Harvard Journal of Law & Technology
Volume 28, Number 1 Fall 2014

THREE'S A CROWD: TOWARDS CONTEXTUAL INTEGRITY IN THIRD-PARTY DATA SHARING

*Natalie Kim**

TABLE OF CONTENTS

I. INTRODUCTION 325

II. A VERY RECENT HISTORY OF THIRD-PARTY DATA SHARING 328

III. THE REGULATORY LINEUP 334
A. Privacy Litigation 334
B. Self-Regulation 335
C. The Federal Trade Commission and Its "Common Law" 338

III. POLICY RECOMMENDATIONS FOR DOWNSTREAM DATA USE REGULATIONS 340
A. Greater Control and Accessibility 341
B. Greater Accountability down the Data Chain 343
C. Privacy By Design 344

IV. CONCLUSION 346

I. INTRODUCTION

"We may also share your information with third parties with whom we have a relationship."[1] Innocuously tucked away in privacy policies, third-party data sharing is a rapidly growing source of online revenue for data controllers[2] in today's data-driven economy.[3] Consumers short on time and attention are increasingly demanding,

---

* Harvard Law School, J.D. 2015. I thank Professor Urs Gasser and the JOLT Editorial Board for their advice and guidance throughout the Note's development.

1. Such language is common amongst retailers and social networking services alike. *See, e.g.*, *Data Use Policy: Information We Receive and How It Is Used*, FACEBOOK, https://www.facebook.com/about/privacy/your-info (last visited Dec. 18, 2014); *Macy's and Macys.com Notice of Privacy Practices*, MACY'S, https://customerservice.macys.com/app/answers/detail/a_id/595 (last updated Jan. 31, 2014).

2. The term "data controllers" refers broadly to entities that collect data directly from users, or "data subjects." For the purposes of this paper, "data controllers" is used interchangeably with "companies." "Data subjects" is used interchangeably with "users" or "consumers." "Third parties" are explicitly referred to as such.

3. *See Big Data Universe Beginning To Explode*, COMPUTER SCIS. CORP., http://www.csc.com/insights/flxwd/78931-big_data_universe_beginning_to_explode (last visited Dec. 18, 2014).

and getting, content curation and personalization.[4] Rather than charging users directly for these services, data controllers sell the data collected from their users to third parties,[5] who are typically data brokers,[6] app developers,[7] and successor businesses. Entire industries based on large, aggregated consumer data sets are rising, such as behavioral advertising[8] and big data research and analytics.[9]

As downstream sharing becomes more widespread, the likelihood of preserving "contextual integrity"[10] — meaning that the context of information sharing matches the individual's preferences — in the specific "node" in the data sharing chain erodes. Figure 1 provides a visual representation of the nodes. Each node refers to a stage of data sharing. The first node most typically involves the user directly volunteering the information to the data controller; this Note is primarily concerned with the second node, which typically involves the data controller sharing user data with downstream customers, such as advertisers. The second node is where contextual integrity begins to

---

4. *See* Dan Meyer, *2014 Predictions: In 2014 Expect More Personalization and 'The Internet of Me,'* RCRWIRELESS (Jan. 17, 2014), http://www.rcrwireless.com/article/20140117/wireless/2014-predictions-in-2014-expect-more-personalization-and-the-internet-of-me/.

5. This paper does not address direct data controller breaches or data breaches by hackers and other unauthorized entities. Third-party data sharing refers to intentional sharing by data controllers to other entities.

6. Data brokers sell aggregated lists of consumer information including criminal, residential, retail, and health-related data. Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA, https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you (last updated Jun. 13, 2014). A special category of information is called "Personally Identifiable Information," or simply "PII." "PII" refers to information that "can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual." The definition of PII "is not anchored to any single category of information or technology" but "requires a case-by-case assessment of the specific risk that an individual can be identified" from a particular combination of collected data. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB MEMORANDUM M-07-1616, SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION (2007).

7. While many mobile apps legitimately require certain PII to function, many apps collect unnecessary PII. As the proportion of data transferred on mobile devices grows, so does the need to establish privacy compliance standards for mobile app developers. *See Privacy in Mobile Apps for App Developers*, TERMSFEED (Jan. 11, 2014), http://termsfeed.com/blog/privacy-mobile-apps-developers/.

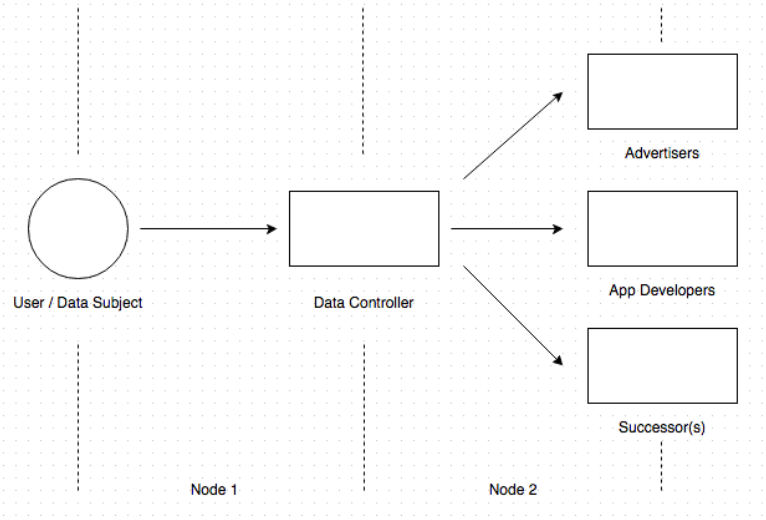
8. Behavioral advertising utilizes methods such as cookies to serve ads targeted to individual preferences. *See* David Auerbach, *You Are What You Click: On Microtargeting*, THE NATION (Feb. 13, 2013), http://www.thenation.com/article/172887/you-are-what-you-click-microtargeting.

9. *See generally* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013) (discusses the impact of big data analytics across fields such as medicine, government, business and research).

10. *See generally* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 101, 118–25 (2004) (introducing contextual integrity as a conceptual framework and the norms of appropriateness and distribution that influence it).

erode.[11] The typical user only has control over first-node sharing between user and data controller. First-node sharing achieves contextual integrity as the user's aim (e.g., to connect with friends) is matched by the data-sharing context (e.g., Facebook). In contrast, contextual integrity in the second node is unclear at best; data is shared without the user's direct involvement. Users are forced to make a bundled choice that disregards temporal and contextual nuances of information sharing. The rise of data as a commodity has undermined user ability to preserve contextual integrity online.

Figure 1: Third Party Data Sharing



With increasing complexity in the data-sharing model, there must be a corresponding increase in nuance for its data privacy counterpart. Possible nodes in third-party data sharing are numerous and growing, yet privacy policies essentially remain a blunt instrument, giving users a binary option between sharing with none or sharing with all (the "all" including currently unforeseeable downstream data collectors). This existing "notice-and-choice" regime deprives consumers of a chance to ensure meaningful contextual integrity for their online identities. This is a problematic intrusion into an individual's right of self-determination online.[12] Human society is a complex network of context-dependent norms of appropriateness and disclosure,[13] and a

11. Although not depicted in the diagram, there can be (and are) third, fourth, fifth nodes and so on.

12. *See* Nissenbaum, *supra* note 10, at 154.

13. *See id.* at 137. Nissenbaum identifies norms of appropriateness and distribution that govern all spheres of social life. These norms differ according to context. The ability to tailor information disclosure according to differing contexts is crucial for autonomy and the

forced uniformity of these contexts could cause unfortunate chilling effects. Uncontrolled data collection could result in crimes, such as identity theft and data breaches, and inequities, such as data-driven profiling of job candidates, tenants, and would-be criminals.

The Federal Trade Commission ("FTC") has filled the statutory vacuum to lead the development of regulations in the online privacy space. Despite criticisms that it is "low-tech, defensive, and toothless,"[14] it remains best suited to implement greater contextual integrity in the third-party data sharing space due to its standardized enforcement procedures, practice of giving notice to industry actors subject to privacy rules, and the compliance incentives it alone can provide. Part I of this Note charts the progress of third-party data sharing, while Part II analyzes the regulatory landscape and concludes that the FTC is best suited for regulating third-party data sharing. Part III enumerates suggestions for achieving better contextual integrity in third-party data sharing: (1) increasing user access and control; (2) encouraging accountability and fairness in liability distribution; and (3) ensuring that the user receives meaningful notice at a time most relevant for making informed and consensual privacy decisions.

II. A VERY RECENT HISTORY OF THIRD-PARTY DATA SHARING

The primary legal instrument conveying representations to consumers regarding third-party data sharing is the privacy policy. Now ubiquitous, the privacy policy was virtually nonexistent before 1998.[15] The rise of the privacy policy began as a self-regulatory effort on the part of industry actors to avoid further regulatory scrutiny.[16] The privacy policy's rapid growth mirrors the exponential growth of the Internet and the privacy issues that accompany it.

Early failures to enforce privacy policies as binding contracts indicate both the difficulty courts faced in grappling with the new problem of online privacy breaches as well as the enduring drawbacks of tort and contract law as avenues for privacy-related remedies. Privacy policies were thought to be general business statements rather than contracts, and, at any rate, it was not clear whether an online

---

shaping of one's identity. Contextual integrity is achieved when information flows match individual preferences.

14. Peter Maass, *Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless*, WIRED (Jun. 28, 2012), http://www.wired.com/2012/06/ftc-fail/all/.

15. While only two percent of websites had privacy policies in 1998, almost all popular commercial websites had one by 2001. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 594 (2014).

16. *Id.* at 593–94.

privacy breach was an actionable harm at all.[17] As a defensive self-regulatory measure, privacy policies from the beginning adopted a binary notice-and-choice, take-it-or-leave-it framework.[18]

Aggregated consumer data was shared with third parties from early on;[19] the FTC began regulatory efforts by targeting direct contradictions of representations made in privacy policies by organizations handling sensitive data about minors. *The National Research Center for College and University Admissions, Inc.* was the first FTC enforcement action regarding third-party data sharing.[20] The National Research Center for College and University Admissions ("NRCCUA"), an educational non-profit, had sent out surveys to high school students stating "[t]his data is [sic] used by colleges, universities and other organizations to assist students and their families by providing them with valuable information."[21] However, NRCCUA also shared this information with commercial marketers.[22] In the settlement order, the FTC barred NRCCUA from further misrepresentations, ordered "clear and conspicuous" disclosure of any future third-party sharing, barred NRCCUA from using the collected personally identifiable information ("PII"), and subjected it to a five-year audit.[23] Other early cases also involved children's PII being sold to third-party advertisers;[24] any proceeds from such third-party sales were ordered disgorged.[25]

NRCCUA was just the tip of the iceberg. The data broker industry had exploded in the 1990s after the advent of the Internet, which provided the opportunity to resell consumer data in bulk to interested

17. *See* Dwyer v. Am. Exp. Co., 652 N.E.2d 1351, 1356 (Ill. App. 1995) (holding that third-party data sharing did not violate data subjects' rights as the sharing was not shown to harm the users economically).

18. *See* Solove & Hartzog, *supra* note 15, at 603.

19. *See, e.g.*, *Google and Privacy*, GOOGLE (Jun. 9, 1999), http://www.google.com/policies/privacy/archive/19990609/ ("Google may share information about users with advertisers, business partners, sponsors, and other third parties.").

20. Complaint, The Nat'l Research Ctr. for Coll. and Univ. Admissions, Inc., et al., 135 F.T.C. 13 (2003), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2002/10/nrccuacmp1-1.htm.

21. *Id.*

22. *Id.*

23. The Nat'l Research Ctr. for Coll. and Univ. Admissions, Inc., et al., 135 F.T.C. 13 (2003), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2003/01/nrccuamuncedo.htm [hereinafter *NRCCUA*].

24. *See, e.g.*, Gateway Learning Corp., FTC File No. 042 3047, 2004 WL 2618647 (2004) (Decision and Order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2004/09/040917do0423047.pdf; Educ. Research Ctr. of Am., Inc., et al., 135 F.T.C. 578 (2003), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2003/05/ercado.pdf.

25. *See, e.g.*, Vision I Props., LLC, d/b/a Cartmanager Int'l, 139 F.T.C. 296 (2005), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2005/04/050426do0423068.pdf.

parties with unprecedented ease.[26] The mostly unregulated era came to an end with a seminal enforcement action against major data broker ChoicePoint, Inc.[27] ChoicePoint was found to have violated the Fair Credit Reporting Act ("FCRA") by furnishing over 163,000 consumer reports to non-validated requesters.[28] The final order stipulated fines of unprecedented magnitude, with $10 million in civil penalties and $5 million in consumer redress. The centerpiece of the settlement was twenty years of independent biannual audits.[29]

The ChoicePoint settlement served as a template for subsequent settlements and signaled an era of deeper FTC involvement in companies' internal privacy practices. For instance, this deeper FTC involvement can be seen in the settlement of *Chitika, Inc.* in 2011, which required a behavioral advertiser that failed to honor opt-out requests to allow opt-outs for at least five years and destroy all data collected from consumers who had elected to opt out.[30] More generally, it has become standard for FTC decision orders to mandate some combination of the following reforms: (1) designation of personnel to coordinate information security programs; (2) data privacy risk assessment through programs such as employee training and establishment of secure information and network systems; (3) design and implementation of reasonable safeguards as identified by the risk assessment; (4) development and use of reasonable steps to select and retain service providers to implement safeguards; and (5) evaluation and adjustment of the information security program according to testing.[31]

However, the ChoicePoint settlement's influence has been inconsistent in other aspects. The twenty-year biannual audit provision is a prominent feature in subsequent decision orders, even those of much smaller scale.[32] Monetary damages in subsequent cases

---

26. *See* Logan Danielle Wayne, *The Data-Broker Threat: Proposing Federal Legislation To Protect Post-Expungement Privacy*, 102 J. CRIM. L. & CRIMINOLOGY 253, 262–63 (2012).

27. *ChoicePoint Settles Data Security Breach Charges; To Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress*, FED. TRADE COMM'N (Jan. 26, 2006), http://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.

28. *Id.*

29. *Id.*

30. Chitika, Inc., 151 F.T.C. 494 (2011), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/06/110617chitikado.pdf.

31. *See, e.g.*, Premier Capital Lending, Inc., et al., FTC File 072 3004, 2008 WL 5266769 (2008) (Decision and Order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/12/081216pcldo.pdf.

32. In March 2009, the FTC settled with Rental Research Services, a data broker that had sold 318 consumer reports to identity thieves. While this is a small breach compared to ChoicePoint's 163,000, it too was subjected to a twenty-year audit provision. *See Consumer Reporting Agency Settles FTC Charges: Sold Tenant Screening Reports to Identity Thieves*, FED. TRADE COMM'N (Mar. 5, 2009), http://www.ftc.gov/news-events/press-releases/2009/03/consumer-reporting-agency-settles-ftc-charges-sold-tenant.

were more easily applied when the amount of unjust enrichment was specific. Rental Research Services was fined $500,000, although the fine was suspended due to their inability to pay.[33] In 2010, data broker U.S. Search was ordered to refund consumers after its "PrivacyLock" feature that charged consumers to protect their records from third-party purchases was proven to be fake.[34]

The increasing avenues for third-party data sharing by the late 2000s led the FTC to engage in industry- or technology-specific investigations under its authority in section 6(b) of the FTC Act.[35] The FTC began a large-scale peer-to-peer ("P2P") file-sharing investigation covering over one hundred entities in 2010.[36] After setting guidelines for businesses with a P2P component,[37] the FTC then sent warning letters or notices to companies suspected of having unsecure practices. Subsequent settlements with EPN, Inc.[38] in 2012 and LabMD, Inc.[39] in 2013 ordered these companies to take reasonable and appropriate actions to guard consumer PII from ending up in unauthorized P2P networks, or if the companies themselves utilize P2P networks to share information with third parties, to ensure security of those networks.

Another industry-wide inquiry on data brokers was signaled in the FTC's March 2012 Report "Protecting Consumer Privacy in an Era of Rapid Change," which proposed greater user accessibility for the data collected by data brokers and advocated new regulation tailored to the data broker industry.[40] An inquiry into data brokers' privacy practices

---

33. *Id*.

34. US Search, Inc. and US Search, LLC., 151 F.T.C. 184 (2011) (Decision and Order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/03/110325ussearchdo.pdf.

35. 15 U.S.C. § 46(b) (2012) (granting the Commission the power to require data collectors "to file with the Commission in such form as the Commission may prescribe annual or special, or both annual and special, reports or answers in writing to specific questions . . . .").

36. *Widespread Data Breaches Uncovered by FTC Probe*, FED. TRADE COMM'N (Feb. 22, 2010), http://www.ftc.gov/news-events/press-releases/2010/02/widespread-data-breaches-uncovered-ftc-probe.

37. *Peer-to-Peer File Sharing: A Guide for Business*, BUREAU OF CONSUMER PROTECTION BUS. CTR., FED. TRADE COMM'N, http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business (last visited Dec. 18, 2014).

38. *See generally FTC Charges Businesses Exposed Sensitive Information on Peer-to-Peer File-Sharing Networks, Putting Thousands of Consumers at Risk*, FED. TRADE COMM'N (Jun. 7, 2012), http://www.ftc.gov/news-events/press-releases/2012/06/ftc-charges-businesses-exposed-sensitive-information-peer-peer.

39. *See generally FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy*, FED. TRADE COMM'N (Aug. 29, 2013), http://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers.

40. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 14 (2012) [hereinafter FTC PRIVACY REPORT].

began in December 2012,[41] culminating in a presentation to the Senate Committee on Commerce, Science and Transportation in December 2013.[42] This effort led to some innovation in self-regulation, such as aboutthedata.com, which allows users to access and correct data that Acxiom, an online advertising data provider, has about them.[43] The FTC also pursued enforcement actions against data brokers such as Spokeo,[44] Filiquarian Publishing,[45] and Certegy Check Services (notable for its $3.5 million fine)[46] for FCRA violations.

Due to the predominance of social networking services as data sharing mechanisms, some of the largest third-party data sharing settlements have involved household names in the social networking sphere. In 2011, the FTC found wide-ranging third-party data sharing violations by Facebook, such as unnecessarily granting app developers consumer PII, sharing data with advertisers after representing that it would not, and allowing a user's friends' third-party applications to access the user's data, even if the user had restricted sharing to "friends only."[47] The FTC also settled with Google over the alleged secret collection of cookies from Safari browser users; Google had previously represented that it would not

41. Natasha Singer, *F.T.C. Opens an Inquiry into Data Brokers*, N.Y. TIMES (Dec. 18, 2012), http://www.nytimes.com/2012/12/19/technology/ftc-opens-an-inquiry-into-data-brokers.html?_r=0.

42. *What Information Do Data Brokers Have on Consumers, and How Do They Use It: Hearing Before the S. Comm. on Commerce, Sci. and Transp.*, 113th Cong. (2013) (statement of Jessica Rich, Director of the Bureau of Consumer Protection of the Federal Trade Commission), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-entitled-what-information-do-data-brokers-have-consumers/131218databrokerstestimony.pdf; *FTC Testifies on Data Brokers Before Senate Committee on Commerce, Science and Transportation*, FED. TRADE COMM'N (Dec. 18, 2013), http://www.ftc.gov/news-events/press-releases/2013/12/ftc-testifies-data-brokers-senate-committee-commerce-science.

43. *See* Katy Bachman, *Acxiom Gives Consumers Control of Their Data: Portal Launches as Washington Debates Data Broker Practices*, ADWEEK (Sept. 4, 2013), http://www.adweek.com/news/technology/acxiom-gives-consumers-control-their-data-152194.

44. *See Spokeo To Pay $800,000 To Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA*, FED. TRADE COMM'N (Jun. 12, 2012), http://www.ftc.gov/news-events/press-releases/2012/06/spokeo-pay-800000-settle-ftc-charges-company-allegedly-marketed.

45. *See Marketers of Criminal Background Screening Reports To Settle FTC Charges They Violated Fair Credit Reporting Act*, FED. TRADE COMM'N (Jan. 10, 2013), http://www.ftc.gov/news-events/press-releases/2013/01/marketers-criminal-background-screening-reportsto-settle-ftc.

46. *See Certegy Check Services To Pay $3.5 Million for Alleged Violations of the Fair Credit Reporting Act and Furnisher Rule*, FED. TRADE COMM'N (Aug. 15, 2013), http://www.ftc.gov/news-events/press-releases/2013/08/certegy-check-services-pay-35-million-alleged-violations-fair.

47. *Facebook Settles FTC Charges That It Deceived Consumers by Failing To Keep Privacy Promises*, FED. TRADE COMM'N (Nov. 29, 2011), http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

engage in such behavior.[48] The record $22.5 million civil penalty remains the largest among third-party data sharing settlements.[49]

To date, the FTC has not yet brought an investigation or an enforcement action for post-acquisition privacy breaches, perhaps due to the relative novelty of acquisitions or mergers involving large transfers of consumer data. The increasing frequency of tech acquisitions may change this regulatory vacuum soon. Advocacy groups' complaints regarding the announced Facebook acquisition of WhatsApp led the FTC to review the merger, and the FTC conditioned its approval on Facebook's promise to preserve the privacy policies that WhatsApp originally agreed to with its users.[50] In the absence of regulatory efforts, current privacy policy provisions dealing with post-acquisition data privacy range from complete liability waivers[51] to promises to retain the privacy levels the user and the bought-out company originally agreed to.[52]

Third-party data sharing and its regulation have a relatively short history, roughly the same age as the new millennium. Data sharing in the beginning of this history was almost entirely first-node, directly between data subject and data controller. However, this initial binary relationship and one-node structure has quickly expanded to include new methods of downstream data sharing. This rapid expansion has left regulators scrambling to develop solutions for each new issue.

---

48. *See* United States v. Google Inc., CV 12-04177 SI, 2012 WL 5833994 (N.D. Cal. Nov. 16, 2012).

49. *Google Will Pay $22.5 Million To Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FED. TRADE COMM'N (Aug. 9, 2012), http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

50. Jennifer Van Grove, *FTC OKs Facebook+WhatsApp, Warns Against Privacy Violations*, CNET (Apr. 10, 2014), http://www.cnet.com/news/ftc-oks-facebook-whatsapp-warns-against-privacy-violations/.

51. *See, e.g.*, *Privacy Policy*, BRIGHTCOVE, http://www.brightcove.com/en/privacy (last updated Apr. 25, 2012) ("We may disclose Personal Information . . . to an affiliate or other third party in the event of any reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock . . . ."); *Uber Privacy Policy*, UBER, https://www.uber.com/en-US/legal/usa/privacy (last updated Jul. 13, 2013) ("We also reserve the right to disclose and transfer all such information . . . in connection with a corporate merger, consolidation, restructuring, the sale of substantially all of our membership interests and/or assets or other corporate change, including, during the course of any due diligence process.").

52. *See, e.g.*, *Privacy Policy*, GOOGLE, http://www.google.com/policies/privacy/#nosharing (last updated Mar. 31, 2014) ("If Google is involved in a merger, acquisition, or asset sale, we will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy."); *Twitter Privacy Policy*, TWITTER, https://twitter.com/privacy (last updated Sept. 8, 2014) ("In the event that Twitter is involved in a bankruptcy, merger, acquisition, reorganization or sale of assets, your information may be sold or transferred as part of that transaction. The promises in this Privacy Policy will apply to your information as transferred to the new entity.").

III. THE REGULATORY LINEUP

It is clear that third-party data sharing is a novel legal area with much potential, both positive and negative, for change. A successful regulatory entity must be able to both adapt quickly to new changes in data sharing practices and apply a balanced approach to minimize losses of contextual integrity while preserving the socially beneficial externalities of big data. The FTC has filled the legislative and judicial void with a series of settlements and enforcement actions. This *de facto* "common law" has been criticized for reasons spanning from bureaucratic excess to lack of adequate investigation and enforcement abilities.[53] Nevertheless, the FTC remains best suited among the alternatives for the role of norm entrepreneur and watchdog in the third-party data sharing and general online privacy space.

A. Privacy Litigation

Using contract law and privacy torts as an alternative to FTC regulatory oversight has largely been unsuccessful. With greater administrative capacity than one agency, the state and federal judiciary could theoretically have enforced privacy breaches and built up online privacy jurisprudence. However, early cases quickly demonstrated that privacy policies were not the enforceable contracts people once thought they were.[54] Existing privacy torts of false light, appropriation, public disclosure of private facts, and intrusion long predated the Internet and could not apply effectively to issues brought about by third-party data sharing.[55]

Likewise, statutes which seem on their face to provide an alternative to FTC oversight do not apply to private breaches of online privacy: The 1974 Privacy Act only applies to public entities,[56] and both the Stored Communications Act and the Electronic Communications Privacy Act ("ECPA") primarily targeted intentional hacking of a criminal nature.[57] For instance, a 2001 challenge to

53. *See, e.g.*, Ken Hess, *Judge Enhances FTC's Power To Sue over Security Breaches*, ZDNET (Apr. 11, 2014), http://www.zdnet.com/judge-enhances-ftcs-power-to-sue-over-security-breaches-7000028357/ ("The broadening of the FTC's powers . . . extends the government's ability to destroy businesses."); Maass, *supra* note 14.

54. *Cf.* Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. INTELL. PROP. L. 57, 91–92 (1999) ("[A] privacy policy bears all the earmarks of a contract, but perhaps one enforceable only at the option of the user.").

55. *See generally* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 388–89 (1960).

56. 5 U.S.C. § 552(f)(1) (2012) ("'[A]gency' as defined in section 551(1) of this title includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government . . . .").

57. *See* 18 U.S.C. §§ 2511(4)(a), 2701 (2012).

DoubleClick's use of cookies to deliver targeted advertising to users on the grounds that it violated ECPA failed, largely because DoubleClick's activities did not fit ECPA's intended scope of wiretapping and electronic snooping.[58]

Privacy litigation faces stumbling blocks in the form of unclear enforceability of privacy policies and a difficulty demonstrating actionable harms within current legal frameworks. In *Dwyer*, the court did not recognize the sale of PII to third parties as an actionable harm.[59] In any case, the tort of appropriation ("appropriat[ing] to his own use or benefit the name or likeness of another") fits badly with the new reality of massive data collection and behavioral advertising.[60] Proponents of contractual breach or promissory estoppel theories similarly failed to successfully demonstrate an actionable legal harm.[61] Other privacy torts served equally little purpose; the tort of public disclosure of private facts required being "highly offensive to the reasonable person" and "not of legitimate concern to the public," which was a poor fit to the sale of aggregated consumer data.[62] While data was being transferred to contexts that consumers had not agreed to, third-party data sharing was not necessarily offensive or publicly disclosed.[63]

The problems of unenforceability and statutory inapplicability prevent privacy litigation from effectively safeguarding contextual integrity in third-party data sharing. The infrequency of successfully litigated privacy lawsuits and class actions are indicative of the difficulties plaintiffs face in either demonstrating a harm recognized by the existing statutory language or negotiating a meaningful remedy through the judicial system in this area.

B. Self-Regulation

Self-regulation has been a dominant regulatory approach in the privacy sphere and continues to be widely popular amongst industry actors and government agencies alike.[64] The focus is providing consumers with notice to enable informed decision-making, rather

58. Solove & Hartzog, *supra* note 15, at 591.
59. See *supra* note 17.
60. *Id.* at 590–91.
61. *Id.* at 596.
62. *Id.* at 591.
63. *Id.*
64. Jim Adler, *When Self-Regulation Works, Your Privacy Is In Good Hands*, TRUSTE BLOG (Jul. 27, 2012), http://www.truste.com/blog/2012/07/27/when-self-regulation-works-your-privacy-is-in-good-hands/; Katy Bachman, *FTC's Ohlhausen Favors Privacy Self-Regulation*, ADWEEK, (Jun. 5, 2013), http://www.adweek.com/news/technology/ftcs-ohlhausen-favors-privacy-self-regulation-150036 (stating Commissioner Ohlhausen has spoken out against baseline privacy legislation and thinks self-regulation in conjunction with FTC enforcement is enough).

than encouraging or discouraging particular ways of data sharing. Proponents argue that industry players know the technology and consumers better than the government does and that regulatory attempts routinely fail to effectively address issues or anticipate innovation.[65] However, this argument is only half-correct. While industry has those advantages, self-regulation by itself is insufficient due to fundamental flaws in the incentive structure and consumer cognitive biases, which undermine the notice-and-choice model's major assumption of rational decision-making.[66]

The current notice-and-choice framework with the privacy policy as the primary instrument of disclosure is largely the product of self-regulatory measures.[67] The Clinton Administration's Information Infrastructure Task Force twice recommended self-regulation through privacy policies for the fledgling e-commerce industry, in its 1995 and 1997 reports on online data sharing.[68] These privacy policies gave users information on data collection and sharing practices and then allowed users to choose whether to continue to use the service. Sometimes, users would be given an opt-out right to elect to have their data not be collected.[69] Legislators codified this proposed framework, mandating privacy policies in statutes such as the Gramm-Leach-Bliley Act ("GLBA").[70]

Despite its popularity, self-regulation alone is not sufficient as a regulatory method due to the lack of competitive or regulatory pressure for companies to optimize privacy practices. While the benefits of third-party data sharing, such as added profits or consumer base, are immediately visible, the costs of doing so are diffuse and long-term.[71] The incentives are simply not aligned in a way that prompts companies to provide consumers with meaningful tools to realize contextual integrity online.[72] Absent regulation, a market failure arises where market forces seek to maximize information sharing and corresponding monetization at the expense of consumer privacy.

---

65. *See* Adler, *supra* note 64.

66. Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–81 (2013).

67. *See* Solove & Hartzog, *supra* note 15, at 588.

68. *Id*. at 594.

69. *Id*. at 592.

70. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended at 15 U.S.C. § 6803 (2012)); *see also* Solove and Hartzog, *supra* note 15, at 594.

71. Consumers are unlikely to walk away from a service due to dissatisfaction with their privacy practices. Hayley Tsukayama, *People Care More About Convenience than Privacy Online*, WASH. POST (Oct. 7, 2014), *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/07/people-care-more-about-convenience-than-privacy-online/

72. *See* Lauren E. Willis, *Why Not Privacy by Default?*, 29 BERKELEY TECH. L.J. 61, 74–80 (2014) (addressing at length the cognitive biases that hamper effective consumer decision-making in the privacy sphere).

Suboptimal corporate incentives and consumer-side cognitive obstacles create notice that is more form than substance. Most privacy policies are lengthy and full of dense legalese, and almost no one reads them.[73] Adding to the impracticality is the sheer number of privacy policies an individual encounters daily — to read all of them would take 250 hours (roughly a month) each year.[74] Even for the rare consumer who reads the privacy policy, understanding the implications is difficult due to framing effects and other manifestations of bounded rationality.[75] The time and resources required for effective notice are too excessive for the average consumer,[76] and worse, companies are not incentivized to ease the task in the absence of regulation.[77]

With such problems in notice, the subsequent consent is unlikely to be meaningful. Many policies offer a binary choice — take it or leave it — forcing users to choose either to disclose information in ways they dislike or not use the service at all.[78] With the increasing utility and widespread use of some online services, opting out entirely because the user disagrees with the service's information sharing practices is untenable.[79] Contextual integrity requires a nuanced ability to calibrate disclosure attuned to different circumstances, but too much choice can often be as bad as having no choice.[80] Excessive granularity in privacy settings only confuses consumers, leading them to exercise less control than if the settings were easier to understand.[81]

Self-regulation's favored notice-and-choice framework ignores consumer-side cognitive biases and company-side lack of incentive to provide the best privacy practices. Notice-and-choice puts considerable onus on consumers to make the right decision in a timely fashion every single time, but given privacy policies' temporal

---

73. Solove, *supra* note 66, at 1884–85.

74. Shankar Vedantam, *To Read All Those Privacy Policies, Just Take a Month Off Work*, NATIONAL PUBLIC RADIO: ALL TECH CONSIDERED (Apr. 19, 2012), http://www.npr.org/blogs/alltechconsidered/2012/04/19/150905465/to-read-all-those-web-privacy-policies-just-take-a-month-off-work.

75. Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES 363, 369 (Alessandro Acquisti et al. eds., 2008) ("[O]ur innate bounded rationality limits our ability to acquire, memorize, and process all relevant information, and it makes us rely on simplified mental models, approximate strategies, and heuristics.").

76. Solove, *supra* note 66, at 1883 ("A number of cognitive problems plague privacy self-management. . . . [E]mpirical evidence and social science literature demonstrate that people's actual ability to make such informed and rational decisions does not even come close to the vision contemplated by privacy self-management.").

77. Willis, *supra* note 72, 67–68 ("Unless robust competition over protecting consumer privacy develops in the marketplace — a doubtful prospect — firms will generally prefer for consumers to be in the Track-Me [data collection as a default] position.").

78. *See, e.g.*, FACEBOOK, *supra* note 1.

79. Solove, *supra* note 66, at 1884.

80. *Id.* at 1885.

81. *Id.*

detachment from downstream data sharing, the likelihood of long-term maintenance of contextual integrity in even a single privacy transaction is low. Maintaining one's contextual integrity in one's overall Internet identity, then, becomes a nearly impossible task.

C. The Federal Trade Commission and Its "Common Law"

In the context of inadequate statutory and judicial alternatives, the FTC has risen to be the primary player in third-party data sharing and online privacy. Its settlement orders and enforcement actions have established a robust "common law" that has de facto precedential power. This *de facto* common law also puts data controllers on notice as to what the expected privacy standards are, minimizing potential inequities that jurisdictional differences in judge-made standards could bring. Critics are wary of this growth in agency power and are skeptical of the FTC's administrative reach and enforcement potential.[82] However, the FTC is currently best situated to institute contextual integrity in third-party data sharing: FTC regulation serves as a necessary and effective supplement to self-regulatory regimes by incentivizing good privacy practices.

Under its general FTC Act authority to prohibit "unfair and deceptive" practice in commerce,[83] the FTC enjoys a wide jurisdiction. Beginning with passage of the FCRA[84] in 1970, the FTC's jurisdictional scope was expanded with the enactment of the Children's Online Privacy Protection Act ("COPPA") in 1998.[85] Other laws directly under the FTC's regulatory purview include the GLBA[86] and the U.S.-EU Safe Harbor Arrangement.[87] Unlike other countries that have centralized data protection agencies,[88] the U.S. has increasingly turned to the FTC in international privacy matters. The FTC has even stepped in to regulate privacy-related disputes, although it does not have a direct enforcement role for statutes such as the

82. Hess, *supra* note 53 (arguing that recent expansion of FTC regulatory authority into data security is vulnerable to abuse).

83. 15 U.S.C. § 45(a)(1) (2012).

84. 15 U.S.C. § 1681s(a)(1) (2012).

85. 15 U.S.C. § 6505(a) (2012).

86. *Id.*

87. *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://www.export.gov/safeharbor/eu/eg_main_018476.asp (last updated Dec.18, 2013).

88. Many EU and Asian countries have adopted this model. Examples include the UK's Information Commissioner's Office, the Germany's Federal Commissioner for Data Protection and Freedom of Information, and South Korea's Korea Internet and Security Agency. *See Who We Are*, INFO. COMM'R'S OFFICE http://ico.org.uk/about_us/our_organisation/introduction (last visited Dec. 18, 2014); GERMANY'S FED. COMM'R FOR DATA PROT. AND FREEDOM OF INFO., http://www.bfdi.bund.de/DE/Home/home_node.html (last visited Dec. 18, 2014); KOREA INTERNET AND SEC. AGENCY, http://www.kisa.or.kr/eng/main.jsp (last visited Dec. 18, 2014).

GLBA[89] and Health Insurance Portability and Accountability Act ("HIPAA").[90]

A common criticism of FTC regulation is that, as an agency, the FTC lacks legal teeth to enforce rulings like the judiciary can.[91] Without a general authority to fine violators, any civil penalties remain rare and, if issued, laughably small.[92] However, the FTC has real enforcement power — it just differs from that of a court. More than fifty percent of FTC decision orders contain a twenty-year audit provision, which is cumbersome and lengthy.[93] Both legal practitioners and industry players pay great attention to these consent orders, respecting them as they would common law rulings.[94] The considerable deference that courts accord to agencies also means that settlement orders are rarely challenged.[95] Solove and Hartzog also emphasize the reach of the FTC's "soft law," analogous to courts' dicta, created through frequent white papers and reports on various cutting-edge technologies and the privacy issues that stem from them.[96]

While the above critique concerns the FTC's lack of power, another critique claims that the FTC does too much, overreaching the power entrusted to it by Congress. In the recently decided *F.T.C. v. Wyndham*, the District Court of New Jersey affirmed the FTC's standing to sue companies on consumers' behalf for data breaches under the "unfairness" prong of its FTCA section 5 authority.[97] Wyndham, along with the Department of Commerce, claimed that this authority blames the victim for being attacked and grants discretionary power Congress did not legislate.[98] Nevertheless, the court rightly held that in the current statutory vacuum, the FTC's exercise of authority is not inconsistent with existing laws.[99] Given the FTC's existing privacy enforcement experience and the lack of other sufficient alternatives, it makes more sense to ensure that the

89. Gramm-Leach-Bliley Act, 15 USC § 6804 (2012).

90. *See, e.g.*, *FTC Affirms Data Security Authority over HIPAA-Covered Entities*, iHEALTHBEAT (Jan. 29, 2014), http://www.ihealthbeat.org/articles/2014/1/29/ftc-affirms-data-security-authority-over-hipaacovered-entities.

91. *See* Ryan Singel, *FTC Tells Net: Agree To Stop Invading Privacy (or We'll Say 'Stop' Again)*, WIRED (Mar. 26, 2012), http://www.wired.com/2012/03/ftc-privacy-report/.

92. Solove & Hartzog, *supra* note 15, at 605–06 ("[T]he FTC issued a $22.5 million dollar fine, the largest fine for privacy violations in its history. But as at least one news media article noted, the fine 'is a small drop in the bucket'. . . .").

93. *Id.* at 606.

94. *Id.*

95. *Id.* at 613.

96. *Id.* at 626.

97. F.T.C. v. Wyndham Worldwide Corp., No. 13-1887 (ES), 2014 WL 2812049, at *8 (D.N.J. Jun. 23, 2014); *see also* Hess, *supra* note 53.

98. Thomas O'Toole, *Wyndham Case Threatens To Put FTC out of Data Security Business*, BLOOMBERG BNA: E-COMMERCE & TECH. L. BLOG (Jul. 18, 2013), http://www.bna.com/wyndham-case-threatens-b17179875319/.

99. *Wyndham*, 2014 WL 1349019, at *10–11.

FTC is exercising regulatory authority properly than it does to assert that the FTC is not suited for the job.

A final critique highlights the FTC's lack of resources to conduct expansive investigations, which leads to unpredictable and arbitrary enforcement.[100] Indeed, the FTC relies on the support of advocacy groups such as the Electronic Frontier Foundation ("EFF") or Electronic Privacy Information Center ("EPIC") and enterprising computer science graduate students to find privacy violations.[101] The number of privacy-related investigations has remained low, with thirty-two legal actions brought as of May 1, 2011.[102] However, these are actually good developments: the FTC should not try to be an enforcer of every small violation nor serve as a complete substitute for self-regulation. Rather, the FTC should attempt to create a general online privacy framework. The successful operation of this framework relies on robust self-regulation and notice from specialist organizations.

A combination of FTC enforcement actions and guidance as well as industry self-regulation is best suited to preserve contextual integrity in third-party data sharing.[103] Self-regulation ensures regulatory measures are up-to-date with technological innovation. FTC guidance encourages companies to provide consumers with privacy options that allow for greater contextual integrity. Finally, FTC enforcement actions incentivize companies to follow through on their privacy promises.

III. POLICY RECOMMENDATIONS FOR DOWNSTREAM DATA USE REGULATIONS

How should the FTC foster contextual integrity in third-party data sharing? Baseline norms are arguably easier to establish in direct, first-node relationships like data breaches and data controllers' privacy violations. The additional step down the chain, to the second node, erodes accountability and enforceability, delaying regulatory progress in this area.[104] Self-regulators' notice-and-choice model has

100. Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673 (2013).

101. Maass, *supra* note 14.

102. *Enforcing Privacy Promises*, FED. TRADE COMM'N, http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises.

103. *See* Solove & Hartzog, *supra* note 15, at 594.

104. In comparison to general privacy violation cases that began in the late 1990s, the first third-party data sharing case did not occur until *NRCCUA* in 2003. Enforcement has not yet reached subsequent buyers — for example, post-acquisition third parties have never been the subject of any FTC investigation.

been insufficient in giving either meaningful notice or choice.[105] To better promote contextual integrity, the FTC needs to look beyond the standard notice-and-choice model by: (1) adding greater consumer control and accessibility; (2) promoting greater accountability and fairness in liability distribution; and (3) encouraging innovative self-regulation for just-in-time privacy by design.

A. Greater Control and Accessibility

The current notice-and-choice model gives consumers too little control and accessibility when it comes to third-party data sharing. One way to mitigate this situation is to afford greater accessibility to third-party data sharing paths and grant opt-out rights where feasible.

One such third-party data-sharing avenue is the post-acquisition transfer of data to buyers. Currently, the vast majority of privacy policies at most give notice to users on the event of the company's sale, and sometimes not even then.[106] Companies that ensure equal privacy levels post-acquisition are few and far between.[107] However, the FTC has recently made progress on post-acquisition contextual integrity by reviewing Facebook's acquisition of WhatsApp, a popular mobile messaging app.[108] WhatsApp had represented that no data would be shared with third parties for advertising purposes, and the FTC conditioned approval of the deal on Facebook continuing to uphold pre-acquisition promises that WhatsApp made to its users.[109]

Another way to improve notice-and-choice would be to incorporate more consumer control on third-party data sharing in privacy dashboards, which serve as up-to-date summaries of an

105. FTC PRIVACY REPORT, *supra* note 40, at 11–12 (discussing how self-regulatory measures have fallen short in providing notice regarding collected data as well as inadvertent or unforeseen downstream data uses that have eroded trust).

106. *See, e.g.*, *Facebook Settles FTC Charges That It Deceived Consumers by Failing To Keep Privacy Promises*, *supra* note 47.

107. *See, e.g.*, *Privacy Policy*, INSTACART, https://www.instacart.com/privacy (last updated May 14, 2014) ("Instacart may share personal information . . . in connection with, or during negotiations of, any merger, sale of company assets, financing or acquisition, or in any other situation where personal information may be disclosed or transferred as one of the business assets of Instacart."); *Privacy Policy*, AIRBNB, https://www.airbnb.com/terms/privacy_policy (last updated Apr. 7, 2014) ("If Airbnb undertakes or is involved in any merger, acquisition, reorganization, sale of assets or bankruptcy or insolvency event, then we may sell, transfer or share some or all of our assets, including your Personal Information.").

108. *See* Letter from Jessica Rich, Director of the FTC's Bureau of Consumer Protection, to Erin Egan, Facebook's Chief Privacy Officer, and Anne Hoge, WhatsApp Inc.'s General Counsel (Apr. 10, 2014), *available at* http://epic.org/privacy/internet/ftc/whatsapp/FTC-facebook-whatsapp-ltr.pdf.

109. *See id.*; Zach Miners, *FTC Clears Facebook's WhatsApp Deal, but Warns on Data Collection*, PCWORLD (Apr. 10, 2014), http://www.pcworld.com/article/2142520/ftc-implores-whatsapp-to-keep-its-promises-on-privacy-in-facebook-deal.html.

individual's data collected by a company.[110] Prominent industry examples include the Google Dashboard and Acxiom's aboutthedata.com, which allow verified users to chart data collection and sharing.[111] Another way, although less effective than voluntary disclosure, is to mandate disclosure if requested.[112] The FTC has already endorsed such measures as part of a broader initiative called "Reclaim Your Name," launched by Commissioner Julie Brill in July of 2013, which seeks to enhance data accessibility and corporate accountability.[113]

Data accessibility and control measures are important steps forward for contextual integrity, which requires the ability to both determine how contexts differ and exercise different information disclosure practices, if desired. Greater accessibility is thus a stepping-stone to exercising meaningful control, which is in turn necessary to maintain contextual integrity in third-party data sharing. The degree of notice and choice is a balancing act; giving consumers too many choices may hinder effective decision-making. Complete opt-in powers for each data sharing transaction (as is advocated by the EU explicit consent paradigm)[114] may not be practically effective due to transaction costs and cognitive biases in decision-making.[115]

Instituting an opt-out right for post-acquisition data sharing and solidifying privacy dashboards as an established standard (like privacy policies ten years ago) would strike an adequate balance. Excessive consent requirements could disincentivize tech-industry mergers, in which consumer data is an important bargaining chip and a driver of high startup valuations. Cumbersome and frequent consent requirements could be seen as paternalistic, annoy consumers who do not mind the data sharing, and reduce the likelihood that consumers will pay attention to instances of data sharing they actually care about. Any opt-out right should be easily accessible yet not disruptive, striking the right balance in both notice and consent. Of course, any opt-out right reduces the pool of users from which data could be collected. However, depriving consumers of opt-out rights altogether risks FTC scrutiny as well as bad publicity for the successor business.

---

110. Erick Schonfeld, *Google Gives You a Privacy Dashboard To Show Just How Much It Knows about You*, TECHCRUNCH (Nov. 5, 2009), http://techcrunch.com/2009/11/05/google-gives-you-a-privacy-dashboard-to-show-just-how-much-it-knows-about-you/.

111. *Dashboard*, GOOGLE, https://www.google.com/settings/dashboard (login required) (last visited Dec. 18, 2014); ABOUTTHEDATA.COM, https://aboutthedata.com/ (last visited Dec. 18, 2014).

112. A state implementation of this idea is the California "Shine the Light" law, which obligates corporate entities to make the data collected about a particular consumer available upon request. *See* CA Civil Code §§ 1798.80–84 (2009).

113 Julie Brill, Commissioner, Fed. Trade Comm'n, Keynote Address at the 23rd Computers Freedom and Privacy Conference (Jun. 26, 2013), *available at* http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf.

114. Solove, *supra* note 66, at 1897.

115. *Id.* at 1898.

While ensuring contextual integrity is an important step forward from mere notice in post-acquisition data privacy, the FTC must go further in encouraging an opt-out right easily accessible by those users who disagree with their data being shared with the new owner.[116]

B. Greater Accountability down the Data Chain

Liability distribution in third-party data sharing is more complex and therefore needs more nuance than standard privacy contracts made between data subject and controller. Under the current notice-and-choice model, the data subject consents to the entire possible chain of data sharing at the first link in the chain. This is harmful both for the consumer (who cannot effectuate contextual integrity) and the data controller (who cannot control or be wholly responsible for all downstream privacy breaches). A more equitable balance of liabilities is required for greater accountability in third-party data sharing.

Data controllers are the actors who initially transfer consumer PII to third parties, the onus should be on data controllers both to provide accurate accounting and to require third parties to uphold the privacy promises that data controllers made to users. Due to the difficulty of tracking down and deleting data once it is out of the data controller's hands, preventive measures by the data controllers are best suited to avoid undesirable or unsecure data transfers. The FTC has moved to penalize data controllers when third-party contractors do not follow adequate security practices. In *GMR Transcription Services Inc.*, the FTC found that GMR had failed to require its contractors to implement security practices such as installing antivirus applications, following adequate data storage and encryption practices, and adopting review measures to ensure compliance with GMR standards.[117] *Wyndham* employed a similar liability distribution in that the FTC fined the data controller for having inadequate security practices that exposed it to data breaches.[118] Such a distribution of liability incentivizes best practices in choosing reliable service providers and affiliated third parties and in upholding consumer promises in these second-order interactions without discouraging participation.

One criticism of a liability regime where the data controller solely bears the blame is that it excessively burdens data controllers and fails to incentivize third parties to adopt and follow adequate privacy

116. FTC is currently conditioning this as an after-the-fact remedy: express consent and opt-out opportunity. *See* Miners, *supra* note 109.

117. GMR Transcription Servs., Inc., et al., FTC File No. 122-3095, 2104 WL 492352 (2014) (Decision and Order), *available at* http://www.ftc.gov/system/files/documents/cases/140203gmragree.pdf.

118. *See* F.T.C. v. Wyndham Worldwide Corp., 2014 WL 1349019, at *6 (D.N.J. Apr. 7, 2014).

practices.[119] The same incentive problems plague a system where the FTC only investigates the third parties in question; data controllers would not have an incentive to relay all privacy promises made, and socially beneficial third-party sharing may be discouraged. Instead, liability distribution should adopt a sliding-scale approach, comparing the data controller's reasonable efforts to keep privacy promises with that of the third party. In *GMR*, while the data controller had failed to implement "reasonable and appropriate security measures,"[120] the FTC should also have held the third party accountable.

The FTC should work with data controllers to set minimum contracting standards with subcontractors and other third parties and ensure that such requirements are represented to the public as part of a controller's privacy policy.[121] The burden is on the data controller to find competent, reliable subcontractors and then contractually obligate them to adhere to company standards. After that, the burden shifts to the subcontractor to adhere to the provisions of the contract. *GMR* will likely only be a precursor to many more third-party data sharing cases, and the distribution of liability must be equitable to ensure continued participation and socially beneficial data sharing.

C. Privacy By Design

Effective choice requires the easy availability of relevant information at the time the decision is being made. Privacy By Design is an approach to protecting privacy that aims to foster this dimension of contextual integrity for individuals by incorporating privacy "at all stages of the design and development of products and services."[122] The FTC has already adopted it as a key privacy framework.[123] Standard privacy policies front-load privacy decision-making before users have had a chance to evaluate key factors such as their experience with the service. The privacy policy is forgotten by the time actual data sharing takes place as the consumer uses the service.

---

119. Amicus Brief of Chamber of Commerce of the United States of America, et al., Fed. Trade Comm'n v. Wyndham Hotels & Resorts, LLC, et al., No. 2:13-CV-01887-ES-SCM (D.N.J. 2012), at 5 ("Permitting the FTC to proceed on a theory that suffering a data breach is an 'unfair' trade practice would expose most businesses in America to the potential for a government enforcement action whenever that business suffers a cyber attack.").

120. *See GMR*, FTC File No. 122-3095.

121. Minimal contracting standards as a way to preserve privacy protections in second-node contexts is slowly gaining ground. *See, e.g.*, Student Online Personal Information Protection Act, S.B. 1177 § 22584(b)(4)(E) (setting contractual guidelines for third party service providers to adhere to); EU General Data Protection Directive draft, Article 14(1)(b) (requiring data subject access to terms of contracts data controllers entered into).

122. Edith Ramirez, Commissioner of the Fed. Trade Comm'n, Remarks at the Privacy by Design Conference (Jun. 13, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-design-and-new-privacy-framework-u.s.federal-trade-commission/120613privacydesign.pdf.

123. *Id.*; *see also* FTC PRIVACY REPORT, *supra* note 40, at 22.

Privacy By Design's concept of just-in-time availability of relevant privacy choices needs to be expanded to include choices about third-party data sharing.

Effective Privacy By Design would be integrated into the service, available when the privacy-related information is most relevant and helpful, but would otherwise remain unobtrusive. Facebook's new "Privacy Checkup" feature[124] is a good example of a privacy-enhancing tool that is situation-specific (appearing to those who have not changed their settings in a while and are posting publicly) and just-in-time (appearing when the user is typing in such a post). Unlike direct sharing, third-party data sharing often happens after-the-fact, making anticipation of downstream data use cases at the point of initial data collection difficult.[125] However, effective notification is still possible through methods such as supplementary information next to targeted advertising, which notifies the user what information has been used to serve the ad and points to a privacy dashboard or similar tool that may be used to set relevant privacy preferences. Consumers could also be notified while behavioral or geo-locational tracking is occurring, again in a variety of easily accessible locations.[126] This way, opportunities to exercise preferences regarding third-party data sharing can bookend the user's experience.

Effective Privacy By Design is clear and simple. The major stumbling block to Privacy By Design lies in the "Design" part — how to provide effective just-in-time information that consumers need in order to make informed decisions without being paternalistic or disruptive. There is much room for improved clarity in conveying privacy information to users, ranging from simplifying privacy policies[127] to reducing clutter on privacy settings pages and other privacy-related tools. Other ideas emphasizing before-the-fact certification include a "Privacy Nutrition Label" or "Privacy Tags" that convey privacy information in a visually simple manner.[128] Some

---

124. "Privacy Checkup" is a Facebook experiment to ensure people are sharing with the people they want to on Facebook when their settings are public. Reed Albergotti, *Facebook's Blue Dino Wants You To Mind Your Posting*, WALL ST. J. DIGITS (Apr. 1, 2014), http://blogs.wsj.com/digits/2014/04/01/facebooks-blue-dino-wants-you-to-mind-your-posting/.

125. *See* Solove, *supra* note 66, at 1902.

126. *See* Yan Fang, *The Death of the Privacy Policy? Effective Privacy Disclosures After* In Re Sears, 25 BERKELEY TECH. L.J. 671, 696 (2010).

127. Many privacy experts suggest a layered privacy policy where consumers are given clear, basic information with accessible links to additional information. *See, e.g.*, Mehmet Munur, Sarah Branam & Matt Mrkobrad, *Best Practices in Drafting Plain-Language and Layered Privacy Policies*, INT'L ASSOC. OF PRIVACY PROF'LS (Sept. 13, 2012), https://www.privacyassociation.org/publications/2012_09_13_best_practices_in_drafting_plain_language_and_layered_privacy.

128. Corey A. Ciocchetti, *The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices*, 26 J. MARSHALL J. COMPUTER & INFO. L. 1, 30–31 (2008).

external browser apps currently attempt to fill the disclosure gap by providing a standardized assessment of privacy practices of the websites that the user visits.[129] Again, the importance of balance cannot be understated: While a simple and clean user interface is crucial for accessibility, these features must be informative enough so as to actually improve understanding.

Effective Privacy By Design should not only assist privacy decisions when they are being made but also raise baseline awareness before those decisions are made. Despite its widespread nature, third-party data sharing remains a relatively obscure part of mainstream privacy discourse. The FTC should continue to work to raise consumer awareness regarding third-party data sharing and the costs and benefits that come with it.[130] This should be combined with initiatives to improve anonymization techniques that reduce consumer risk of re-identification and identity theft. Current anonymization techniques are easily circumvented by re-identification.[131] However, researchers continue to develop promising new techniques such as differential privacy (injecting a privacy-preserving intermediary between recipient and data set)[132] and synthetic data sets (a computer-generated data set calibrated to yield the same statistical inferences as the real data set without exposing data subjects' PII).[133] The FTC should remain abreast of these advances and raise the baseline for technology that companies are expected to use when handling aggregated consumer PII so that users face privacy decisions in already improved contexts.

IV. CONCLUSION

Third-party data sharing is here to stay and will only accelerate as the technology industry explores and develops further avenues of aggregated data use. In an era of cheap, rapid data sharing, maintaining contextual integrity in third-party data sharing is harder than ever. Despite its imperfections, the FTC remains the best

129. *Privacy Dashboard*, W3C, http://code.w3.org/privacy-dashboard/ (last visited Dec. 18, 2014).

130. Media exposure and consumer attention are often prerequisites for meaningful institutional change in privacy. *See* Chris Jay Hoofnagle & Jennifer King, *Consumer Information Sharing: Where the Sun Still Don't Shine*, BERKELEY LAW 2, https://www.law.berkeley.edu/files/sb27report.pdf (last visited Dec. 18, 2014).

131. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymity*, 57 UCLA L. REV. 1701, 1716–25 (2010) (discussing how anonymization as a privacy protection model is increasingly eroding with new re-identification techniques).

132. MICROSOFT CORP., DIFFERENTIAL PRIVACY FOR EVERYONE (2012), *available at* http://www.microsoft.com/en-us/download/details.aspx?id=35409.

133. *See, e.g.*, Rakesh Agrawal & Ramakrishnan Srikant, *Privacy-Preserving Data Mining*, 29 ACM SIGMOD REC. 439, 447 (2000); John M. Abowd & Lars Vilhuber, *How Protective Are Synthetic Data?*, *in* PRIVACY IN STATISTICAL DATABASES 239, 239 (Josep Domingo-Ferrer & Yücel Saygin eds., 2008).

institution to develop, with the input of industry leaders, effective safeguards for consumer privacy that will foster continued innovation. Looking beyond the notice-and-choice model to greater control and accessibility, ensuring accountability in each node of the data sharing chain, and incorporating Privacy by Design are essential steps in the process of reclaiming consumer control over PII and disincentivizing reckless sharing of consumers' PII.