacy notices should be clearer, shorter, and more standardized, to enable better comprehension and comparison of privacy practices."[44]

B. Litigated Privacy Harms and Notice and Choice

Aside from the theoretical perspective on notice and choice, individuals and the FTC perceive online privacy harms that warrant redress. When individuals experience significant wrongs, they will seek redress for those privacy harms through litigation. Similarly, when the FTC perceives commercial practices that cause significant harm to consumers, the agency will bring enforcement actions. These litigation events serve as a valuable proxy for the privacy harms that matter most to the public. By looking at both types of litigation events together, a general set of critical harms can be identified, though other harms may also exist and not be litigated because the practices are hidden.[45] These litigated harms can offer a window on the theory

---

in Cyberspace, 52 VAND. L. REV. 1609, 1613 (1999) ("The Internet's potential to improve shared life in the United States will be squandered unless we structure the kinds of information use necessary for democratic community and individual self-governance.").

[42] *See* Cranor, *supra* note 22, at 278 (*citing* LORRIE FAITH CRANOR, PRIVACY POLICIES AND PRIVACY PREFERENCES, *in* SECURITY AND USABILITY: DESIGNING SECURE SYSTEMS THAT PEOPLE CAN USE 448 (Lorrie Faith Cranor & Simson Garfinkel, eds., 2005).

[43] *See Id*. at 278-79.

[44] Press Release, Fed. Trade Comm'n, FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010).

[45] Other studies have addressed issues either with respect to the FTC or with respect to specific litigation, but none have provided a full picture. *See, e.g.*, Sasha Romanosky, David A. Hoffman, & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*,

about the effectiveness of the notice and choice framework. In other words, the privacy harms must be able to align with the privacy protections of notice and choice.

III. PRIVACY EVENTS AND HARMS

With the goal in mind of identifying the alignment between privacy harms, and "notice and choice," the data set compiled to support the research for this Article consisted of (i) all federal class action complaints alleging online privacy violations filed during the period from the first FTC online privacy complaint (February 12, 1999) to November 11, 2013 and (ii) all Federal Trade Commission complaints and settlements addressing online privacy over the same period. This universe of litigation was analyzed to identify particular types of privacy harms in search of redress through legal proceedings.[46] For reasons described below, separate methodologies were used to identify the online privacy federal class actions and FTC actions.

A. *Litigation*

To determine which online privacy issues are important to consumers, federal class action lawsuits that alleged violations of consumers' privacy rights were analyzed. The rationale is that these lawsuits serve as a proxy for the harms that were most significant to consumers when they became aware of specific data practices.

1. *Search Parameters*

To find class action lawsuits, keyword searches were conducted in the Pleadings Index available on the Westlaw Next electronic legal database.[47] To determine the search parameters, search terms were

---

J. EMPIRICAL LEGAL STUD., (forthcoming), *available at* http://ssrn.com/ abstract= 1986461 (analyzing breach litigation); Woodrow Hartzog & Daniel J. Solove, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014) (discussing FTC cases).

[46] *See* Joel R. Reidenberg, N. Cameron Russell, Alexander J. Callen, and Sophia Qasir, *Privacy Enforcement Actions* (Fordham CLIP: June 2014), *available at* http://law.fordham.edu/assets/CLIP/CLIP_Privacy_Case_Report_-_FINAL.pdf (cataloging and listing all the cases compiled for this Article).

[47] WestlawNext - "Trial Court Documents – Pleadings." This database offers full-text search for complaints, answers, petitions, and other pleadings. Document type was restricted to "Civil Complaints."

selected that would necessarily have to be included in any substantial class action litigation concerning Internet privacy policies. To cast the broadest possible net of relevant terms, the search was structured to include the following Boolean search term: "personal information" & "data" & "privacy" & "online" & "class action!"

While the results included some false positives, this approach both ensured that all sufficiently relevant cases are were identified and reduced the risk that a relevant case might be omitted from the final report. This approach also assures that others can reproduce the search using the same search terms in the database described, and can update the search, as needed, in the future.

The search was limited temporally to private class action complaints filed between February 12, 1999 and November 11, 2013. This date filter was applied to garner meaningful results capturing the current trends, as well as match the period of FTC online privacy cases. It also provided a manageable number of results.[48]

2. *Results*

This search generated 661 federal cases. These results were narrowed to 620 relevant cases in federal court proceedings. The complaints for these proceedings were then individually reviewed and filtered according to document type and content. Non-complaint documents that had been included within the search results (such as Petitions), cases unrelated to online privacy (such as securities-related cases, or those alleging offline or non-privacy related deceptive trade practices), and those involving online privacy issues on mobile devices were excluded from review Any duplicate complaints were also omitted. When an amended complaint was included, only the most recent complaint was reviewed and added to the data set.

Frequently, many complaints were filed arising from the same event or incident. For example, forty-nine complaints were filed against Sony Computer Entertainment America arising from a data breach that exposed customers' personally identifiable information; twenty-four complaints were filed against Countrywide Financial Corporation for unauthorized disclosure of customer information; and three complaints were filed against Google for collecting unencrypted data sent over wireless networks that was gathered while collecting

---

[48] The ultimate search inquiry read: advanced: (personal & information & data & privacy & online) & ("Class Action") & DA(aft 01-01-2003) & DT(((COMPLAINT PETITION) % (REPLY RESPONSE ANSWER COUNTER-CLAIM COUNTER-PETITION CROSS-CLAIM COUNTER-COMPLAINT))).

images for Google Street View.[49] In instances such as these, we made a determination as to whether a group of complaints arose from a single "discrete event," and, if so, the event was used as the trigger for the harm analysis. We based this determination on the identity of the named defendant, the date the action was filed, the allegations contained in the complaint, and the asserted causes of action.

Ultimately, the data set for analysis consisted of 165 class action cases arising from approximately eighty-nine discrete events.

3. *Role of Jurisdiction and Competence*

Private litigants who sue in federal court for violations of online privacy rights bring claims under federal, state, and common law. The types of claims that litigants could bring were limited by three main factors: (1) litigants' ability to establish standing, (2) pleading a cognizable cause of action, and (3) plausibly alleging a class action.

This section will discuss the ability of private party litigants to bring class action suits for online privacy violations in terms of these three potential limitations.

a. *Standing*

The U.S. Constitution limits those who can bring suit through the Article III standing requirement. A plaintiff can only bring an action against a party who caused the plaintiff to suffer a concrete and particularized injury that is capable of redress.[50] A remote or speculative injury is insufficient to establish standing.[51]

Standing is particularly difficult to establish in online privacy cases because the nature of the harm has not yet been defined.[52] Whether a putative class can establish standing may depend on the asserted cause of action.[53] Although lack of standing is a defense that

---

[49] Privacy Enforcement Actions, *infra* note 58, at 27–28.

[50] Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992); Raines v. Byrd, 521 U.S. 811 (1997).

[51] *Lujan*, 504 U.S. at 556 (holding that environmentalists lacked standing to challenge the Endangered Species Act because they had no concrete plan to visit the affected species); *see also* Low v. LinkedIn, 900 F. Supp. 2d 1010 (N.D. Cal. 2012) (holding that plaintiffs lacked standing because they failed to assert a concrete and particularized injury).

[52] *See, e.g.*, Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 477 (2010).

[53] *See, e.g.*, *Low,* F. Supp. 2d at 1021, 1028–29 (holding that plaintiffs had standing under the Stored Communications Act, but not under the False Advertising Law); Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 861 (N.D. Cal. 2011) (finding that plaintiffs had met

the defendant may assert, a party seeking to bring a lawsuit must nevertheless establish at the pleading stage that they suffered an injury or one of their legally cognizable rights was invaded.[54]

Furthermore, because our study was limited to complaints filed in federal court, litigants must satisfy the requirements for federal jurisdiction. This requirement, however, is not likely a significant bar to bringing suit within this study's data set because, as discussed below, many complaints alleged claims arising under federal law.

b. *Cause of Action*

The greatest limit on bringing an action for an invasion of online privacy is establishing or determining a cause of action. While the complained-of conduct may fit into common law causes of action, such as breach of implied contract, conversion, or negligence, for example, there are few statutory and no common law actions that deal directly with issues of online privacy. Scholarship in the field highlights the gaps in existing law and demonstrates the need for, and provides suggestions for, significant reform in this area.[55]

c. *Class Action Requirement*

If a cause of action is available, litigants will still need to establish eligibility for class certification. To be certified as a class action, a putative class must meet the requirements of Rule 23 of the Federal Rules of Civil Procedure. Under Rule 23 (a):

---

the general pleading requirements for standing, but had failed to allege more particularized elements of the injury for individual cases of action). *But see In re* Facebook Privacy Litig., 791 F. Supp. 2d 705 (N.D. Cal. 2011) (finding that plaintiffs had standing to bring claim under the Wiretap Act).

[54] *Claridge*, 785 F. Supp. 2d at 861.

[55] *See, e.g.*, Reidenberg, *supra* note 41; Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85 (2002); Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91 (2009); Timothy J. Van Hal, Note, *Taming the Golden Goose: Private Companies, Consumer Geolocation Data, and the Need for a Class Action Regime for Privacy Protection*, 15 VAND. J. ENT. & TECH. L. 713 (2013). For a contrasting view, see Catherine Schmierer, *Better Late than Never: How the Online Advertising Industry's Response to Proposed Privacy Legislation Eliminates the Need for Regulation*, 12 RICH. J.L. & TECH. 13 (2011).

> "(1) the class [must be] so numerous that joinder of all members is impossible, (2) there are questions of law or fact common to the class; (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; and (4) the representative parties will fairly and adequately protect the interests of the class."[56]

If the class is seeking money damages under Rule 23(b)(3), then, in addition to fulfilling the requirements of Rule 23(a), the class must establish that the common questions of law or fact are predominant to any individualized issues, and that litigating the issue as a class action is the superior method of resolving the dispute fairly and efficiently.[57]

Although the issue of class certification is litigated after the initial pleading stages, the issue is nevertheless relevant at the pleadings stage because the putative class must at least plausibly establish its appropriateness in the complaint. The class action pleading requirement, however, is likely not a significant deterrent to filing suits involving invasions of online privacy because whether a company engaged in actionable conduct would affect many, if not all, of the company's customers.

4. *Federal Claims*

This section will discuss the most common federal statutory provisions under which litigants sue.[58] Most of the reviewed complaints were brought under three federal statutes: the Stored Communications Act[59] (59 cases, 36 percent), the Electronic

---

[56] FED. R. CIV. P. 23(a).

[57] FED. R. CIV. R. 23(b)(3).

[58] For a detailed overview of the claims asserted, see Joel R. Reidenberg, N. Cameron Russell, Alexander J. Callen, and Sophia Qasir, Privacy Enforcement Actions (Fordham CLIP: June 2014) http://law.fordham.edu/assets/CLIP/CLIP_Privacy_Case_Report_-_FINAL.pdf (hereinafter "Privacy Enforcement Actions") (cataloging and listing all the cases compiled for this Article.).

[59] Stored Communications Act, Pub. L. No. 99–502, 100 Stat. 1860 (codified as amended at 18 U.S.C. §§ 2701–2711 (2006)).

Communications Privacy Act[60] (82 cases, 50 percent), and the Computer Fraud and Abuse Act[61] (51 cases, 31 percent).[62]

The Stored Communications Act (SCA) makes it illegal for someone to, without permission, "obtain[ ], alter[ ], or prevent[] authorized access to[,] a wire or electronic communication while it is in electronic storage."[63] The statute also provides a civil cause of action for private litigants that specifies a minimum penalty of $1,000 and allows for the availability of punitive damages.[64]

The Electronic Communications Privacy Act (ECPA) also provides a private right of action. ECPA makes it unlawful to "intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[65] ECPA allows prevailing plaintiffs to collect as damages the greater of $100 per day for each day of the violation or $10,000.[66]

The Computer Fraud and Abuse Act (CFAA) is an anti-hacking statute that prohibits unauthorized individuals from accessing or conspiring to access a computer for restricted data.[67] The CFAA provides a private right of action and allows individuals who have suffered damage or sustained a loss due to a violation of this statute to collect compensatory damages, injunctive relief, or other equitable relief.[68]

---

[60] Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

[61] Computer Fraud and Abuse Act of 1986, Pub. L. No. 99–474, 100 Stat. 1213 (codified as amended at 18 U.S.C. 1030).

[62] Privacy Enforcement Actions, *supra* note 58, at 30. As class action complaints commonly plead multiple causes of action, the percentage breakdown, when totaled, exceeds 100 percent.

[63] 18 U.S.C. § 2701 (a).

[64] *Id.* at § 2707 (c).

[65] *Id.* § 2511(1)(a).

[66] *Id.* § 2520(c)(2).

[67] *Id.* § 1030(a). The CFAA also includes a criminal component for unauthorized access of government computers or accessing information relating to the national defense or foreign affairs. *Id.* Discussion of those provisions, however, is beyond the scope of this Article.

[68] *Id.* § 1030(g).

5. *Ancillary State Law Claims*

This section will discuss the most frequent state law claims asserted under ancillary jurisdiction in federal litigation.[69] These state claims involve both statutory law and state common law. The most frequent statutory state law claims arose under California law, including California's Unfair Competition Law[70] (76 cases, 46 percent), the Consumer Legal Remedies Act[71] (47 cases, 28 percent), Computer Criminal Law[72] (36 cases, 22 percent), Invasion of Privacy[73] (22 cases, 13 percent), and False Advertising Law[74] (13 cases, 8 percent), among others.[75]

Privacy claims are often brought under state statutes prohibiting unfair competition and deceptive business practices that harm consumers.[76] Courts tend to determine whether a practice is "unfair" or "deceptive" on an ad hoc basis, depending on the particular context. For example, some online privacy complaints alleged that websites' engaged in unfair or deceptive practices when they told consumers that they would not share or disclose personally identifiable information and then did so.[77] Other complaints alleged that websites misled consumers about what personal information would be collected.[78] In California, the violation of the Unfair Competition Law

---

[69] For a more detailed overview of the claims asserted, see Privacy Enforcement Actions, *supra* note 58 (cataloging and listing all the cases compiled for this Article).

[70] CAL. BUS. & PROF. CODE § 17200 (West 2014). Of the reviewed complaints, 76 alleged violation of the California Unfair Competition Law.

[71] CAL. CIVIL CODE § 1750 (West 2014).

[72] CAL. PENAL CODE § 502 (West 2014).

[73] CAL. PENAL CODE § 630 (West 2014).

[74] CAL. BUS. & PROF. CODE § 17500 (West 2014).

[75] The percentages do not equal 100% due to overlaps in the case claims. Because most reviewed complaints were filed in California, they tended to assert California state law claims. Litigants, however, have also brought claims under unfair or deceptive trade practice statutes of various other states, including Florida, Illinois, Massachusetts, New York, and Texas. *See Privacy Enforcement Actions*, *supra* note 58, at 30–31.

[76] *See Privacy Enforcement Actions*, *supra* note 58, at 30-31.

[77] *See* Privacy Enforcement Actions, *supra* note 58.

[78] *See* Privacy Enforcement Actions, *supra* note 58.

entitles prevailing plaintiffs only to injunctive relief or restitution.[79] The Consumer Legal Remedies Act (CLRA) also prohibits unfair and deceptive trade practices.[80] Unlike the Unfair Competition Law, however, the CLRA allows prevailing to litigants to collect damages,[81] punitive damages,[82] and reasonable attorneys' fees.[83]

Another set of statutory privacy claims arise under state computer crime laws enacted to parallel the federal Computer Fraud and Abuse Act.[84] For example, California's Computer Crimes Law makes it unlawful for any individual to gain unauthorized access to a computer, computer system, or computer network.[85] In addition to imposing criminal penalties, the statute allows injured parties to bring a civil action to recover compensatory damages or seek injunctive relief.[86] Private litigants may also be entitled to recover attorneys' fees.[87]

Lastly, there are also a number of specific state statutes addressing invasions of privacy that are asserted by litigants.[88] For example, the California state legislature enacted an "Invasion of Privacy" statute to protect the "free exercise of personal liberties" that is threatened by technological developments of devices that eavesdrop on private communications and invade citizens' privacy rights.[89] Although the invasion of privacy statute is a criminal statute, injured parties may bring civil actions for damages, to recover the greater of $5,000 or treble damages sustained by the plaintiff, or for injunctive relief.[90]

---

[79] CAL. BUS. & PROF. CODE § 17203 (West 2014). If the state attorney general or a district attorney brings a civil action on behalf of the people of the State of California, then the violator may be subject to a civil penalty not exceeding $2,500 per violation. *Id.* § 17206.

[80] *See* CAL. CIVIL CODE § 1770 (listing practices proscribed by the statute).

[81] In a class action, the total award of damages must be greater than $1000. CAL. CIV. CODE § 1780(a)(1).

[82] CAL. CIV. CODE § 1780(a)(4).

[83] CAL. CIV. CODE § 1780(e).

[84] *See Privacy Enforcement Actions*, *supra* note 58, at 30-31.

[85] CAL. PENAL CODE § 502(c).

[86] CAL. PENAL CODE § 502(e)(1).

[87] CAL. PENAL CODE § 502(e)(2).

[88] *See Privacy Enforcement Actions*, *supra* note 58, at 30–31.

[89] CAL. PENAL CODE § 630.

[90] CAL. PENAL CODE § 637.2.

Unlike other statutes, a plaintiff (or class of plaintiffs) need not sustain, or be threatened with, actual damages.[91]

With respect to the common law, complaints frequently allege a number of contract and quasi-contractual claims, such as breach of contract (52 cases, 32 percent), breach of implied contract (29 cases, 18 percent), breach of the implied covenant of good faith and fair dealing (19 cases, 12 percent), and breach of express or implied warranty (7 cases, 4 percent).[92] Litigants also include claims for a range of common law torts, including negligence (36 cases, 22 percent), intentional or negligent misrepresentation (7 cases, 4 percent), a privacy tort[93] (65 cases, 39 percent), conversion (17 cases, 10 percent), bailment (7 cases, 4 percent), and unjust enrichment (87 cases, 53 percent).[94]

Complaints alleging contractual claims proceed on the premise that the privacy policy creates a contract between the website and the user, and that the policy will govern the website's use of individuals' personally identifiable information.[95] Contract claims have been brought for a range of cases.[96] In these suits, litigants allege that websites collected or disseminated private information—even if the user may have initially disclosed that information voluntarily. For example, litigants sued Facebook over the "Friend Finder Service" because the tool used images of the user for advertising purposes.[97] Intrusion upon seclusion and public disclosure of private fact claims

---

91 CAL. PENAL CODE § 637.2(c).

92 *See Privacy Enforcement Actions*, *supra* note 58, at 31–32.

93 Privacy torts are categorized as one of four possible actions: intrusion upon seclusion, public disclosure of private fact, false light, and appropriation.

94 *See Privacy Enforcement Actions*, *supra* note 58, at 31–32 for a full range of the claims raised by litigants in online privacy lawsuits.

95 *See, e.g.*, Gould v. Facebook, Inc., Case No. 10-cv-02389 (N.D. Cal. Dec. 10, 2010); Robertson v. Facebook, Inc., Case No. 10-cv-02408 (N.D. Cal. June 1, 2010); Claridge v. Rockyou, Inc., Case No. 09-cv-06032-PJH (N.D. Cal. Apr. 11, 2011); Carson v. Lendingtree LLC, Case No. 08-cv-00247 (W.D.N.C. May 30, 2008); Yunker v. Pandora Media, Case No. 11-cv-3113 (N.D. Cal. Mar. 26, 2013); *In re* LinkedIn User Privacy Litig., Case No. 12-cv-03088 (N.D. Cal. Mar. 28, 2014); Johnson v. Microsoft, Inc., Case No. 06-cv-00900-RSM (W.D. Wash. July 28, 2011); *see also* Privacy Enforcement Actions, *supra* note 58.

96 *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960); *see also* Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 8–9 (2007) (noting that Prosser's four categories of privacy torts have been incorporated into modern American jurisprudence).

97 *See* Cohen v. Facebook, Inc., Case No. 10-cv-05282-RS (N.D. Cal. Aug. 11, 2011).

were also raised against companies that allegedly installed spyware that directed users' communications to a third party advertiser,[98] failed to secure users' personal information,[99] made users' search data available on a public website,[100] or shared customer information without consent.[101] False light claims were alleged when a website aggregated online activity of users to create and sell databases based on their interests and preferences.[102] General invasion of privacy claims were asserted in cases where the defendant circumvented users' browser's privacy settings to collect information[103] or collected (or disseminated) information without users' consent.[104]

Less frequent, but also asserted by litigants, were the common law claims for two variants to trespass to property.[105] The first was conversion. Conversion is a civil equivalent for a theft infraction—when one person exercises a property right inconsistent with that of another.[106] In an online context, litigants have asserted claims for

---

[98] *See, e.g.*, Valentine v. Wideopen W. Fin., Case No. 09-cv-07653 (N.D. Ill. Mar. 26, 2012); Green v. Cable One, Inc., Case No. 10-cv-00259 (N.D. Ala. Feb. 3, 2010); Mortensen v. Bresnan Commc'n, Case No. 10-cv-00013 (D. Mont. July 15, 2013).

[99] *See, e.g.*, Penson v. Amazon, Case No. 12-cv-00340 (W.D. Ky. Sept. 27, 2012); Elliot v. Amazon, Case No. 12-cv-00341 (W.D. Ky. Sept. 27, 2012); Stevens v. Amazon, Case No. 12-cv-00339 (W.D. Ky. Sept 27, 2012); Carson v. Lendingtree LLC, Case No. 08-cv-00247 (W.D.N.C. July 23, 2008); Spinozzi v. Lendingtree LLC, Case No. 08-cv-00229 (W.D.N.C. July 23, 2008); Low v. LinkedIn Corp., Case No. 11-CV-01468-LHK (C.D. Cal. July 12, 2012).

[100] *See, e.g.*, Doe v. AOL LLC, Case No. 06-cv-05866 (N.D. Cal. Jan. 16, 2009).

[101] *See, e.g.*, Gaos v. Google, Inc., Case No. 10-cv-04809 (N.D. Cal. Mar. 29, 2013); Walker v. Facebook, Case No. 12-cv-00798 (D. Mont.); Quinn v. Facebook, Case No. 12-cv-00797 (D. Haw.).

[102] Complaint, Couch v. Space Pencil, No. 05606, 2011 WL 5924382 (N.D. Cal. Sept. 14, 2011); *see also* Gutierrez v. Instagram, Inc., No. 6550, 2012 WL 6709572 (N.D. Cal. Dec. 27, 2012).

[103] *See, e.g.*, Frohberg v. Media Innovative Grp. LLC, Case No. 12-cv-02674-WFK-JO (E.D.N.Y.); Mazzone v. Vibrant Media Inc., Case No. 12-cv-02672-NGG-JO (E.D.N.Y.); *In re* Google Inc. Cookie Placement Consumer Privacy Litig., Case No. 12-md-02358-SLR (D. Del.).

[104] *See, e.g.*, Virtue v. Myspace, Inc., Case No. 11-cv-01800-RRM –RML (E.D.N.Y.) (bringing an invasion of privacy claim for the unauthorized disclosure of personal information and browsing history); Simios v. 180Solutions, Inc., Case No. 05-cv-05235 (N.D. Ill. Apr. 14, 2006) (Invasion of privacy claim asserted for causing spyware that tracked plaintiffs' Internet activity to be downloaded on users' computer).

[105] *See* Privacy Enforcement Actions, *supra* note 58.

[106] 18 AM. JUR. 2d *Conversion* § 80 (describing acts constituting conversion).

conversion in situations when a company uses the personal information of its users without proper compensation or permission,[107] circumvents privacy controls to collect personal information,[108] or fails to secure private information.[109]

The second set of trespass claims asserted is bailment infringements. Bailment exists when the owner of property (the bailor) entrusts another person (the bailee) with possession of property for a limited period, after which the bailee must return the property to the bailor.[110] Litigants proceeding with a claim for bailment in an online context alleged that they entrusted personal information to a website (the "bailor"), who then failed to keep that information secure.[111]

B. *Federal Trade Commission Enforcement Actions*

The enforcement actions of the Federal Trade Commission reflect the consumer harms that the FTC perceives to be most important and that fall within the FTC's jurisdiction. To determine the nature of these harms, we reviewed FTC complaints, which were available via the FTC website as of November 11, 2013 and which the FTC categorized as relating to privacy issues.

1. *Search Parameters*

The FTC categorized its enforcement actions and published the relevant complaints on the agency's website. These complaints were accessible from the FTC's homepage (http://www.ftc.gov/) by following the links to "Consumer Protection" → "Business Information" → "Legal Resources" → "Privacy and Security" on the

---

[107] *See, e.g.*, Gutierrez v. Instagram, Inc., Case No. C 12-6550 (N.D. Cal.); Low v. LinkedIn Corp., Case No. 11-CV-01468-LHK (C.D. Cal.); Leong v. Myspace, Case No. CV-10-8366 (C.D. Cal.); Gudac v. Zynga Games, Case No. 10-cv-04793 (N.D. Cal.).

[108] *See, e.g.*, Nobles v. Google, Inc., Case No. 12-cv-03589-LB (N.D. Cal.) (circumvented controls); Maguire v. Facebook, Inc., Case No. 12-cv-0807 (N.D. Cal.) (surreptitious collection); Feist v. RNC Corp., Case No. 11-cv-05436 (S.D.N.Y.) (monitored, intercepted, and manipulated users' search histories).

[109] *See, e.g.*, Elkhettab v. Countrywide Fin. Corp., Case No. 08-cv-00638 (C.D. Cal.).

[110] U.C.C. art. 7 (2003); 8A AM. JUR. 2d *Bailments* § 28.

[111] *See, e.g.*, Bell v. Blizzard Entm't., Case No. 12-cv-09475 (C.D. Cal.); Gutierrez v. Instagram, Inc., Case No. C 12-6550 (N.D. Cal.); Moses v. Countrywide Fin. Corp., Case No. 08-cv-05416 (C.D. Cal.); Funes v. Instagram, Inc., Case No. 12-civ-6482 (N.D. Cal.).

dropdown menu → "select subtopic" on the second dropdown menu. The relevant subtopics were: (1) Children's Privacy, (2) Consumer Privacy, (3) Data Security, and (4) the Gramm-Leach-Bliley Act.[112] No keywords or electronic searches were necessary to identify these cases, as the FTC's website provided a chronological list of cases for each of above-listed subcategories as of the research period for this study.

Some cases included multiple complaints. In these instances, only the oldest complaint for that case was reviewed.[113] The earliest complaint reviewed by Fordham CLIP dated to February 12, 1999, while the most recent complaint reviewed dated to October 22, 2013.

2. *Results*

According to the FTC's website, there were a total of 116 distinct cases.[114] The distribution of these cases, as of November 11, 2013, within the FTC's broad categories was as follows:

- Children's Privacy - 23 cases
- Consumer Privacy - 46 cases
- Data Security - 50 cases
- Gramm-Leach-Bliley Act - 26 cases

3. *Role of Jurisdiction and Competence*

The enabling statute of the FTC has a crucial impact on the way the FTC's privacy enforcement claims are brought. Congress passed the Federal Trade Commission Act (the "Act") on September 26, 1914 that established the FTC and sought to protect American consumers from wrongful business practices.[115] The Act, as amended, prohibits

---

[112] The report did not include FTC complaints subcategorized as relating to (1) Credit Reporting, (2) the Red Flags Rule, or (3) the U.S.-EU Safe Harbor, as these are not specifically relevant to online privacy, unless such complaints were cross-listed in one of the other four categories.

[113] There is one exception, where the second, newer complaint was used, because the FTC had a broken link to the oldest complaint for *In re Educational Research Center of America, Inc.; Student Marketing Group, Inc.; Marian Sanjana; and Jan Stumacher,* File No. 022 3249, Docket C-4079 (2003).

[114] *See Privacy Enforcement Actions*, *supra* note 58, at 4. Some cases involved multiple claims and were cross-listed among multiple categories.

[115] *See* ch. 311, 38 Stat. 717 (codified as amended at 15 U.S.C. §§ 41–58).

the "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce"[116] and empowers the FTC to enforce these prohibitions.[117] Congress has expanded the FTC's jurisdiction over the years, and today the FTC enforces or administers more than seventy laws, including a wide variety of consumer protection laws spanning areas from credit reporting to telemarketing.[118] For online privacy, however, the FTC's jurisdiction only extends to unfair and deceptive practices.

The enabling statute's limitation to unfair and deceptive practices severely circumscribes the agency's authority over online privacy issues. Despite the progressive expansion of its overall powers, the FTC still lacks explicit statutory authority to generally protect online consumer privacy. The FTC's general privacy efforts must rely on the authority under Section 5 of the Act to "prevent" persons "from using . . . unfair or deceptive acts or practices in or affecting commerce."[119]

The FTC has long defined a deceptive practice as a "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[120] Typically, the FTC looks to whether or not a person or company broke a promise or engaged in a misleading act. The archetypical scenario involves a company's breach of its own privacy policy. Under this deception theory, a company would be permitted, without repercussion, either to tell consumers whether and how their personal information will be exploited, provided it upholds its word; or to promise them nothing about their online privacy at all. In other words, under the deception theory, the FTC could pursue a company for violating its own privacy policy, but it could not require that company to have a privacy policy in the first place. Nor could it require specific provisions in a company's online privacy policy. This limited authority "leads to the curious situation whereby a company without a privacy policy is arguably less likely to be punished for

---

[116] *See* 15 U.S.C. § 45(a)(1).

[117] *See id.* §§ 41, 45.

[118] *See About the FTC*, FED. TRADE COMM'N, http://www.ftc.gov/about-ftc (last visited Feb. 24, 2014); *Statutes Enforced or Administered by the Commission*, FED. TRADE COMM'N, http://www.ftc.gov/enforcement/statutes (last visited Feb. 24, 2014).

[119] *See* 15 U.S.C. § 45(a)(2); *see also About the FTC*, FED. TRADE COMM'N, http://www.ftc.gov/about-ftc (last visited Feb. 24, 2014).

[120] FTC Policy Statement on Deception, Appended to Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), *available at* http://www.ftc.gov/ftc-policy-statement-on-deception (last visited Mar. 12, 2014).

privacy invasive practices than a company with a privacy policy."[121] Indeed, the vast majority of complaints the FTC has brought under Section 5 have alleged deception.

With respect to "unfair practices," the FTC defines such a practice as one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition."[122] Unlike deception, an unfair practice does not require breach of an overt promise or act. Substantial harm typically involves monetary, health, or safety injuries and excludes speculative, subjective or emotional harms like those often claimed in privacy cases.[123]

Not surprisingly, the FTC invokes unfairness less frequently than it invokes deception. This is because unfair practices are often harder to demonstrate and prove as compared to deceptive practices. For example, in the case of *FTC v. Wyndham*,[124] the FTC alleged that Wyndham "failed to employ reasonable and appropriate measures to protect personal information against unauthorized access," and that such failure is inherently unfair. Wyndham contested the FTC's assessment, arguing that the FTC did not establish clear standards for data security by which to abide.[125] However, as Professors Daniel J. Solove and Woodrow Hartzog have observed, the FTC's collective "data security jurisprudence forms a rather detailed list of inadequate security practices."[126] They contend that the FTC can show unreasonableness by relying upon departures from industry standards regarding data security—standard practices which the FTC itself has encouraged over the years through targeted enforcement activities.[127]

---

[121] *See Federal Trade Commission: Overview of Statutory Authority to Remedy Privacy Infringements*, ELEC. PRIVACY INFO. CTR., http://epic.org//privacy/internet/ftc/Authority.html (last visited Feb. 24, 2014).

[122] 15 U.S.C. § 45(n).

[123] FTC Policy Statement on Unfairness Appended to Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984).

[124] *See* FTC v. Wyndham, Complaint, FTC File. No. 1023142 (June 26, 2012), http://www.ftc.gov/sites/default/files/documents/cases/2012/06/120626wyndamhotelscmpt.pdf. Wyndham has thusfar unsuccessfully challenged the FTC decision in court. *See* FTC v. Wyndham, D. N.J. Case 2:13-cv-01887-ES-JAD (Opinion, Apr. 7, 2014).

[125] See FTC v. Wyndham, D. N.J. Case 2:13-cv-01887-ES-JAD (Opinion, Apr. 7, 2014) (denying Wyndham's motion to dismiss).

[126] *See* Solove & Hartzog, *supra* note 45.

Indeed, as Professors Breaux and Baumer have shown, the FTC cases over a recent ten-year period establish a set of "reasonable" security standards.[128]

Beyond the authority to pursue unfair and deceptive practices, Congress has granted the FTC enforcement authority for particular practices mandated by two other statutes. Specifically, the Children's Online Privacy Protection Act ("COPPA") restricts the online collection of personal information directly from children under the age of 13 without parental consent.[129] And, the Gramm-Leach-Bliley Act ("GLBA") requires financial institutions to develop privacy policies and notify consumers of them at least annually, as well as provide consumers opportunities to "opt out" from disclosures of personal financial information to unaffiliated third parties.[130] These statutes provide a narrower and less frequently asserted, purview for FTC enforcement of online privacy than does Section 5's "unfair and deceptive practice" jurisdiction.

In short, aside from "unfair and deceptive practices" and the narrowly defined COPPA and GLBA practices, the FTC does not have legal jurisdiction to protect consumers from other online privacy harms. Due to these jurisdictional limitations, the FTC must frame any enforcement actions to fit within the existing authority. As a result, when the FTC seeks to redress a new form of online privacy harm, it must be framed in the complaint as either an "unfair" or a "deceptive" practice or be within the narrow protections of COPPA and GLBA.[131]

IV. TYPOLOGY OF HARMS

Once we identified the relevant complaints brought by the FTC and private litigants, we looked beyond the formal formulation of the claim or cause of action to determine a typology of the *underlying* harms being asserted in each litigation event. This approach looked to

---

[127] *See* Solove & Hartzog, *supra* note 45, at 52–53.

[128] *See* Travis D. Breaux & David Baumer, *Legally "Reasonable" Security Requirements: A 10-Year FTC Retrospective*, 30 COMPUTERS & SECURITY 178 (2011).

[129] *See* Pub. L. 105–277, 112 Stat. 2681 (1998) (codified at 15 U.S.C. §§ 6501–6506); 16 C.F.R. § 312.

[130] *See* Pub. L. 106–102, 113 Stat. 1338 (1999) (codified as amended in relevant part at 15 U.S.C. §§ 6801-6809 and §§ 6821–6827).

[131] *See* Solove & Hartzog, *supra* note 45.

the true substance of the wrongful event rather than the way a claim was formulated to fit within the existing constraints of the legal landscape. We organized the vast amount of complaint data by themes that were apparent from the claims and their situational contexts. In effect, this is a categorization of the harms as articulated by the claims. The harms that were most frequently asserted were (1) unauthorized disclosure of personal information, (2) surreptitious collection of personal information, (3) failure to secure personal information, and (4) unlawful retention of personal information.

These categories are similar to those identified by Professors Solove and Hartzog.[132] Solove and Hartzog focused exclusively on the FTC's Section 5 actions and categorize privacy actions that alleged "deception" or "unfairness." Their categories for claims based on deception were: 1) broken promises of privacy; 2) general deception; 3) insufficient notice, and 4) data security. For unfairness based claims, their categories were: 1) retroactive changes; 2) deceitful data collection; 3) improper use of data; 4) unfair design or unfair default settings; and 5) unfair data security practices.[133]

In contrast to Solove and Hartzog's work, this study examines a combination of FTC actions and private lawsuits to identify a more complete typology that includes data from all existing federal avenues for bringing online privacy claims. Our unauthorized disclosure harms are somewhat more inclusive and correspond to several of Solove and Hartzog's categories, namely their classification of improper use and design/default setting claims under the FTC's unfair practice prong and broken promises and general deception under the FTC's deceptive practice prong. The surreptitious collection harms match Solove and Hartzog's deceitful collection (unfairness) and general deception along with insufficient notice (deception). And, the security harms are the same as Solove and Hartzog's, though Solove and Hartzog do not address retention as a separate issue. Our distinct and broader categories of harm derive from the examination of a combination of both class action litigation and the FTC settlements.

This section discusses the typology of the four sets of identified harms and presents examples of some of the alleged wrongful actions underlying them.

---

[132] *See* Solove & Hartzog, *supra* note 45.

[133] *See* Solove & Hartzog, *supra* note 45.

A. *Unauthorized Disclosure of Personal Information*

The privacy enforcement actions reflect a profound desire to remedy unauthorized disclosures of personal information. The cases emphasize that disclosures of personal information collected from website users and given to third parties without the clear permission of users is perceived as a wrongful act. These types of disclosures arise in various circumstances, ranging from ordinary commercial transactions to cases involving social media.[134] For example, several private actions were filed against AMR Corporation, an airline, for disclosing customer information in violation of a stated privacy policy.[135] Social networking services, like Zynga,[136] Facebook,[137] Pandora,[138] Myspace,[139] and LinkedIn,[140] are also popular defendants accused of transmitting or selling user information to third parties without user consent. In the private actions against Facebook, litigants complained of Facebook's use of users' names and photographs for advertising purposes without permission.[141] The FTC also accused Facebook of misleading consumers into believing they could restrict access to their information.[142] It further alleged that Facebook had retroactively applied material changes to the sites

---

[134] *See, e.g.*, *In re* Microsoft Corp., Complaint, File No. 0123240 (Aug. 8, 2002).

[135] Complaint, Baldwin v. AMR Corp., No. 04-00750 (N.D. Tex. Aug. 6, 2004); Complaint, Kimmell v. AMR Corp., No. 04-00750 (N.D. Tex. Aug. 6, 2004); Complaint, Rosenberg v. AMR Corp., No. 04-02564 (E.D.N.Y. July 9, 2004).

[136] *In re* Zynga Privacy Litig., No. 10-04680 (N.D. Cal. Jan. 10, 2011); *see also* Albini v. Zynga, Case No. 10-4723 (N.D. Cal. Oct. 19, 2010); Graf v. Zynga Game Network, Inc., Case No. 10-04680-JW (N.D. Cal. Oct. 18, 2010); Gudac v. Zynga Games, Case No. 10-04793 (N.D. Cal. Oct. 22, 2010); Schreiber v. Zynga Game Network, Case No. 10-4794 (N.D. Cal. Oct. 22, 2010).

[137] *In re* Facebook Consumer Privacy Litig., No. 10-00429 (N.D. Cal. June 8, 2010).

[138] Deacon v. Pandora Media, Inc., Case No. 11-cv-04674-LB (N.D. Cal. Sept. 20, 2011); Yunker v. Pandora Media, Inc., Case No. 11-cv-3113 (N.D. Cal. May 30, 2013).

[139] Leong v. Myspace, Case No. 10-8366 (C.D. Cal. Nov. 3, 2010); Virtue v. Myspace, Inc., Case No. 11-01800 (E.D.N.Y. Apr. 13, 2011).

[140] *In re* LinkedIn User Privacy Litig., No. 12-03088 (N.D. Cal. Apr. 30, 2013).

[141] E.K.D. v. Facebook, Inc., Case No. 12-cv-01216-LHK (S.D. Ill. June 1, 2011); Cohen v. Facebook, Inc., Case No. 10-cv-05282-RS (N.D. Cal. July 18, 2011); Fraley v. Facebook, Inc., Case No. 11-cv-01726 (N.D. Cal. Mar. 11, 2011).

[142] *In re* Facebook, Inc., Complaint, File No. 092 3184 (Dec. 5, 2011).

privacy settings, without informed consent, resulting in disclosure of information that had previously been restricted.[143]

Several private suits were also brought against Netflix for sharing users' video viewing history without properly removing associated personally identifiable information.[144] In one FTC action, a toy retailer represented that personal information would only be used to "personalize your online experience," but later sought bankruptcy approval to transfer information to third parties.[145] In another, a pharmaceutical company disclosed customer information in an email's "To:" line.[146] Finally, the FTC pursued an educational products company that decided to allow the rental of personal data to third parties without seeking consumer consent, even though it had explicitly promised to inform users of material changes to its privacy policy.[147]

B. *Surreptitious Collection of Personal Information*

Another important harm perceived by users is the surreptitious collection of personal information by websites. Surreptitious collection arises when a defendant collects information about a user without adequate disclosure. In some cases, companies disclosed some but not all of the types of information collected. In others, they disclosed some but not all means of collection or sources targeted for collection,[148] as in cases involving undisclosed history sniffing.[149] In still others, data collection was effectuated through the use of spyware,[150] phishing,[151] or pre-texting.[152] In a series of actions, the FTC

---

[143] *Id.*

[144] Comstock v. Netflix, Inc., No. 11-01219 (N.D. Cal. Mar. 11, 2011); Rura v. Netflix, Inc., No. 11-01075 (N.D. Cal. Mar. 8, 2011); Bernal v. Netflix, No. 11-00820 (N.D. Cal. Feb. 22, 2011); Milans v. Netflix, No. 11-03079 (N.D. Cal. Jan. 26, 2011); Doe v. Netflix, No. 09-05903 (N.D. Cal. Dec. 17, 2009).

[145] FTC v. Toysmart.com, LLC, Complaint, File No. X000075, Case No. 00-11341-RGS, ¶¶ 9–11 (D. Mass July 10, 2000).

[146] *In re* Eli Lilly and Company, Complaint, File No. 012 3214 (Jan. 18, 2002).

[147] *In re* Gateway Learning Corp., Complaint, File No. 0423047 (July 7, 2004).

[148] *In re* Path, Inc., Complaint, File No. 122 3158 (Feb. 1, 2013).

[149] *See, e.g.*, *In re* Epic Marketplace, Inc., Complaint, File No. 112 3182 (Dec. 5, 2012).

[150] *See, e.g.*, Complaint, Mortensen v. Bresnan Commc'n, No. 10-cv-00013 (D. Mont. Feb. 16, 2010); Complaint, Deering v. CenturyTel Inc., No. 10-cv-00012 (D. Mont. Feb. 11, 2010); Complaint, Green v. Cable One, Inc., No. 10-cv-00259 (N.D. Ala. Feb. 3, 2010);

pursued a number of rent-to-own computer companies, who, unbeknownst to users, had used key loggers, deployed fake software registration input forms, taken screenshots, and remotely operated users' webcams to collect information.[153] In other cases, data was collected after circumventing users' privacy settings[154] or by implementing unauthorized surveillance measures such as cookies.[155] There were cases where companies continued collecting data after users opted out of collection or had deactivated or deleted their accounts.[156] There were also instances involving unfair or deceptive instructions, interfaces, or default settings that made it particularly onerous for consumers to protect their data.[157] Another common event giving rise to surreptitious collection claims were websites that would install cookies that would continue to collect information about the users' activity, even after they signed out of the website.[158]

Complaint, Kirch v. Embarq Mgmt. Co., No. 10-cv-02047 (D. Kan. Jan. 26, 2010); Complaint, Valentine v. Wideopen West Finance, No. 09-cv-07653 (N.D. Ill. Nov. 10, 2008); Amended Complaint, Simios v. 180Solutions, Inc., No. 05-cv-05235 (N.D. Ill. Apr. 14, 2006); Complaint, Michaeli v. Exact Advertising, No. 05-cv-8331 (S.D.N.Y. Sept. 27, 2005).

[151] *See, e.g.*, FTC v. Hill, Complaint, File No. 0323102 (Mar. 22, 2004).

[152] *See, e.g.*, FTC v. Information Search, Inc., Complaint, File No. 0623102, Case No. 106-CV-01099-AMD, (D. Md. Apr. 18 2001).

[153] *See, e.g.*, *In re* Aspen Way Enterprises, Inc., Complaint, File No. 1123151 (Sept. 25, 2012).

[154] *See, e.g.*, *In re* Google Inc. Cookie Placement Consumer Privacy Litig., Case No. 12-md-02358 (D. Del. Dec. 19, 2012); U. S. v. Google, Inc., Complaint, Case No. 512-cv-04177-HRL (N.D. Cal. Aug. 8, 2012).

[155] *See, e.g.*, Couch v. Space Pencil, Case No. 11-cv-05606-LB (C.D. Cal. Sept. 14, 2011); Garvey v. Kissmetrics, Case No. CV 11-3764 (N.D. Cal. July 29, 2011); Del Vecchio v. Amazon.com, Case No. 2:11-cv-00366-RSL (W.D. Wash. Mar. 2, 2011); Bose v. Interclick, Inc., Case No. 10-cv-9183 (S.D.N.Y. Dec. 8, 2010); White v. Clearspring Tech., Case No. 10-cv-5948 (C.D. Cal. Oct. 18, 2010); Davis v. Videoegg, Inc., Case No. CV 10-7112 (CBM) (C.D. Cal. Sept. 23, 2010); La Court v. Specific Media, Inc., Case No. 10-cv-01256 (C.D. Cal. Aug. 18, 2010); Valdez v. Quantcast, Case No. 10-cv-05484 (C.D. Cal. June 23, 2010).

[156] *See, e.g.*, Missaghi v. Blockbuster, Inc., Case No. 11-cv-02559 (D. Minn.); Hodsdon v. Bright House Networks LLC, Case No. 2-cv-01580-AWI-JLT (D. Cal.); Hodsdon v. DirecTV, Case No. 12-cv-02827 (N.D. Cal.).

[157] *See, e.g.*, FTC v. Frostwire LLC, Complaint, File No. 112 3041, Case No. 111-cv-23643 (S.D. Fl. Oct. 7, 2011); *In re* HTC America, Inc., Complaint, File No. 122 3049 (Feb. 22, 2013).

[158] *See, e.g.*, *In re* Facebook Consumer Privacy Litig., No. 10-00429 (N.D. Cal. June 8, 2010).

C. Inadequate Security for Personal Information

Users see data security failures as a significant harm. In cases brought against parties for failure to secure personal information, the wrongful conduct was essentially that the responsible party did not implement adequate controls to secure consumers' personal information.[159] The FTC is very active in the area of data security, and the question of "adequacy" manifests across a wide array of procedures, from network security, authorization to access information and credentials, employee oversight and training, information disposal, breach detection and prevention, and breach response.[160]

Although there have been fewer "events" in which companies have been privately sued for failure to secure customer information compared to the other types of harms, the data security litigation tends to spawn a large number of individual cases. Thus, although there were only seventeen events identified as security issues, there were over ninety-six related private cases filed.[161]

D. *Wrongful Retention of Personal Information*

Lastly, the complaints reflect that wrongful retention of personal information is seen as a noteworthy harm. Users brought wrongful retention claims against companies that failed to destroy personal information after the users terminated their relationships with the

---

[159] *See, e.g.*, Complaint, Szpyrka v. LinkedIn, No. 12-cv-03099 (N.D. Cal. June 16, 2012) (alleging violations of California's Unfair Competition Law, the California Consumer Legal Remedies Act, breach of contract, breach of implied contract, breach of implied covenant of good faith and fair dealing, and negligence); Complaint, Peterson v. Sony Computer Entm't. Am. LLC, No. 11-cv-2242-RS (N.D. Cal. May 6, 2011) (alleging violations of the Electronic Communications Privacy Act, Computer Fraud and Abuse Act, California Customer Records Act, California Competition Law, False Advertising Law, California Consumer Legal Remedies Act, California Computer Criminal Law § 502, breach of implied warranty, breach of express contract, and negligence). One careful, empirical analysis maps the security requirements that emerge from FTC enforcement actions. *See* Breaux & Baumer, *supra* note 128 (FTC enforcement actions institutionalize security requirements for firms).

[160] *See, e.g., In re* Genica Corporation, Complaint, File No. 0823113 (Feb. 5, 2009); FTC v. Wyndham, Complaint, FTC File. No. 1023142 (June 26, 2012); *In re* TRENDnet, Inc., Complaint, File No. 122 3090 (Sept. 4, 2013); *In re* CVS Caremark Corporation, Complaint, File No. 0723119 (June 23, 2009).

[161] *See* Privacy Enforcement Actions, *supra* note 58, at 28.

company.[162] Thus, regardless of whether an economic loss occurs, such retention of personal information is perceived to harm the public. Many privacy policies are silent as to a users' ability to remove personal information from a website and as to what a company will do with the users' information if the user terminates the relationship.

There were six FTC complaints alleging improper retention.[163] Half of them involved privacy policies or similar promises.[164] The FTC brought all six complaints under Section 5. Two complaints relied on the deception theory,[165] two on unfairness,[166] and two were somewhat ambiguous.[167]

V. MAPPING A ZONE OF EFFECTIVENESS FOR NOTICE AND CHOICE

The typology of harms shown through the class action litigation and FTC actions provides a useful metric for evaluating the scope of effectiveness of the notice and choice regime. In particular, the typology enables us to articulate the zones or areas in which notice and choice can and cannot work. Some of the perceived harms are not susceptible to resolution *ex ante* by notice and choice. Others can be addressed by meaningful notice and choice. This section will discuss first those harms that the notice and choice framework effectively addresses, followed by a discussion of those harms which are simply incurable by a notice and choice regime. Notwithstanding the

---

[162] *See, e.g.*, Mendoza v. Microsoft, Inc., Case No. 13-cv-00378-DAE (W.D. Tex. May 1, 2013); Hodsdon v. Bright House Networks LLC, Case No. 12-01580 (E.D. Cal. Sept. 26, 2012); Burton v. Time Warner Cable Inc., Case No. 2:12-cv-06764 (C.D. Cal. Aug. 8, 2012); Hodsdon v. DirecTV, Case No. 12-cv-02827 (N.D. Cal. June 1, 2012); Priyev v. Google, No. 13-00093 (N.D. Ill. Feb. 29, 2012); Missaghi v. Blockbuster, Inc., Case No. 11-cv-02559 (D. Minn. Sept. 6, 2011); Comstock v. Netflix, Inc., No. 11-01219 (N.D. Cal. Mar. 11, 2011); Rura v. Netflix, Inc., No. 11-01075 (N.D. Cal. Mar. 8, 2011); Bernal v. Netflix, No. 11-00820 (N.D. Cal. Feb. 22, 2011); Milans v. Netflix, No. 11-03079 (N.D. Cal. Jan. 26, 2011); Doe v. Netflix, No. 09-05903 (N.D. Cal. Dec. 17, 2009).

[163] *See* Privacy Enforcement Actions, *supra* note 58, at 20.

[164] *In re* Life is good, Inc., File No. 0723046 (Jan. 17, 2008); *In re* CBR Systems, Inc., Complaint, File No. 1123120 (May 3, 2013); *In re* Ceridian Corp., Complaint, File No. 1023160 (June 15, 2011).

[165] *In re* Life is good, Inc., File No. 0723046 (Jan. 17, 2008); *In re* CBR Systems, Inc., Complaint, File No. 1123120 (May 3, 2013).

[166] *In re* BJ's Wholesale Club, Inc., Complaint, File No. 0423160 (June 16, 2005); *In re* DSW Inc., Complaint, File No. 0523096 (Dec. 1, 2005).

[167] *In re* Ceridian Corp., Complaint, File No. 1023160 (June 15, 2011); *In re* CardSystems Solutions, Inc., Complaint, File No. 0523148 (Feb. 23, 2006).

contents of a particular privacy policy, the latter are plainly outside notice and choice's "zone of effectiveness."

A. *Areas where Notice and Choice Satisfy User Autonomy*

The basic premise of notice and choice is that individuals have autonomy and control over their own information. The privacy harms show that individuals view control as choosing what personal information to divulge, when to release it, with whom it will be shared, and how the recipient will use it. Exercising such control effectively, however, requires as a prerequisite proper notice describing the recipient and the parameters of such recipient's use and retention of the information. When a notice fails, the issue is not whether a user would ever choose to disclose information, but the extent to which the user's choice as to whom and for what purposes has been undermined.

An accurate, complete and readable notice accompanied by meaningful choice can resolve many of the harms categorized as unauthorized disclosure, surreptitious collection, and, to a more limited extent, improper retention. The notice must disclose practices that are both followed and not inherently "unfair" (as discussed in Part III.B.) Notice and choice only averts these privacy violations sounding in deception, so long as society does not still deem the disclosed practice to be inherently "unfair."

1. *Unauthorized Disclosure: Sufficiency of Notice as a Cure*

Notices that are complete, understandable for users, accurate, and specific can avoid the harm of unauthorized disclosure. A notice that accurately and specifically describes all practices applied to the personal data in a way that users will understand establishes the basis for user consent. Broad or vague statements as well as incomprehensible statements about collection practices may be functionally equivalent to the absence of notice. For example, vague statements, like "we share your information only with affiliates" would not meaningfully communicate the identity of recipients of personal information and their uses of the information. Similarly in *Sears*, a notice stated that the company would track "online browsing," but did not adequately explain that tracking "online browsing" supposedly embraced a wide variety of collection techniques and data types.[168] Vague notices do not provide users with meaningful information

[168] *See* Complaint, *In re* Sears Holdings Mgmt. Corp., File No. 0823099 (June 4, 2009).

about practices to which they are asked to consent. Such vague and incomplete notices deny users the ability to control their personal information. Consent in such circumstances would be defective and users would perceive disclosures as unauthorized.

By contrast, notice that is complete, accurate, and specific regarding the terms that explain how, with whom, and for what purpose a user's information will be shared enables effective consent from the user.

2. *Surreptitious Collection: Detailed Notice of Methods of Collection and Type of Data Collected*

Like unauthorized disclosure harms, surreptitious collection can also be avoided *ex ante* through proper notice. If all methods of collection and all types of data collected are disclosed, then there is nothing surreptitious about a set of collection practices. Nevertheless, surreptitious collection can occur when flagrantly deceptive or unfair actions, like phishing or pretexting, are taken to induce disclosure of personal information.[169] Similarly, spyware may be deployed to collect information from unknowing users.[170] In these types of cases, both the methods of collection and the types of data collected are concealed from consumers. Similarly, in some cases, the data collected is simply beyond the scope of terms of the company's privacy policy.[171] The harm of surreptitious collection can be avoided *ex ante* by detailed notice of collection methods and data collected. However, insufficient detail in a notice regarding collection practices obliterates the possibility of meaningful consent. Once again, meaningful consent requires a notice that completely, accurately, and specifically describes each method of data collection and each type of data collected.

---

[169] *See, e.g.*, FTC v. Hill, Complaint, File No. 0323102 (Mar. 22 2004); Complaint, FTC v. Sun Spectrum Comm. Org., Inc., File No. 0323032, Case No. 03-8110 (S.D. Fla. Dec. 2, 2003).

[170] *See, e.g.*, *In re* Aspen Way Enterprises, Inc., Complaint, File No. 1123151 (Sept. 25, 2012).

[171] *See, e.g., In re* HTC America, Inc., Complaint, File No. 122 3049 (Feb. 22, 2013); *In re* Microsoft Corp., Complaint, File No. 0123240 (Aug. 8, 2002).

3. *Retention: Durational Specificity*

The harm of wrongful data retention may also be resolved, in part, by an adequate notice. Such a notice would provide durational specificity for the period of data retention. Notices can approach the issue of data retention by asserting a right to retain data indefinitely, by establishing a time limit on data retention, or by remaining silent. Both asserting a right to indefinite retention and remaining silent may still, however, create a perceived harm from wrongful retention. For example, there were six FTC complaints alleging improper retention and in two of these cases, the FTC pursued the companies for storing data indefinitely.[172] In three complaints, the FTC alleged that companies had kept information for which there was no longer a "business need."[173] In one complaint, the defendant, a card payment processor, had kept financial information for up to 30 days.[174] The FTC prosecuted these retention practices because the FTC believed that the practices created unnecessary risks to consumer information by increasing the likelihood of misuse or of exposure during a data breach.[175] A proper notice would alert consumers to these risks so that they could make informed decisions about the duration of their information's exposure. Nevertheless, outer boundaries can still exist that would contradict a website's privacy notice.

A. *Areas where Notice and Choice Cannot Satisfy User Autonomy*

While the notice and choice framework may be effective to protect against privacy harms in some areas, the framework will inherently be unable to protect against some of the articulated harms. Breaches of commitments made in notices will violate the terms of user consent and create unauthorized disclosures, the inadequacy of data security cannot be cured by notice, and mismatches for data retention preclude the capability for notice to avoid the privacy harms. This section will address these areas in which notice and choice is ineffective.

---

[172] *See* Complaint, *In re* Ceridian Corp., File No. 1023160 (June 15, 2011); Complaint, *In re* Life is good, Inc., File No. 0723046 (Jan. 17, 2008).

[173] *See* Complaint, *In re* CBR Systems, Inc., File No. 1123120 (May 3, 2013); Complaint, *In re* BJ's Wholesale Club, Inc., File No. 0423160 (June 16, 2005); Complaint, *In re* DSW Inc., File No. 0523096 (Dec. 1, 2005).

[174] *See* Complaint, *In re* CardSystems Solutions, Inc., File No. 0523148 (Feb. 23, 2006).

[175] *Id.*

1. *Unauthorized Disclosure: Breaches*

Notice and choice cannot resolve any failure of a website to adhere to the terms of the notice. As evidenced in the class action litigation and FTC enforcement cases, website privacy policies are seen as contracts.[176] Many cases thus arise amidst broken promises to refrain from certain types of disclosure, as in *National Research Center for College and University Admissions*,[177] *Eli Lilly*[178] and *Toysmart.com*.[179] Notice and choice cannot resolve the problem of broken privacy promises. In those cases, the individual providing personal information does so under the promised conditions and only under those conditions. Uses straying beyond the purposes disclosed in the notice are, by definition, unauthorized.

2. *Security: Technical Adequacy of Security Measures*

Notice and choice is also ineffective in addressing the data security harms. Notice itself does not keep personal information technically secure. Moreover, notwithstanding notice disclosures, the litigation indicates that there are certain baseline standards for security that cannot be waived or disclaimed.[180] In other words, notice and choice cannot negate negligent security practices. While a website may promise to keep users' personal information secure, it is difficult, if not impossible, to specify the methods with which the website will secure information. At most, the website can state that it will comply with industry standards or take "reasonable measures" to keep the information secure. These disclosures, however, will not prevent data breaches from occurring. The suits brought against companies for failure to secure personally identifiable information do not focus on

---

[176] *See supra* notes 97–102 and accompanying text.

[177] *See* Complaint, *In re* Nat'l Research Ctr. for Coll. & Univ. Admissions, Inc., File No. 0223005 (Oct. 2, 2002).

[178] *See* Complaint, *In re* Eli Lilly & Co., File No. 012 3214 (Jan. 18, 2002).

[179] *See* Complaint, FTC v. Toysmart.com, LLC, File No. X000075, Case No. 00-11341-RGS, ¶¶9–11 (D. Mass. July 10, 2000). Although the FTC may bring suit for practices that are unfair, in most cases, the FTC alleges both deception and unfairness in their complaints. For cases where the alleged conduct is based on unfairness, however, it may not be necessary to even have a privacy policy because the allegation refers to the practice, rather than the notice regarding the practice. This issue is discussed *infra* Part IV.

[180] *See* Breaux & Baumer, *supra* note 128 (showing 39 security requirements to address the legal security vulnerabilities).

whether there was notice about the security methods or that the company exceeded the scope of consent.[181] In essence, notice was irrelevant to the harm. The issue in these cases is that a third party was able to access information that was not, in fact, kept reasonably secure by the party entrusted with the information.[182] Thus, a notice and consent framework cannot be used to address problems with data security.

3. *Retention: Mismatch Between Stated Duration and Business Need*

Finally, notice and choice cannot be effective to address the harms associated with the wrongful retention of personally identifiable information. Wrongful retention arises through mismatches between company practices and external metrics for storage duration.

The litigation indicates that the public expects data retention periods to be limited to the period that is reasonably required by a company's business need. Notice may define the business need, but cannot unilaterally define what the public would see as a "reasonably required" period of retention for that business need. For example, in some of the lawsuits companies specified in their notices that they would retain customer information even after the user terminated the relationship or removed some personal information.[183] These notices did not exonerate the public expectation for shorter storage terms, and users perceived the practice as a clear harm. In essence, user consent may not authorize unreasonable storage durations.

Companies also have an incentive to keep flexibility in the duration of storage and draft broad privacy policies. To minimize litigation risk, these policies may be nonspecific or permissive on the issue of storage duration. The vagueness will not, however, protect against wrongful retention claims. On the opposite end, companies

---

[181] First Amended Complaint, *In re* LinkedIn User Privacy Litigation, No. 03088 (N.D. Cal. Nov. 26, 2011). At the time of suit, LinkedIn's Privacy policy stated that "[a]ll information that [users] provide [to LinkedIn] will be protected with industry standard protocols and technology." *Id.* at 2. The allegation in the suit was that LinkedIn was negligent and failed to follow industry standards—not that it did not provide sufficient notice or that there was an issue about user consent. *Id.*

[182] *See supra* Parts III.B.3 and IV.C.

[183] *See Amazon.com Privacy Notice*, AMAZON, http://www.amazon.com/ gp/ help/customer/ display.html?nodeId= 468496 (last updated Mar. 3, 2014) ("You can add or update certain information on pages such as those referenced in the 'Which Information Can I Access?' section. When you update information, we usually keep a copy of the prior version for our records.").

have various recordkeeping and reporting obligations and may need to retain different pieces of customer information for varying periods of time. Specific disclosure in this instance may be difficult and cause the privacy policy to become cumbersome, long, and even more difficult to understand.[184]

Because companies generally do not, and may not be able to, provide notice to consumers about how long their personal information will be retained, and objective duration standards exist which cannot be disclaimed, the notice and consent framework in these areas are likewise outside of the "zone of effectiveness."

VI. CONCLUSION

This empirical analysis has important policy ramifications. This is the first comprehensive articulation of privacy harms as perceived by litigants in federal cases. As such, the Article provides a typology of the most important privacy issues for consumers from the perspective of events that motivate consumers and regulators to sue. Significantly, this Article shows that harm is frequently not perceived by the public as an economic loss and provides empirical evidence for courts to recognize the four categories—unauthorized disclosure, surreptitious collection, inadequate security and wrongful retention—as litigable harms.

With respect to the efficacy of notice and choice, the empirical evidence shows that the framework can, in theory, work to prevent unauthorized disclosures and surreptitious collection, but that the framework fails to cover the harms of inadequate security and wrongful retention. Even where notice and choice might work, boundary lines can still exist and harm can occur despite the provision of notice because society may still deem a particular practice as unacceptable.[185]

Lastly, for the harms within the zone where notice and choice can work, the implementation of notice and choice will need to be more

---

[184] There is, of course, some middle ground. For example, the policy could state that personal information will be retained to the extent required by law. Such a statement, however, would still fail to put the user on notice of what information is being kept. There would be no way for a customer to ensure that the data collector will retain only legally required information and not any other.

[185] For example, Solove and Hartzog's analysis of FTC cases catalogs unfair practices. *See* Solove & Hartzog, *supra* note 45. Similarly, notice would not immunize an online credit grantor that gathers personal information banned from consideration in the granting of credit (i.e. marital status and race).

effective, as the critiques of the existing mechanisms are quite compelling.[186] Proposals such as Ryan Calo's alternative notice and choice delivery vehicles appear very promising.[187] Similarly, Jonathan Mayer and Arvind Narayanan's work on privacy substitutes will be helpful to determine where technologies can assist in development.[188]

---

[186] *See supra* Part II.A.2.

[187] *See* Calo, *supra* note 10.

[188] *See* Jonathan Mayer & Arvind Narayanan, *Privacy Substitutes*, 66 STAN. L. REV. ONLINE 89 (2013).