Redefining Consumer Harm

Rikki Wolff

Docket No. 180821780– 8780–01

SUMMARY

To create a risk management centered regime mitigating consumer harm, there must first be an expanded understanding of consumer harm. The understanding of privacy harm has been incorrectly limited to tangible injury. In the current approach, data breaches, inadvertent disclosures, and the selling of data to third parties may not constitute harm until the information has been used to one's detriment.[1] The narrow conception of privacy harm has led to the dismissal of many privacy plaintiffs' cases for failing to prove "actual damages".[2] In a digitized world the potential for harm is immense. Previous paper records of personal information were difficult to search and often destroyed after use, today digital data held by different entities can be pooled to create easily searchable profiles that can be retained indefinitely for little to no cost.[3] As this data is shared among parties it is stored in multiple locations to which multiple people have access, leaving it even more susceptible to hackers and exposure.[4] These large databases and the current understanding that there is no harm without concrete injury "disempowers" the consumer, "stripping them of control over their personal information" and creates a system that is "indifferent to their welfare".[5] The current understanding of privacy harm gives consumers little recourse or opportunities for redress when previously volunteered information is disclosed or compromised with courts often holding "there can be no privacy in

[1] Doe v. Chao, 540 U.S. 614, 620 (2004).
[2] Id.
[3] Richard Posner, *Privacy, Surveillance, and Law*, 75 U. Chi. L. Rev. 245, 248 (2008)
[4] Id. at 249.
[5] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan. L. Rev. 1393, 1423 (2001).

that which is already public".[6] This understanding of privacy and harm is antiquated and unnecessarily burdensome upon the consumer. Participation in today's society is nearly impossible without the voluntary disclosure of sensitive information across multiple platforms.[7] Consumers are left "powerless and vulnerable without any meaningful form of participation in the collection and use of their information".[8] This knowledge that personal data provided for the necessary functions of everyday affairs is now stored in multiple locations under vulnerable conditions, being exploited by third party marketers, or has already been compromised in a breach can cause consumers anxiety and disrupt behavior.[9] This in itself should be a recognized privacy harm. The current federal regime only exacerbates the lack of consumer autonomy through fragmented regulation and no default rule for consumer protections. A broad understanding of privacy harm would provide consumers with the ability to be heard in court for the risks most commonly faced in the current digital landscape and in turn encourage platforms to put more thought into their data practices.

HARM AS LOSS OF CONTROL OVER FLOW OF INFORMTAION

Spurred by the invention of the instantaneous camera and the rabid reporting of personal affairs in the newspapers Louis Brandeis and Samuel Warren wrote their now famous law review article positing one's "right to be let alone".[10] While their claim that invasions of privacy caused by "modern enterprise and invention" have subjected individuals to "mental pain and distress, far greater than could be inflicted by mere bodily injury"[11] remains true, the concern that "what is

[6] Gill v. Hearst Publ'g. Co., 253 P.2d 441 (Cal. 1953).
[7] Neil M. Richards; Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 Calif. L. Rev. 1887, 1921 (2010).
[8] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan. L. Rev. 1393, 1398 (2001).
[9] Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 Nw. J. Tech. & Intell. Prop. 321, 337 (2013).
[10] Samuel D. Warren, Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).
[11] Id. at 196.

whispered in the closet shall be proclaimed from the housetops" must be reexamined in the digital economy. The biggest challenge to consumer privacy is not that intimate data will be exposed but rather data freely shared with one shall be stored, manipulated, sold, or even compromised by another. Alan Westin offers an understanding of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[12] This is a more modern and consumer friendly understanding rather than the rigid understanding of privacy as secrecy that requires keeping information, typically discreditable information, hidden.[13] Privacy as secrecy is impractical for consumers because far more information is shared voluntarily.[14] For the consumer, privacy cannot be the "absence of information"[15] because it is nearly impossible to keep information hidden when disclosure has become necessary to the functioning of society. Privacy should not be measured by the steps taken to hide information from prying eyes but rather understood as "regulating the flow of information".[16]

With shopping, banking, and even healthcare services moving online consumers are required to surrender the information once stored away in hardcopy file cabinets to multiple website text boxes. While it is true consumers voluntarily provide information knowing it will be used and viewed by the platform, they do so in return for the performance of a service, this should not mean the consumer forfeits all control over their information going forward. The storing, compiling, and sharing of information by and between platforms following initial disclosure strips the consumer of all control over the spread of their information and erodes

[12] Alan F. Westin, Privacy and Freedom (1967).
[13] Daniel J. Solove, *Conceptualizing Privacy*, 90 Calif. L. Rev. 1087, 1106 (2002).
[14] Richard Posner, *Privacy, Surveillance, and Law*, 75 U. Chi. L. Rev. 245, 247 (2008).
[15] Charles Fried, *Privacy*, 77 Yale L.J. 475, 482 (1968).
[16] Ari Ezra Waldman, *Privacy as Trust*, 6 (2018).

privacy. This loss of control in itself should be recognized as privacy harm by the administration.

HARM IN DATA COLLECTION AND SHARING PRACTICE

The internet is new storage place for information and the ease with which that information can be stored and aggregated created a new billion-dollar industry centered around the collecting and sharing of information.[17] This industry is dependent upon the voluntary disclosure of consumer information. Consumers voluntarily disclose information in exchange for a service but in doing so relinquish control to that data indefinitely and for purposes unbeknownst to them. This new data sharing practice leaves the consumer a helpless bystander with no ability to reclaim control over their information or seek redress for the discomfort caused by their data making the rounds from platform to platform.

Companies collect data two ways, directly and covertly. Data is collected directly by retaining "registration and transactional data", the data a consumer must enter in exchange for service such as credit card number, address, and previous purchases. Companies collect data covertly by tracking browsing habits and recording how one engages with the website, including how the link was accessed and how much time was spent on a particular page.[18] Through this data companies create user profiles to better target advertisements. As life continues to require an increase in the amount of information shared, companies can compile permanent records of "unparalleled pervasiveness and depth" on individuals.[19] Companies then aggregate consumer profiles and this mass of data is sold to marketing firms and other third parties. The average

[17] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan. L. Rev. 1393,1410 (2001).
[18] Id.
[19] Id.

consumer's information is contained in at least fifty data bases.[20] This loss of individual control over data to the ether causes the consumer great pain as they are left wondering who has accessed their data, who can potentially access their data, and how that data can be used to their detriment.

Additionally, the practice of aggregation has made it nearly impossible for individual consumers to hold companies accountable for the distress caused by the sharing of personal data. Courts have held individual personal information has no "compensable value"[21]. In *Dwyer v. American Express*, cardholders brought suit against American Express for the privacy invasion experienced by the categorization and sale of their personal data. Not only did the court find there could be no invasion in compiling information voluntarily disclosed but also that individual information has "little to no intrinsic value".[22] Rather it is the company collecting the data that creates value by "categorizing and aggregating"[23]. The valuation of one's information needs to be redefined in order to create a regime that can truly combat privacy harm. The true value in one's information is not in its "intimacy" or the value assigned to it by the owner but "the ability it provides to others to gain power and control over an individual".[24] This power imbalance created by the ability of multiple platforms to expose consumers to uncertainty through irresponsible and overzealous collection is a privacy harm that affects consume peace of mind but also consumer practices.

As each keystroke is recorded, and every purchase is logged, one's inbox becomes inundated with mysterious online offers, it can feel as if the computer knows all and personhood

---

[20] Id. at 1408.
[21] In re Jetblue Airways Corp. Privacy Litigation, 379 F.Supp.2d 299 (2005).
[22] Dwyer v. American Express Co., 273 Ill App 3d 742 (Ill. App. Ct. 1995).
[23] Id.
[24] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan. L. Rev. 1393, 1452 (2001).

has been reduced to nothing more than their browsing habits and online orders. Roger Clarke has defined this new "systematic use of personal data systems in the investigation or monitoring of the actions" as "dataveillance".[25] Behavior is being studied and privacy infringed not through the hidden camera of some "Orwellian big brother" but rather by the steady collection of consumer data.[26] Daniel Solove writes the often used "big brother" metaphor for the increased tracking and storing of data by companies is wrong.[27] Information is not being gathered by other humans but by company computers which process and aggregate data for sale. These companies exist not as one ever watching big brother but as "a myriad of little brothers" whose processes and "thoughtless decision making" have left consumers vulnerable. This vulnerability must be understood as a privacy harm to help consumers regain some ownership over the flow of their data and ownership in the way they interact with web platforms.

CONSUMER ATTITUDES

The Administration's desire to preserve innovation continues to ignore and mischaracterize the harm experienced by the users of these innovations. Unchecked innovation and the self-regulation of the industry has left consumers out of the privacy equation with no means of pushing back against newer and more invasive practices. Innovation increasing efficiency also requires an increase in the amount of information disclosed by the consumer. Consumers continued use of online services and data sharing platforms is currently viewed as a lack of care or concern for privacy but that is incorrect. Instead consumers have reluctantly accepted the lack of privacy that has been forced upon them. Richard Posner wrote "the fact that

[25] Id. at 1417.
[26] Id.
[27] Id. at 1396.

one cannot negotiate modernity without continuously revealing personal information to a variety of demanders has habituated most Americans to radically diminished informational privacy". [28]

Consumers have not stopped caring about their privacy but have simply acquiesced to this new regime because they have no means to challenge it. According to a 2014 Pew Research Center survey, 91% of Americans agreed that "consumers have lost control over how personal information is collected and used by companies".[29] Another survey conducted by Harris Interactive found 98% of consumers expressed a "strong desire for better controls over how their personal information is collected and used".[30] A 2018 survey conducted by Blue Fountain Media found only 4% of web users have faith in how google handles user information and only 18% of users said they are "very confident" trusting retailers with personal information.[31]

This mistrust is not healthy for the consumer and it is not good for business. Consumers feel they are being used just for their purchasing power and the value of their shared data. A regime that recognizes the harm caused to the consumer by loss of autonomy would lead to even greater use and consumer engagement.[32] It is time the consumer is treated as a valued part of the digital economy and the government appreciate what the consumer is required to give up both in their actual information and in their peace of mind.

CURRENT LEGAL PATCHWORK'S FAILURE TO ADDRESS HARM

The present lack of trust and lack of personal control experienced by consumers has been

---

[28] Richard Posner, *Privacy, Surveillance, and Law*, 75 U. Chi. L. Rev. 245, 249 (2008).
[29] Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, (Nov. 12, 2014) http://www.pewinternet.org/2014/11/12/public-privacy-perceptions
[30] Janet Jaiswal, *Survey Results Are In: Consumers Say Privacy is a Bigger Concern Than Security on Smartphones*, TrustArc (April 27, 2011) https://www.trustarc.com/blog/2011/04/27/survey-results-are-in-consumers-say-privacy-is-abigger-concern-than-security-on-smartphones/
[31] Brian Byer, *Internet Users Worry About Online Privacy but Feel Powerless to Do Much About It*, (June 20, 2018) https://www.entrepreneur.com/article/314524
[32] Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 Nw. J. Tech. & Intell. Prop. 321, 340 (2013).

exacerbated by the fragmented federal regime regulation. Even if not all consumers are concerned about the sharing of their data or may not experience the same anxiety, this does not mean those who do experience pain should be left without protection and without remedy. Companies should not be allowed to cause consumers pain as a default rule. In arguing for a strong default rule against consumer uneasiness, Clark D. Asay uses the example of armed robbery laws. Few believe laws against armed robbery are bad just because a minority of the population is ever affected. "Simply because only some will experience some harm absent regulation is not good reason to rule out the regulation."[33] Just because not everyone will be disturbed or violated by the compiling and proliferation of one's data that does mean the practice should continue unchecked.

Many Americans believe they are entitled to assert certain privacy rights but there is a large "disconnect" between the rights Americans believe they have and the rights that exist under present laws.[34] While constitution entitles ones to "zones of privacy" that zone exists in relation to the nature of the information, looking to how intimate or stigmatizing it may be".[35] However, the Supreme Court has held there is no general right to informational privacy.[36] In addition to no recognized right, courts have also failed to recognize the harm created by information being out of one's control.[37] In *Doe v. SEPTA*, an employee disclosed his HIV status to receive prescriptions through his employee insurance, this was then inadvertently shared with SEPTA officials and he experienced different treatment from other employees. While there was no discrimination, Doe noted his workspace "seemed more lonely than before".[38] The court found the disclosure to his doctor in exchange for the filling of a prescription to be a "minimal

[33] Id.
[34] Michael C. James, *A Comparative Analysis of the Right to Privacy...*, 29 Conn. J. Int'l L. 257, 269 (2014)
[35] Griswold v. Connecticut, 381 U.S. 479 (1965).
[36] Whalen v. Roe, 429 U.S. 589 (1977).
[37] Doe v. Southeastern Pennsylvania Transportation Authority, 72 F.3d 1133, 1143 (3d Cir. 1995).
[38] Id.

intrusion" ignoring the pain caused by Doe's inability to decide for himself if and when to tell his co-workers he was HIV positive.

In addition to the hesitation to expand the constitutional understanding of privacy, these protections apply only to state action. Consumers wishing to protect their privacy against private companies are left to fit claims into a very narrow federal framework. This rigid regulation in distinct areas ignore the vulnerability experienced by the everyday consumer with some activity and data platforms falling through regulatory cracks completely.[39] Currently companies are required to do the bare minimum in informing the consumer of their data use practices. The FTC requires commercial websites disclose a statement of what, when, and how user data is collected.[40] These policies are often difficult to find and even more difficult to read, they are long, and full of vague practice descriptions and legalese. If the average were to read the privacy policy for every site they visited it would take 244 hours per year.[41] Even Chief Justice John Roberts has said he does not read every consumer agreement he is confronted with.[42] The consumer has no real knowledge of what data is being collected and how. Additionally, consumers cannot be said to have adequate choice as for many of these online services there is simply no alternative.

Once again, the consumer is left powerless in the disclosure and spread of their information. Notice-and-choice leaves the consumer without a legal leg to stand on once they feel the violation and mental uneasiness of their data being exposed. Courts have dismissed cases stating "general statements of policy" are not contracts and breach of such privacy policy

---

[39] Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, Teach Privacy, Nov. 13, 2015, https://teachprivacy.com/problems-sectoral-approach-privacy-law/
[40] Ari Ezra Waldman, *Privacy as Trust*, 80 (2018).
[41] Lorrie Faith Cranor, *Necessary but not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. Telecomm. & High Tech. L. 273, 274 (2012).
[42] Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 Nw. J. Tech. & Intell. Prop. 321 (2013).

cannot entitle consumers to damages.[43] Providing a privacy policy should not be carte blanche for companies to collect and appropriate user data. The simple providing of a private policy does little to inform a consumer or prevent vulnerability, if anything it makes consumer data more vulnerable to the language tricks and loopholes devised by the large companies.

There is no default federal law protecting individual privacy instead sectoral regulations cover varying industries and service providers. If a company does not fall within the specific industry or if the type of information collected does not fit within the law, then the law does not apply to the entity or the data.[44] Section § 2702(a)(1) of ECPA regulates "the voluntary disclosure of customer communications or records" and provides an example of the systems shortcomings. It states: "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service". A law regulating the spread of previous voluntarily disclosed information is exactly what the Administration needs in order to address the powerlessness experienced by consumers when their data is repurposed. However, this particular law falls short in application. Courts have limited this law to those "selling Internet access itself".[45] In *Crowley v. CyberSource Corp,* the court held Amazon.com and all other online retailers are not electronic service providers despite all communication with costumers occurring electronically.

Federal law leaves consumers without recourse to reclaim ownership of their data or remedy for mental distress by allowing all other "privacy law" enforcement against companies

[43] In re Jetblue Airways Corp. Privacy Litigation, 379 F.Supp.2d 299 (2005).
[44] Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 Nw. J. Tech. & Intell. Prop. 321, 326 (2013).
[45] In re Jetblue Airways Corp. Privacy Litigation, 379 F.Supp.2d 299 (E.D. N.Y.2005).

falling outside of the existing regulatory statutes in the hands of the FTC.[46] The federal regime fails to recognize the pain of the consumer by once again stripping them of control. The inability of consumers to bring an individual suit misses the mark on evaluating the harm experienced. It is not only the deceptive practices that are harmful and need to be rectified but it is the loss of autonomy created by the practice.

CONCLUSION

For the Administration to achieve its goals the vulnerability and anxiety created by online services storing and selling consumer data must be recognized as a privacy harm to the consumer. Privacy must be understood as the ability to regulate the flow of one's own information. Current company practices have left consumers disillusioned. Even worse, the current federal regime has given private companies the seemingly unchecked ability to aggregate and sell data and left consumers powerless without the ability to seek redress in the courts.

[46] Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures,* 11 Nw. J. Tech. & Intell. Prop. 321, 327 (2013).