PRIVACY GOVERNANCE FOR INSTITUTIONAL TRUST (OR ARE PRIVACY VIOLATIONS AKIN TO INSIDER TRADING?)

KIRSTEN MARTIN*

ABSTRACT

Currently, we frame individuals online as in a series of exchanges with specific firms, and privacy, accordingly, is governed to ensure trust within those relationships. However, the focus on the relationship between consumers and specific firms does not capture how the online environment behaves. The aggregation and secondary use of consumer data is performed by market actors behind the scenes without any relationship with consumers. Trusting a single firm is not enough; individuals must trust the online market in general. Such institutional trust has gone under-examined in regards to privacy online. Little has been done to measure how aggregating and using consumer data supports a larger online market and impacts institutional trust online.

This paper explores how privacy governance should also be framed as protecting a larger market to ensure consumers trust being online. In a series of studies, I empirically examine (a) how typical secondary uses are judged along a generalized (for the good of the market) versus reciprocal (for the good of the consumer) exchange and impact institutional and consumer trust, and (b) whether governance mechanisms (limitations on the use of data such as adequate notice, auditing, non-identifiable information, limited storage, etc.) increase consumer trust in companies. I find:

- *Respondents find secondary uses of consumer data more appropriate if judged more within a generalized exchange (academic research) or within a reciprocal exchange (product search results) or both (credit security). However, most secondary uses of data are deemed privacy violations and decrease institutional trust online.*
- *Using privacy notices is the least effective governance*

* Associate Professor, George Washington University. I would like to thank the participants of the *Washington University Law Review* Symposium on Privacy and Trust in a Digital Age (September 2018) for their helpful comments on an earlier version of this paper. I am grateful for support from the National Science Foundation under Grant No. No. 1649415. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

mechanism of those included here whereas being subject to an audit was as effective as using anonymized data in improving consumer trust.

- *Institutional trust online impacts a consumer's willingness to engage with a specific online partner in a trust game experiment*

The findings have implications for public policy and practice. Secondary uses of information online need not only be justified in a simple quid-pro-quo exchange with the consumer but could also be justified as appropriate for the online context within a generalized exchange. However, the majority of secondary uses currently popular cannot be justified as within either a general exchange or a reciprocal exchange and are judged inappropriate, violations of privacy, and decrease both interpersonal and institutional trust.

Second, if privacy violations hurt not only interpersonal consumer trust in a firm but also institutional trust online, then privacy would be governed similar to insider trading, fraud, or bribery—to protect the integrity of the market. Punishment for privacy violations would be set to ensure bad behavior is curtailed and institutional trust is maintained rather than to remediate a specific harm to an individual.

TABLE OF CONTENTS

INTRODUCTION 1369
I. REGULATING PRIVACY AND TRUST 1377
A. *Regulating Privacy to Protect Individual Rights* 1378
B. *Regulating Privacy to Protect Relationships* 1379
C. *Regulating Privacy for Institutional Trust* 1381
D. *Research Implications* 1382
II. STUDY 1: SECONDARY USES OF CONSUMER INFORMATION 1384
A. *Design Study 1* 1384
B. *Results Study 1* 1386
C. *Discussion Study 1* 1387
III. STUDY 2: VIGNETTE STUDY ON USE OF DATA AND TRUST 1387
A. *Design Study 2* 1388
1. *Vignette Factors (Independent Variables in the Vignette)* 1388
2. *Vignette Design* 1389
3. *Rating Task* 1390
4. *2x2 Design* 1391
B. *Results Study 2* 1392
1. *Consumer Trust in a Firm* 1392
2. *Governance Mechanisms* 1393
3. *Institutional Trust* 1396
C. *Discussion Study 2* 1398
IV. STUDY 3: EXPERIMENT 1398
A. *Design Study 3* 1400
B. *Results Study 3* 1401
C. *Discussion Study 3* 1401
V. DISCUSSION AND CONCLUSION 1403
A. *Institutional Trust and Privacy Violations* 1404
B. *Secondary Use of Data* 1406
C. *Governance Mechanisms* 1407
CONCLUSION 1408

INTRODUCTION

Trust makes markets work. Trust facilitates transactions, supports individuals entering a market, decreases the need for expensive safeguards, and limits bureaucratic inefficiencies. Sometimes trust is personal, such as when we decide to trust a local dry cleaner to take care of our clothes. Other times trust is more general, such as when I took my daughter to a hospital

based only on the recommendation of a stranger.[1]

For consumers concerned about privacy online, trust has been elusive. Online, consumers increasingly judge firms to be untrustworthy including firms who keep information for a secondary use,[2] who partner with a data aggregator,[3] or who store information.[4] Regulators and scholars seek to understand how privacy is related to trust between market actors, e.g., through the Federal Trade Commission's (FTC) focus on informed choice within a relationship, through the promotion of information fiduciaries or data stewards that emphasize honesty and discretion within a relationship,[5] or through a more robust tort for breach of confidentiality between market actors.[6] Such focus on interpersonal trust seeks to optimize transactions between market actors.[7] When trust is insufficient and a market actor needs expensive safeguards to protect themselves against opportunistic partners, the actor considers alternative forms of governance, such as choosing a competitor, building out the competence themselves, or switching governance structures.[8] Repeated bad acts by firms are identified and

---

1. My daughter split open her hand playing basketball at a tournament in Teaneck, New Jersey. We live in Maryland. I asked a stranger for the nearest hospital, a few agreed on the best one, and, five minutes later, we walked in. The triage nurse took her vitals, a stranger gave her a few shots and took a needle to her hand. I showed someone a piece of plastic with insurance information. One hour later, she was back on the bench watching her teammates.

2. Kirsten Martin, *The Penalty for Privacy Violations: How Privacy Violations Impact Trust Online*, 82 J. BUS. RES. 103, 104 (2018).

3. Kirsten Martin & Helen Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, 31 HARV. J.L. & TECH. 111, 120 (2017).

4. Pedro Giovanni Leon et al., *Privacy and Behavioral Advertising: Towards Meeting Users' Preferences*, SYMP. ON USABLE PRIVACY & SECURITY 6 (2015); JOSEPH TUROW ET AL., AMERICANS REJECT TAILORED ADVERTISING AND THREE ACTIVITIES THAT ENABLE IT 23 (2009); JOSEPH TUROW ET AL., THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO EXPLOITATION 4 (2015); Blase Ur et al., *Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising*, SYMP. ON USABLE PRIVACY & SECURITY 4 (2012).

5. As noted by Professors Richards and Hartzog,

> Missing from the individual view of privacy and security law is the more nuanced understanding that in a connected society, privacy is not just an individual concern, but a major building block for society as a whole. This is privacy's trust gap. Our dominant legal framework is frequently insufficient or incapable of comprehending the real and important injuries to the trust we need to flourish in our networked, digital society.

Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1200–01 (2017). Further, "Trustworthy data stewards have four characteristics that promote trust: they are honest, discreet, protective, and loyal." *Id.* at 1213. *See also* Jack Balkin on information fiduciaries. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C.D. L. REV. 1183 (2016).

6. Rather than examining whether information is in public or private, Waldman suggests we examine if the information was shared within a trusting relationship. Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559, 600–01 (2014).

7. Brown et al. note an ideal situation where "[l]ow effort or bad quality is penalized by the termination of the relationship." Martin Brown et al., *Relational Contracts and the Nature of Market Interactions*, 72 ECONOMETRICA 747, 747 (2004).

8. Uncertainty, vulnerability, and a lack of trust in market interactions can be solved with long

handled in the market by other actors. Accordingly, privacy regulators and scholars attempt to facilitate trust within the relationship between individuals and firms.[9]

However, the focus on fixing the relationship between consumers and specific firms does not capture how the online environment behaves.[10] The majority of the work done in the online ecosystem of consumer data is done by market actors with no relationship with the consumer. Data brokers aggregate consumer data from different sources and sell information to firms who then use the information when it is not in a consumer's interest.[11] These data traffickers "do not have a relationship with either individual users whose information they possess or with major platforms," and "there is no contractual relationship between the data traffickers and the individuals with profiles in their databases."[12] Figure 1 depicts one vision of the anonymous online ecosystem of actors involved in consumer data. Such tracking is pervasive: on average, 25 third-party trackers are found on news, arts, and sports websites.[13] In fact, data traffickers—to include those

---

term, committed relationships in order to avoid "costly hierarchy." Sergio G. Lazzarini et al., *Dealing with the Paradox of Embeddedness: The Role of Contracts and Trust in Facilitating Movement out of Committed Relationships*, 19 ORG. SCI. 709, 710 (2008). *See generally* Peter Kollock, *The Emergence of Exchange Structures: An Experimental Study of Uncertainty, Commitment, and Trust*, 100 AM. J. SOC. 313 (1994); Ranjay Gulati, *Does Familiarity Breed Trust? The Implications of Repeated Ties for Contractual Choice in Alliances*, 38 ACAD. MGMT. J. 85 (1995).

9. And I have argued to fix the immediate relationship between user and firm in regards to privacy online, but here I argue such fixes are not enough. Kirsten Martin, *Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online*, 18 FIRST MONDAY 12 (2013).

10. One issue with focusing on transactions or relationships that is not covered here is that we miss systemic problems such as pollution, or where the harms fall on those outside the immediate (even trusted) relationship. For example, Peppet notes the third-party impact of disclosing information: "consumers may receive a discount for using a driving or health monitor, privacy may unravel as those who refuse to disclose are assumed to be withholding negative information and therefore stigmatized and penalized." Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U. L. REV. 1153, 1156 (2011). Lyon discusses the cumulative impact of a surveillance society. DAVID LYON, THEORIZING SURVEILLANCE 12 (2006). Ryan Calo notes the difficult of citizens to perceive and affect surveillance. Ryan Calo, *Can Americans Resist Surveillance*, 83 U. CHI. L. REV. 23, 23–24 (2016); Citron and Gray as well as Cohen summarize the generalized perception of society from the individual decisions to be surveilled; harms that are not captured in the individual exchanges. Danielle Keats Citron & David C Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 265 (2013); Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 183–84 (2008). Both Fromkin and Martin separately take this one step further by likening the cumulative harm from surveillance to pollution. A. Michael Froomkin, *Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements*, 2015 U. ILL. L. REV. 1713, 1715 (2015); Kirsten Martin, *Ethical Issues in the Big Data Industry*, 14 MIS Q. EXECUTIVE 67, 69 (2015).

11. TEDx Talks, *Why Companies Should Respect Our Privacy | Kirsten Martin | TEDx Charlottesville*, YOUTUBE (Feb. 14, 2018), https://www.youtube.com/watch?v=6iWINQiRQ9g.

12. The term "data trafficker" is from Professor Lauren Scholz. Lauren Henry Scholz, *Privacy Remedies*, 94 IND. L.J. (forthcoming 2019), https://ssrn.com/abstract=3159746.

13. STEVEN ENGLEHARDT & ARVIND NARAYANAN, ONLINE TRACKING: A 1-MILLION-SITE

trafficking in the consumer data behind the scenes—are the market actors who make money under the current regime.[14]

While we currently focus on optimizing interpersonal trust online as if we are in a market of local dry cleaners, consumers are facing a confusing market more akin to the medical system or financial securities, with many anonymous actors working behind the scenes to create the experience and deliver the service. In such a situation, generalized trust in the institution matters more because individuals cannot gain evidence of trustworthiness of specific individuals or firms.[15] In other words, when information is not available about firms or the quality of the product, we rely upon *institutional trust* to uphold norms and quality standards.[16] Institutional trust means the threat of opportunism of one firm does not matter as much because we trust the system to take care of bad actors.[17]

MEASUREMENT AND ANALYSIS 6 (May 18, 2016) 6, http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf.

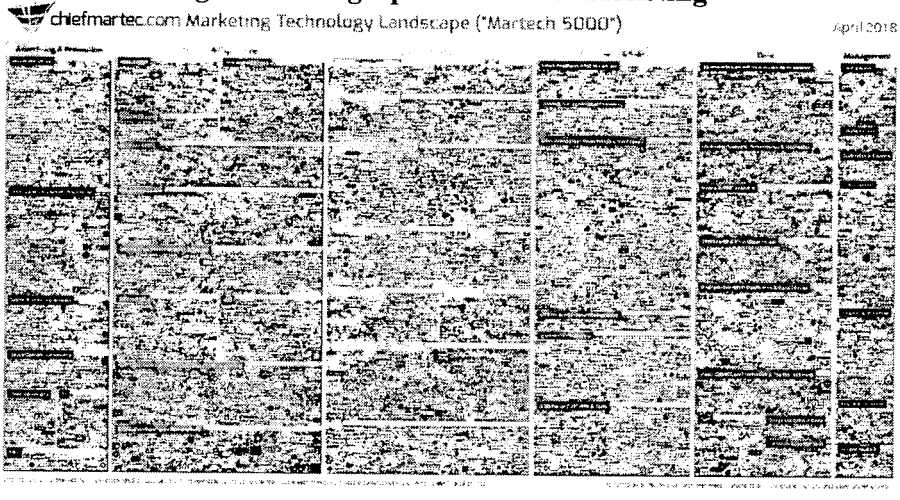
14. Sarah Spiekermann et al., *The Challenges of Personal Data Markets and Privacy*, 25 ELECTRON MARKETS 161, 161 (2015); Max Read, *How Much of the Internet Is Fake? Turns Out, a Lot of It, Actually.*, NEW YORK MAGAZINE, Dec. 26, 2018, http://nymag.com/intelligencer/2018/12/how-much-of-the-internet-is-fake.html.

15. "In the absence of previous relationships, the trustworthiness of a potential trustee primarily depends on two factors: the image of intermediaries that the trustor relies on for obtaining information about trustees . . . and/or the trustworthiness of institutions that back up trustees." Dmitry Khodyakov, *Trust as a Process: A Three-Dimensional Approach*, 41 SOC. 115, 122 (2007). *See also* T. Yamagishi, *Trust as a Form of Social Intelligence*, *in* TRUST IN SOCIETY 121–48 (K. Cook ed., 2001).

16. Trust can be at multiple levels: (1) trust disposition of an individual or a general tendency to trust; (2) interpersonal trust tied to person or market actor, based on social characteristics such as the trustworthiness of the trustee; and (3) a more generalized trust such as "institutional" trust, tied to formal societal structures, based on individual or firm-specific attributes or on intermediary mechanisms. Michael Pirson et al., *Public Trust in Business and its Determinants* 8–9 (Fordham Univ. Schools of Bus. Working Paper No. 2012-002); *see* Lynne G Zucker, *Production of Trust: Institutional Sources of Economic Structure*, 8 RES. ORG. BEHAV. 53 (1986) (Professor Zucker focuses on trust in institutions rising in the U.S. with the spread of credentialing, a shift to service (rather than products), as well as regulation and legislation).

17. Oliver E Williamson, *Opportunism and Its Critics*, 14 MANAGERIAL AND DECISION ECON. 97, 97 107 (1993).

Figure 1: Infographic of online marketing[18]



Institutional trust is not a unique phenomenon.[19] When dealing with strangers, people still become vulnerable to others: "They walk into an unfamiliar branch office of their bank or into a hospital emergency room."[20] Such institutional trust is regularly measured in larger systems with information asymmetries such as with banks, newspapers, congress, big business[21] or in law and medicine.[22] And privacy online has all the markers of a system that would rely upon institutional trust with anonymous actors outside the reach of consumers and information asymmetries wherein the consumer is the least informed.

We treat interactions online as a series of exchanges with specific firms and justify tracking, sharing, aggregating, and using consumer information as within a *reciprocal exchange* between two parties. However, the aggregation and secondary use of consumer data, the subject of much concern, is performed by market actors behind the scenes without any relationship with consumers. A *generalized exchange*, where the benefits

18. Scott Brinker, MARKETING TECHNOLOGY LANDSCAPE SUPERGRAPHIC (2018): MARTECH 5000 (ACTUALLY 6,829) CHIEF MARTEC (2018), https://chiefmartec.com/2018/04/marketing-technology-landscape-supergraphic-2018/ (last visited Feb. 21, 2019).

19. *See generally* Pauline Ratnasingam et al., *The Role of Facilitating Conditions and Institutional Trust in Electronic Marketplaces*, 3 J. OF ELECTRONIC COM. ORG. 69 (2005); *See also* D Harrison McKnight et al., *Initial Trust Formation in New Organizational Relationships*, 23 ACAD. MGMT. REV. 473 (1998); Susan P Shapiro, *The Social Control of Impersonal Trust*, 93 AM. J. SOC. 623 (1987); Zucker, *supra* note 16.

20. Shapiro, *supra* note 19, at 635.

21. Betsey Stevenson & Justin Wolfers, *Trust in Public Institutions over the Business Cycle*, 101 AM. ECON. REV. 281, 281–87 (2011).

22. Mark A. Hall, *Law, Medicine, and Trust*, 55 STAN. L. REV. 463, 463–527 (2002).

received are not directly related to the transaction but rather are for the good of the online institution, may offer a better explanation of consumer exchange online.[23] A generalized exchange would suggest that consumers would approve uses of information that benefit a larger community or where the purpose and benefits are just—similar to the justification in other institutions with anonymous actors such as medical and financial systems.

Little has been done to measure how aggregating and using consumer data supports a larger online market and impacts the institutional trust online. This paper explores how privacy governance should be framed as protecting a larger market or institution. I position maximizing institutional trust as a natural extension of work in regulating privacy. In a series of studies, I then examine (a) whether secondary uses of consumer information are deemed appropriate within a generalized exchange online, (b) how uses along a generalized versus reciprocal exchange impact institutional and consumer trust, and (c) whether governance mechanisms (limitations on the use of data such as adequate notice, auditing, non-identifiable information, limited storage, etc.) increase consumer trust in companies using consumer data. I use three empirical studies:

1. I categorized uses of consumer data by the degree the use is perceived to be within a reciprocal exchange (benefit immediate actors) and general exchange (within furtherance of the institution).
2. Using a factorial vignette survey based on secondary uses identified in Study 1, I examined how different governance mechanisms help increase the consumer trust for each use for both legally mandated governance and market demanded governance. The goal is to identify what actions data brokers or data aggregators can take to use the information while not damaging consumer trust.
3. Finally, I ran an experiment to test if institutional trust—which is negatively impacted by the secondary use of data—impacts consumer economic behavior and willingness to engage online.

23. Within a generalized exchange, members contribute resources (e.g., information) and receive benefits of the pooled resources. Nobuyuki Takahashi, *The Emergence of Generalized Exchange*, 105 AM. J. SOC. 1105, 1105–34 (2000).

I found:

- Respondents find secondary uses of consumer data more appropriate if within a generalized exchange (academic research) or within a reciprocal exchange (product search results) or both (credit security). Secondary use of information can be justified outside a simple quid pro quo reciprocal exchange with the consumer. Most uses studied here are lower on both scales than using data to place ads—the standard bearer justifying secondary use of data online.
- While firms that use consumer data within a generalized or reciprocal exchange are trusted more than firms who use data to place ads, overall the secondary uses of consumer data decrease institutional trust online.
- A specialized data broker focused on a limited number of uses of information reinforces the trustworthiness of firms using data within a generalized exchange.
- Using privacy notices is the least effective governance mechanisms of those included here whereas being subject to an audit was as effective as using only non-personally identifiable information (non-PII) in improving trust. By being subject to an audit, data brokers were still deemed trustworthy even when storing information for a year.
- Secondary uses within a generalized exchange (e.g., credit security or academic research) rather than outside any generalized exchange (marketing) impacts trust more than any governance mechanism such as changing from notice to an audit. In other words, secondary use is more important to trust than any attempts to govern the information flow.
- Governance mechanisms based on market demands versus legal mandates are equally effective to engender trust.
- Institutional trust online impacts a consumer's willingness to engage with a specific online partner in a trust game experiment as well as amplifying the effectiveness of auditing as an effective governance mechanism to increase consumer trust.

The findings have implications for public policy and practice. The flow of information online—the sharing, aggregation, and use of consumer data—need not only be justified in a simple quid-pro-quo exchange with the

consumer but could also be justified as necessary or appropriate for the online market within a generalized exchange. This opens up additional legitimate flows of information for firms and places less pressure on firms to justify why the collection of information is benefiting the consumer specifically. However, the majority of the twenty-seven secondary uses studied here cannot be justified as within a general exchange (benefiting the broader community) or a reciprocal exchange (benefiting the consumer directly). And, uses of information that are not beneficial to the individual or necessary for the market or context were still judged inappropriate, violations of privacy, and as decreasing both interpersonal and institutional trust. The findings suggest a typology to identify what types of secondary uses of information are judged appropriate by consumers.

Second, and perhaps most importantly, this paper offers an additional mechanism for regulating privacy to maintain institutional trust online. The online environment has the markers of a market where generalized institutional trust is important to market actors. If privacy violations hurt not only interpersonal trust between a consumer and a firm but also institutional trust online in general, then privacy would be governed similar to insider trading, fraud, or bribery to protect the integrity of the market rather than only an individual. Punishment for a privacy violation would be set to ensure bad behavior is curtailed and institutional trust is maintained rather than to remediate a specific harm to an individual.

I. REGULATING PRIVACY AND TRUST

While the study of privacy governance has focused on different sectors, the types of records to be protected, or as within civil versus criminal courts,[24] more recently, Professors Woodrow Hartzog and Neil Richards have taken a step back to examine how privacy governance can be justified either by negative or positive duties. Do market actors have an obligation to 'do no harm' or do market actors have a positive obligation to foster trust?[25] Within this shift to frame privacy regulations as seeking to foster a positive outcome, the governance of privacy can also be seen as having different goals, or at different levels of analysis: (a) as protecting the individual, (b) as protecting relationships or transactions, or (c) as protecting a larger market or institution. I explore each below to understand how this shift to understand the role of privacy governance in support of the institution fits within existing work on regulating privacy and trust.

The different layers of privacy law should be seen as parallel to the layers of governance in medical, financial, and cybersecurity sectors as shown in Table 1. Importantly, each layer or type of governance complements the others to achieve a regulatory goal and govern bad behavior in the market.

---

24. See also the general balkanization of privacy laws into types such as government records, financial data, consumer data, health, etc. Daniel J. Solove & Paul M. Schwartz, *An Overview of Privacy Law*, *in* PRIVACY LAW FUNDAMENTALS 1–29 (2015).

25. Hartzog and Richards see two bodies of privacy law: torts and FIPS, which they frame as the 'harm' principle and 'control' principle, and see both as oriented in negative terms, with the implication that "privacy is almost always a negative and costly concept, a harm to be avoided, or a consent to be obtained before something positive can happen." Neil M Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 437 (2016). Richards and Hartzog state, "[i]nstead of trying to protect us against bad things, privacy rules can be used to create good things, like trust. In this paper, we argue that privacy can and should be thought of as enabling trust in our essential information relationships." *Id.* at 431.

Table 1: Governing for Individual Rights, Efficient Relationships, Institutional Trust

	Individual Rights/Harm	**Relationships**	**Institution**
Medical	Liberty, right to bodily integrity, pursuit of health	Doctor-patient	Conflict of Interest, HIPAA, Professionalization, Hospital standards
Financial	Property rights	Investor-Broker Consumer-Bank	FDIC, Insider trading, conflict of Interest, professionalization
Privacy	Torts, Privacy harms, Surveillance, revenge porn laws, right to technological due process. Right to autonomy	Consumer-Firm (FTC) Privacy as Confidentiality	***Focus of This Paper*** As well as calls for Consumer Review Boards, the professionalization of data scientist, or minimum privacy standards
Cybersecurity	Right to Information (GDPR) Credit Reporting Rights	Firm-Consumer (FTC) Firm-Shareholder (SEC)	Duties to report to other firms to protect the market.

A. Regulating Privacy to Protect Individual Rights

Many arguments for privacy governance focus on the impact on the individual; laws protect individuals from harm of the misuse of personal information[26] and the desire to find protective rights.[27] Individuals have a right to the information that describes them whether in credit reporting or generally.[28] Similarly, Professor Danielle Citron identifies a series of

26. Individuals also have a right to be protected from what Ryan Calo calls privacy harms. Privacy harms can be objectively measured or more subjective similar to assault or unwanted observation. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133 (2011).

27. Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 878 (2002). *See generally* Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141 (2014).

28. Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623, 1623 (2013); Chris Jay Hoofnagle, *How the Fair Credit Reporting Act Regulates Big Data*, FUTURE OF PRIVACY

individual rights such as to technological due process,[29] to cyber civil rights,[30] to protection from revenge porn,[31] and to the protection from hate crimes online.[32] As Professor Ari Waldman rightly identifies, a line of court cases such as *Griswold v. Connecticut*, *Roe v. Wade*, and *Lawrence v. Texas* protect individuals from societal intrusion. The protection of the individual can be both negative, where an individuals' private sphere is a place of freedom *from* something,[33] as well as positive, where privacy is for an "opportunity to grow, develop, and realize our full potential as free persons."[34]

The justification for such privacy governance is to protect the individual versus the world and are similar to regulations of property rights as the underpinning of the financial markets or a foundational right to autonomy in medicine as depicted in Table 1.

B. Regulating Privacy to Protect Relationships

A second layer of privacy governance seeks to protect relationships or transactions between market actors. Individuals share information with others, such as friends, doctors, lawyers, and companies, and privacy rules expand to govern the disclosure of information within relationships. Rather than focusing on the individual, these governance approaches seek to ensure the relationship between parities respect the privacy of both and is sustainable.

First, the FTC's notice and choice regime attempts to maximize choice and trust between market actors.[35] In the United States, the FTC focuses on a firm providing adequate notice of their privacy practices in order to facilitate informed consumers making a choice in the market. Fixes to the FTC's reliance on notice and choice to govern the relationship between

---

FORUM WORKSHOP ON BIG DATA AND PRIVACY: MAKING ENDS MEET 3 (2013); Guide to the General Data Protection Regulation (GDPR), INFORMATION COMMISSIONER'S OFFICE (2016), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (last visited Feb. 22, 2019).

29. *See generally* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008).

30. *See generally* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009).

31. *See generally* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014).

32. *See generally* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014).

33. Waldman, *supra* note 6, at 562.

34. *Id.*

35. The Federal Trade Commission (FTC) has been enforcing companies' privacy policies through its authority to police unfair and deceptive trade practices. CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 145 (2016); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 583 (2014).

firms and consumers, such as adding a duty of discretion, an obligation of honesty, and a duty of protection and adding loyalty as an important concept,[36] still focus on fine-tuning the relationship between data subject and the firm.[37]

Similarly, but outside the focus on notice and consent, is the call for better contracting between firms and individuals in regards to privacy. As I have pointed out, we may desire a market of simple exchanges with online privacy, "where information is known, enforcement is possible, and uncertainty is minimal." However, the current online environment is one where identity and reputation matter and credible contracting between market actors is necessary.[38] Importantly, the approach is to optimize the relationship between market actors.

More recently, Waldman explicitly makes the transition to protect relationships of trust rather than protect a collection of individual rights.[39] Similarly, Richards and Hartzog "argue that privacy can and should be thought of as enabling trust in our essential information relationships."[40] Professors Waldman, Richards, and Hartzog, make two shifts: first, to protect relationships and, second, to move from a negative right to not be harmed to a more positive right to be in a relationship of trust.

This focus on governing privacy within a relationship is similar to the layer of regulations and rules governing the doctor-patient relationship in medicine or the investor-broker relationship in finance in Table 1. The aim is to ensure the relationship is based on trust and is sustainable.

---

36. Richards & Hartzog, *supra* note 25, at 459–71.

37. Previous issues with FIPS center on the ability of consumers to (mistakenly) sell their 'privacy' too easily and too cheaply. A. Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461, 1461–1543 (2000). The reliance on notification to communicate the terms of an exchange is problematic, since notices are hard to find, misleading and misinterpreted, and time consuming. Pedro Giovanni Leon et al., *What Do Online Behavioral Advertising Privacy Disclosures Communicate to Users?*, PROC. OF THE 2012 ACM WORKSHOP ON PRIVACY IN THE ELECTRONIC SOC. 19 (2012); Kirsten Martin, *Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online*, 34 J. PUB. POL'Y & MARKETING 210, 220 (2015); Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP 543, 544 (2008).

38. Martin, *supra* note 9.

39. Waldman sees breaches of privacy as a breach of trust. "To this end, this Article proposes a robust tort for breach of confidentiality as one tool to protect privacy in a networked world and illustrates the functionality of this tort through a case study of privacy in previously disclosed information. Waldman, *supra* note 6, at 560.

40. Solutions, correctly, are framed as increasing trust in information relationships through duties of discretion, honesty, and protection. And "modern privacy law is incomplete because from its inception it has failed to account for the importance of trust . . . . Trust in information relationships is necessary for the digital economy not just to function, but to flourish." Richards & Hartzog, *supra* note 25, at 435.

C. Regulating Privacy for Institutional Trust

An under-examined area for privacy governance is at the market or institutional level. We treat interactions online as a series of exchanges with specific firms. Privacy, accordingly, is governed to ensure trust within those relationships. The focus on governing relationships can miss systemic harms and externalities not covered within an immediate transaction. For example, the collection, aggregation, and use of consumer data can create a perception of general surveillance, where individuals feel they are being watched even when they are not.[41] Here we focus on how the possible bad acts of some decrease the institutional trust in general online. Systemic harms—such as the harm to institutional trust—is not captured when focused on a single relationship.

Institutional trust focuses on procedural norms and structural constraints as enforcing good behavior rather than an individual or firm's trustworthiness.[42] Online, institutional trust captures the belief that there are impersonal structures that enable a consumer to act in anticipation of successful future endeavors even without clear trust signals from specific firms.[43] With institutional trust, market actors rely on the system to take care of bad acts and untrustworthy behavior and to foster integrity in the market. Importantly, the aggregation and secondary use of consumer data, the subject of much concern, is performed by market actors behind the scenes without any relationship with consumers. Individuals therefore must trust 'being online' in general.

Institutional trust is important to allow individuals to enter new markets and form new relationships rather than remain with current (perhaps less valuable) relationships. In other words, trust in the institution relieves some of the pressure to find trustworthy signals in individual firms.[44] For example, in the financial industry, "if investors believe that the stock market

---

41. Martin, *supra* note 10, at 77.

42. Susan P. Shapiro, *The Social Control of Impersonal Trust*, AM. J. SOC. 623, 636 (1987).

43. Ratnasingam et al., *supra* note 19, at 70. Ratnasingam, Gefen, and Pavlou propose four facilitating conditions to institutional trust online: (1) IT connectivity, (2) standards, (3) security, and (4) uniform product descriptions. Privacy was not included at the time. *Id.*

44.

> Two mechanisms may encourage movement out of committed relationships in those conditions. First, formal contracts should serve as a safeguard to market participants, in the sense that they limit potential losses due to opportunistic behavior. Second, trust in general others (as opposed to trust in familiar people) reduces participants' perception of hazards in market exchanges and hence promotes transactions among strangers. By increasing the propensity to initiate new exchanges, general trust also diminishes the role of contracts in causing movement out of committed relationships.

Lazzarini et al., *supra* note 8, at 709.

is systematically unfair and accords advantages to insiders and others with superior access to material nonpublic information, then investors may exit the market, to the detriment of the marketplace and society generally."[45] Therefore insider trading, which is difficult to govern as a harm to an individual,[46] is governed to maintain institutional trust and the integrity of the securities market. In fact, Professor Laura Beny found insider trading laws impact ownership dispersion and that sanctions on insider trading impact the dispersion of ownership for top ten companies in the economy: "large public corporations tend to have greater ownership dispersion in countries whose formal insider trading laws contain greater sanctions for insider trading violations."[47] When individuals trust the system to take care of bad actors, more individuals enter the market.

Importantly, when institutional trust matters, or when individuals need to believe the norms and structures will work to identify and punish bad actors and reward good behavior, then violations need not be justified by quantifying harm to an individual or a firm. Instead, crimes such as bribery, fraud, insider trading, and corruption are punished to maintain the integrity of the market and institutional trust.

D. Research Implications

The shift to include the online institution as an important level of analysis for privacy governance has two important implications.

First, the governance of privacy online has focused on the immediate relationship between the consumer and what I call the gatekeeper firm.[48] Whether or not a consumer approves of the collection of their data online is seen as an exchange where consumers provide information and are provided benefits by a firm: free online content, targeted ads, better search results, tailored services, etc. And, the sharing, aggregation, and use of consumer data post-disclosure is justified as fitting within a reciprocal, quid-pro-quo exchange with consumers.

However, if the online institution is an operative level of analysis to govern, then a generalized exchange, where the benefits received are not

---

45. Kimberly D. Krawiec, *Fairness, Efficiency, and Insider Trading: Deconstructing the Coin to the Realm in the Information Age*, 95 NW. U. L. REV. 443, 470 (2000).

46Alternatively, insider trading laws are justified to make transaction efficient or minimize investor harm. Nicholas L. Georgakopoulos, *Insider Trading as a Transactional Cost: A Market Microstructure Justification and Optimization of Insider Trading Regulation*, 26 CONN. L. REV. 1, 1 (1993).

47. Laura Nyantung Beny, *Do Insider Trading Laws Matter? Some Preliminary Comparative Evidence*, 7 AM. L. & ECON. REV. 144, 166 (2005).

48. Kirsten Martin, *Data Aggregators, Consumer Data, and Responsibility Online: Who Is Tracking Consumers Online and Should They Stop?*, 32 THE INFO. SOC'Y 51, 51–63 (2016).

directly related to the transaction but rather are for the good of the online institution, may offer a better explanation of consumer exchange online.[49] A generalized exchange would suggest that consumers would approve uses of information that benefit a larger online community or where the purpose and benefits are just. For example, people fill out the U.S. Census when the use of the data to benefit society is explained—and not when the benefit to their immediate community is emphasized. Similar rationales are used to explain contributions to philanthropy, intergenerational exchanges, medical research, and consumer credit. A generalized exchange would also be consistent with privacy as the appropriate flow of information[50] or privacy as a social contract[51]: privacy violations occur when the flow of information is outside a given context or violates the norms of the community.

Within this framing, the consequences of market actors—both harms and benefits—are assessed within a larger institution. Does the collection and use of data hurt or benefit the online institution? Is the information flow appropriate for the general context?[52] This shift to focus on the larger institution—and the role of privacy with institutional trust online—is in keeping with approaches to privacy that broaden the focus from disclosure to an individual to information flows within a larger community, context, system, or society.[53]

Below, I empirically examine (a) whether secondary uses of consumer information are deemed appropriate along a generalized exchange online, (b) how uses within a generalized versus reciprocal (quid-pro-quo) exchange impact institutional and consumer trust, and (c) whether governance mechanisms (limitations on the use of data such as adequate notice, auditing, non-identifiable information, limited storage, etc.) increase consumer trust in companies using consumer data.

---

49. Within a generalized exchange, members contribute resources (e.g., information) and receive benefits of the pooled resources. Takahashi, *supra* note 23, at 1128.

50. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 127 (2010).

51. Kirsten Martin, *Understanding Privacy Online: Development of a Social Contract Approach to Privacy*, 137 J. BUS. ETHICS 551, 554–55 (2016).

52. Nissenbaum, *supra* note 50, at 127.

53. For example, Nissenbaum explicitly focuses on the context as the operative focus to understand if the flow of information is deemed appropriate whereas Martin focuses on the social contract community as determining privacy norms. *See generally* NISSENBAUM, *supra* note 50; Martin, *supra* note 51. Bambauer notes the flow and not just the handoff, explaining that "[p]ersonal information passes through four distinct states where regulation can apply: observation, capture (when a record is created), dissemination, and use." Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 209 (2012). Strahilevitz broadens the examination to an individuals' social network. *See generally* Lior J. Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005). Much of surveillance scholarship also moves away from trust in a single actor towards the decisions of a larger community or society. Calo, *supra* note 10; Cohen, *supra* note 10, at 183; Priscilla M. Regan, *Response to Bennett: Also in Defence of Privacy*, 8 SURVEILLANCE & SOC'Y 497, 497 (2011).

II. STUDY 1: SECONDARY USES OF CONSUMER INFORMATION

In order to categorize the secondary uses of information as along two axes—as along a generalized exchange and along a reciprocal exchange—I first identified a range of uses from marketing materials, government reports, academic research, and privacy reports. These uses can be categorized into 6 areas: product/marketing, risk assessment, fraud/security, research, people search, and political action. Table 2 contains the possible uses of consumer data as operationalized in this survey.

A. Design Study 1

After a series of control questions (gender, age, trust online, privacy concerns), a traditional survey was run where respondents were asked to rate either (A) if the use was appropriate, (B) if the use was within a reciprocal exchange (benefit the user directly), and (C) if the use was within a generalized exchange (benefit a larger community). The secondary use (bolded portion) was randomly assigned 30 times for each respondent as listed in Table 2.

> Prompt: For each possible use, a data broker has gathered your general information from browsing habits online, purchasing history (automobiles owned), hobbies and interests online, offline activity such as grocery purchases, and even type of contacts you have from social networking sites to build a profile.
>
> The data broker would use the information (browsing history, search results, purchases) **to be accessible to companies conducting research to improve technical performance online.**

The respondent was assigned to one of three conditions. This rating used a slider and recorded a continuous rating (-100 to +100) for each.

1. Appropriate Use
   Please rate the degree to which this use is appropriate.
   Not Appropriate — Appropriate

2. Reciprocal Exchange
   Please rate the degree you believe this use of information would benefit you directly.
   Does Not Benefit Me — Benefits Me

3. General Exchange
   Please rate the degree you believe this use of data benefits a larger community.
   Does not benefit community — Benefits Community

Table 2: Appropriate Use of Information Categorized

Category of Use		As Operationalized in Survey
Product/Marketing		
Ads	Ad	to determine which ad to place when you are online
	Personalize	to personalize an ad for product you've searched for
Product Offering	FinProd	to determine the type of financial product (bank account, savings plan) you will be offered
	ConsProd	to determine the search results when you are looking for an item at an online retail store.
Lead generation	LeadGenUniv	to generate a list of potential customers to contact for a for-profit university
Investment advice	CustInvestAdv	to customize investment advice by a bank
Risk Assessment		
Insurance	AutoIns	to assess your risk for car insurance coverage
	HealthIns	to determine your rate and coverage for health insurance
Loan/Financing	TVLoan	to assess your risk profile for financing a large TV.
	CarLoan	to assess your risk profile for a car loan.
Employment	JobApp	to screen job applicants
Housing	Rent	to assess your risk profile for a possible apartment rental
Fraud		
	Credit card	for fraud prevention by your credit card company
	IDCheck	to verify your identity when filling out applications
	Financing	to verify your identity when applying for financing
Security		
	CyberSec	to look for patterns of use of hackers who are potential threats to cyber security by a private company
	CyberSecGovt	to look for patterns of use of hackers who are to cyber security by the government
Research		
Academic	AcadRsrch	to be accessible to academic researchers conducting studies on individual behavior
Private Firm	ProdImpr	to be accessible to companies conducting research to improve product delivery online
	TechImpr	to be accessible to companies conducting research to improve technical performance online
Public Interest	EducRsrch	to be accessible to academic researchers conducting studies on consumer behavior
	GovtImpr	to be accessible for governments looking to improve services in their local area
People Search		
	Admissions	for university admissions to gain a more fine-grained profile of applicants.
	FindPpl	for people or organizations to be able to locate you for future contact
	Employment	for potential employers to gain a more fine-grained profile of applicants.
	Law	for law enforcement to investigate possible suspects or investigate a crime generally.
Political Action		
Fundraising	PolFund	to identify people for political fundraising
Information	PolInfo	to identify people possibly interested in mailings about a politician

B. Results Study 1

The results for the traditional survey—where the respondents rated the degree to which the use of the information by the data broker was appropriate, within a generalized exchange, or within a reciprocal exchange—are in Table 3. The average rating the secondary use was appropriate was -21.12, suggesting consumers on average do not find the secondary use by data brokers to be appropriate.

Table 3: Sample Descriptive Statistics for Study 1

	Rating = Appropriate Use Survey 1	Rating = Reciprocal Use Survey 2	Rating = Generalized Use Survey 3
N	260	269	252
Ave Rating	-21.12	-15.60	-13.89
% Age Over 35	43%	41%	43%
% Male	50%	50%	51%

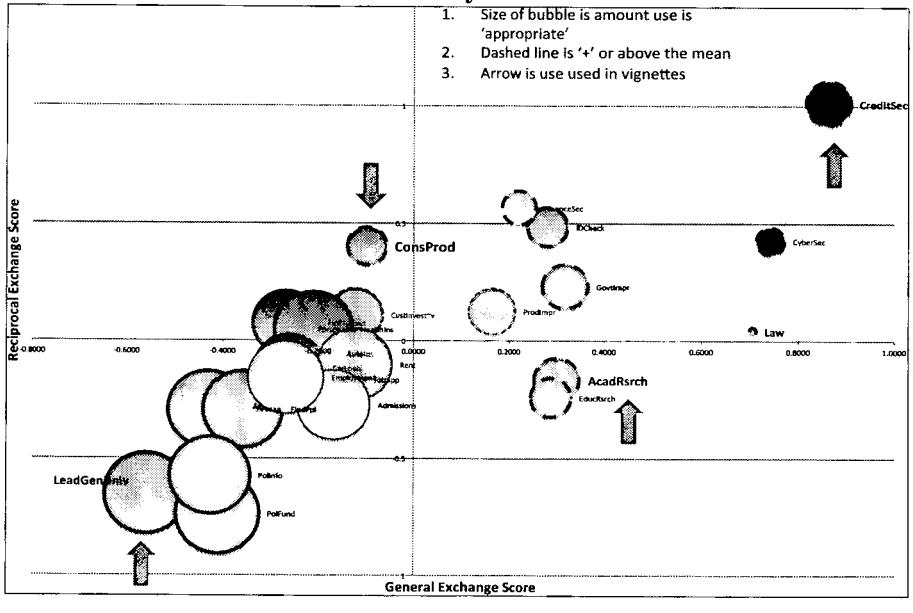
Figure 2 plots each secondary use by the average rating as within a generalized exchange (x-axis) and within a reciprocal exchange (y-axis). For example, credit security in the upper right quadrant, is judged to be relatively high within the generalized exchange (benefits the larger community) and reciprocal exchange (benefits you directly). Alternatively, using information for lead generation for a for-profit college is judged as outside both a generalized exchange and reciprocal exchange.

In order to increase the theoretical generalizability of the ratings for generalized exchange and reciprocal exchange, I standardized the ratings of generalized exchange and reciprocal exchange (*mean* = *0* and *s.d.* = *1*). The results are plotted in the bubble chart in Figure 2 with the size of the bubble equal to the degree the use is considered appropriate. The dotted line perimeter is above the average (ad placement is the average) where a solid perimeter is below the average. The size of the bubble remains the magnitude. As would be expected, uses with a higher score for generalized and reciprocal exchange were judged more appropriate (dotted outline of bubble—thicker as more positive). Secondary uses that were, on average, rated not within a generalized or reciprocal exchange were judged less appropriate (solid outline of bubble—thicker as more negative).

C. Discussion Study 1

Study 1 shows that respondents differentiate the secondary uses along the three dimensions—degree within a generalized or reciprocal exchange and the degree the use is appropriate. Further the results in Figure 2 offer theoretically interesting uses for the vignette survey in Study 2 (identified by the red arrows) in order to measure how each type of use (high and low ratings for generalized exchange and reciprocal exchange) impacts consumer trust. Study 1 illustrated that consumers differentiate the types of uses whereas Study 2 will measure if those differences matter to consumer trust and when taking into consideration possible governance policies such as limiting storage of information and including a review board or auditors.

Figure 2: Secondary uses of data plotted using standardized scores (*mean = 0* and *s.d. = 1*). Red arrows mark uses of information for Study 2.



III. STUDY 2: VIGNETTE STUDY ON USE OF DATA AND TRUST

Study 2 examines how secondary uses along a generalized versus reciprocal exchange (identified in Study 1) impact institutional and consumer trust. The goal is to identify what actions data brokers or data aggregators can take to use the information while not damaging consumer trust.

Study 2 seeks to answer three broad questions:

1. Is institutional trust impacted by the secondary use of consumer data?
2. Do different types of secondary use (high versus low generalized and reciprocal exchange) impact trust?
3. Do different governance policies on the use of data—limiting the storage, allowing data audits, etc.—impact trust in using consumer data?
    - Does changing from a broad-use to a specific-use data broker positively impact consumer trust in using data?
    - Does making the qualifications legally mandated versus a market demand impact consumer trust?

Using a factorial vignette survey based on secondary uses identified in Study 1, I examined how different *governance mechanisms* help increase the consumer trust for each use for both legally mandated governance and market demanded governance. Factorial vignette surveys support varying multiple contextual factors simultaneously while relying on a simple judgment for the rating task, namely, the degree to which the described data broker is trusted. Factorial vignette surveys present respondents with randomly generated vignettes in which experimentally designed factors—the independent variables—are systematically varied across the vignettes.[54] Respondents rated forty vignettes randomly created with replacement and were given the same rating task for all vignettes.

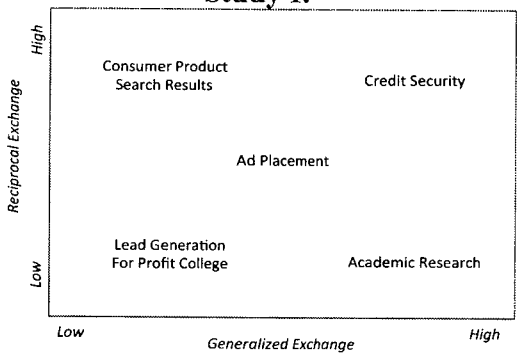
A. Design Study 2

1. Vignette Factors (Independent Variables in the Vignette)

a. Secondary Use. Five conceptually distinct secondary uses of information were chosen from Study 1 as depicted in Figure 3. Ad placement is both practically relevant and theoretically interesting as the use with the average score for appropriateness. I also chose a secondary use from each quadrant from the bubble chart in Figure 2 along the two axes—generalized and reciprocal exchange.

54. Guillermina Jasso, *Factorial Survey Methods for Studying Beliefs and Judgments*, 34 SOC. METHODS & RES. 334, 342 (2006).

Figure 3 – Uses of information for vignette study based on results of Study 1.



b. Governance Mechanisms. A range of protective measures for the consumer was included in order to identify which practices would positively impact consumer trust. Adequate notification[55] was included as well as a review board,[56] professional data scientist,[57] an auditor,[58] and non-PII.[59] Non-PII techniques were included to identify the how alternatives compared to the most 'protective' measure in theory—without any comment on the feasibility.

c. Storage. The duration the information was stored varied from one month to ten years to capture another protective measure.

2. *Vignette Design*

Template[60]:

A data broker collects consumer [Information] from online and offline sources for later use including [Secondary Use]. The

55. Florencia Marotta-Wurgler, *Does "Notice and Choice" Disclosure Regulation Work? An Empirical Study of Privacy Policies* (Univ. of Michigan Law & Econ. Research Paper Series, Working Paper No. 13, 2015), https://www.law.umich.edu/centersandprograms/lawandeconomics/workshops/Documents/Paper13.Marotta-Wurgler.Does%20Notice%20and%20Choice%20Disclosure%20Work.pdf; Kirsten Martin, *Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online*, 45 J. LEGAL STUD. 191, 192 (2016).

56. *See generally* Ryan Calo, *Consumer Subject Review Boards: A Thought Experiment*, 66 STAN. L. REV. ONLINE 97 (2013).

57. Martin, *supra* note 10, at 84.

58. Megan Gray, *Understanding and Improving Privacy "Audits" Under FTC Orders*, STANFORD CTR. FOR INTERNET & SOC'Y BLOG (April 2018), http://cyberlaw.stanford.edu/blog/2018/04/understanding-improving-privacy-audits-under-ftc-orders.

59. Arvind Narayanan & Vitaly Shmatikov, *Myths and Fallacies of "Personally Identifiable Information"*, 53 COMM. ACM 24, 24–26 (2010).

60. Information Type. Two information types were included: consumers' preferences and consumer purchases (this factor was not significant).

company stores the information to use for [Duration]. Based on recent regulations, the company also [Governance Mechanism].

Example:

A data broker collects consumer preferences (app use, browsing history, social network activities) from online and offline sources for later use including for fraud prevention by credit card companies.

The company stores the information to use for one month.

Based on recent regulations, the company also is audited by an accounting firm to ensure the use of data is consistent with stated goals.

Table 4: Vignette Factors for Study 2.

Vignette Factors		Operationalized in Vignette
Secondary Use	Credit Security	For fraud prevention by credit card companies/ fraud prevention
	Acad. Research	to support researchers conducting studies on individual behavior/ academic research
	Ad	to determine which ad to place when you are online/ marketing
	Consumer Product	to determine the search results when you are looking for an item at an online retail store/ retail support
	Lead Generation Univ	to generate a list of potential customers to contact for a for-profit university/ identifying potential customers
Governance Mechanisms	Non-identifiable	Summarizes the data so that it is not identifiable and can only make general predictions.
	Professionalization	Uses a data certified professional (similar to a CPA) on all data use projects
	Review Board	gets the approval of a review board before new analysis or uses of identifiable consumer data.
	Audited	Is audited by an accounting firm to ensure the use of data is consistent with stated goals.
	Notice	Explains how they gather and use of consumer data in a notice on their website.
Duration	Time	1 month, 6 months, 1 year, 2 years, 5 years, 10 years

3. *Rating Task*

The respondents rated their degree of trust in the data broker by scoring their agreement with the statement "I trust this data broker."

4. *2x2 Design*

Four factorial vignette surveys were run as depicted in Figure 4. First, the type of data broker was either a broad use data broker or a specific use data broker tied to the use assigned for that vignette. This captures any benefit to data brokers specializing in a type of use or a specific market. Second, the governance mechanism—notification, audit, non-PII, etc.—was either due to a legal mandate or a market demand. This captured whether market or non-market actions were more effective at engendering trust.[61]

Figure 4: 2x2 design of factorial vignette survey.

	Broad Data Broker	Specialized Data Broker
Legal	**A data broker** collects consumer [INFORMATION] from online and offline sources for later use including [SECONDARY USE]. The company stores the information to use for [DURATION]. **Based on recent regulations**, the company also. [QUALIFIER].	**A data broker that specializes in [USE]** collects consumer [INFORMATION] from online and offline sources – in order [SECONDARY USE]. The company stores the information to use for [DURATION]. **Based on recent regulations**, the company also [QUALIFIER].
Market	**A data broker** collects information from online and offline sources – such as [INFORMATION] -- in order to [SECONDARY USE]. Only keeps the information for xx months. **In order to remain competitive in their industry**, the company also. [QUALIFIER]	**A data broker that specializes in [USE]** collects information from online and offline sources – such as [INFORMATION] -- in order to [SECONDARY USE]. The company stores the information for xx months. **In order to remain competitive in their industry**, the company also. [QUALIFIER].

61. *See generally* Kollock, *supra* note 8.

Table 5: Sample Descriptive Statistics for Study 2 (also depicts order of questions)

Data Broker Requirement	Specific Legal Survey 1	Broad Legal Survey 2	Specific Market Survey 3	Broad Market Survey 4
N	476	510	482	520
% Male	53%	49%	58%	53%
% Age Over 35	46%	46%	43%	40%
Ave Rating (40 vignettes)	-4.6	-6.1	-3.1	-6.7
Trust Online (Base = +12.4)	-22.6	-20.5	-19.5	-21.3
Privacy Concern	54.9	57.1	53.9	54.7
Privacy Important	75.9	77.3	75.9	78.1

B. Results Study 2

1. Consumer Trust in a Firm

To test if the secondary use of data—as along a continuum of reciprocal and generalized exchange—impacts consumer trust, the trust rating task was regressed on the vignette factors and the results are in Table 6 for the specific use and broad use data broker. The results show that secondary uses of information that were rated as within a reciprocal exchange (*consumer product use* = $3.46, p<0.001$), generalized exchange (*academic research* = 20.42, $p<0.001$), or both (*credit security* = 24.89, $p<0.001$) positively impact trust compared to using information to place an ad. The secondary use that was rated as outside either a reciprocal and generalized exchange (lead generation for a for profit university) negatively impacts trust (-11.67, $p<0.001$) compared to using information to place an ad.

Table 6: Regression of consumer trust rating task on vignette factors

Regression Results	Specific Use Data Broker		Broad Use Data Broker	
	Coef	p	Coef	p
PurchaseInfo	0.00	0.99	-0.27	0.60
(Null = Preference)				
StorageTime	-5.05	0	-6.23	0
AcadRsrchUse	**20.42**	0	**13.53**	0
ConsProdUse	**3.46**	0	**6.42**	0
CreditSecUse	**24.89**	0	**19.17**	0
LeadGenUnivUse	**-11.67**	0	**-11.94**	0
(Null = Ad)				
AuditQual	9.67	0	6.85	0
NonIDQual	12.29	0	7.56	0
ProfessionQual	5.37	0	2.06	0.01
ReviewBrdQual	3.41	0	1.63	0.05
(Null = Notice)				
_cons	-3.03	0.091	3.36	0.06

2. *Governance Mechanisms*

a. *Specific Use versus Broad Use Data Brokers*

In addition, stating the data broker is targeted to a specific use amplifies the benefit of secondary uses within a generalized exchange as shown in Figure 5 (Credit Security Use $\chi 2 = 13.13, p<0.001$; Academic Research $\chi 2 = 18.31, p<0.001$). Secondary use within a generalized exchange (for the general benefit) is perceived as increasing trust—particularly if data broker is specialized.

All proposed governance mechanisms—using a review board, hiring a professional data scientist, storing only non-PII, being subject to an audit -- were an improvement to increasing trust compared to adequate notification (the current default governance mechanism in the U.S.). Figure 6 illustrates the relative importance of each governance mechanism to consumer trust compared to adequate notice. Using an auditor or anonymized data has a larger impact on trust when the data broker is specialized over a broad use data broker. Governance mechanisms are more impactful to consumer trust with a specific use data broker compared to a broad use data broker.

Figure 5: Types of Use: Generalized versus Reciprocal exchange

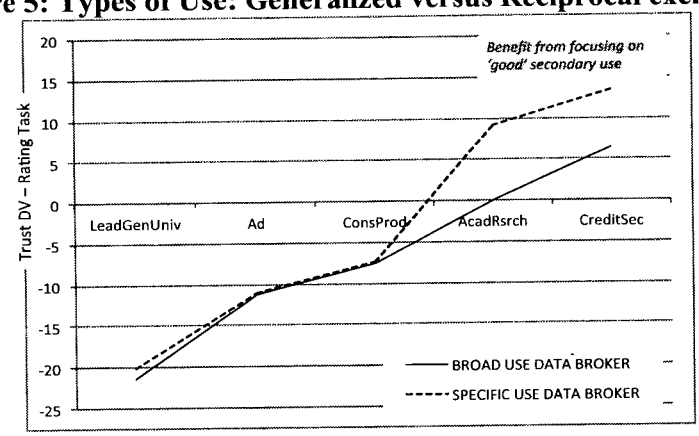
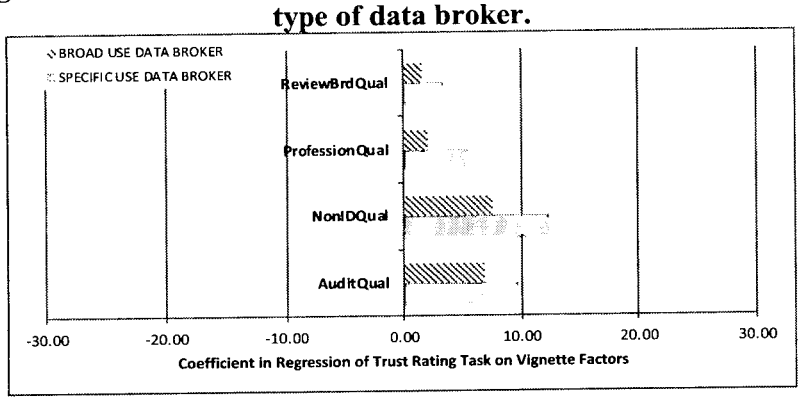


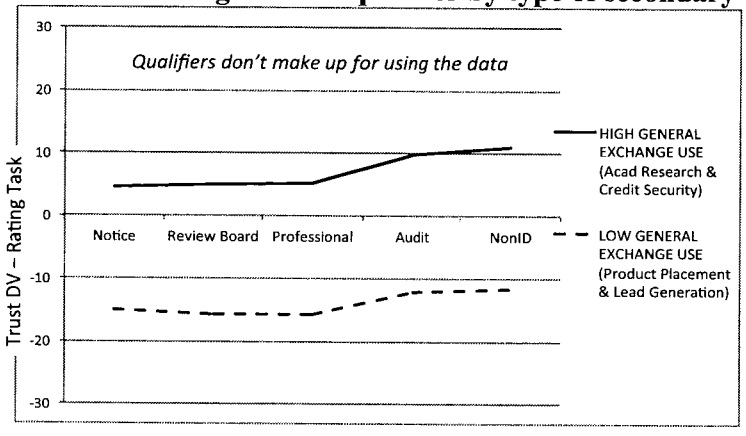
Figure 6: Coefficients of vignette factors – Use and Qualifiers – by type of data broker.



However, Figure 7 plots the average trust rating for each governance mechanism by high generalized exchange use (academic research or credit security) and low generalized exchange use (consumer product placement and lead generation). Figure 7 illustrates the (relatively) greater impact of the type of use compared to any change in the qualifier included. The impact on trust from a generalized exchange use (difference between solid and dashed line) is greater than any change in qualifiers (changes along a line). Specifically, the coefficient for high exchange uses (credit security and academic research) are significantly larger than the benefit of the top qualifiers (non-PII and auditor).[62]

62. The positive impact of using data for academic research is greater than the governance

Figure 7: Trust rating for each qualifier by type of secondary use.



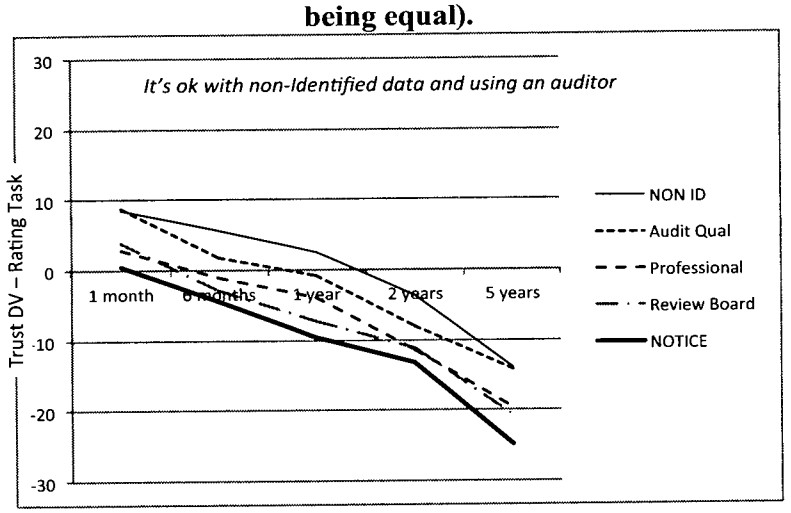
Previously, storage of consumer data has been judged inappropriate when measured in surveys with consumers deeming any storage more than a week to be a violation of trust or inappropriate.[63] To test how the different qualifiers may extend the amount of storage deemed to still be trustworthy behavior, the trust rating for each duration of storage by each qualifier is plotted in Figure 8. I find that using an auditor led consumers to still trust firms even if data is stored up to a year (all else being equal). NB using merely a notice replicates previous findings that almost any storage is not seen as trustworthy behavior.

Governance mechanisms are important but do not make up for the trust violating behavior of secondary uses of information outside a generalized exchange.

mechanism of being subject to an audit ($\chi 2 = 15.03, p<0.00$) or non-PII ($\chi 2 = 4.97, p<0.03$). Similarly, the positive impact of using data for credit security use is greater than the governance mechanism of being subject to an audit ($\chi 2 = 59.14, p<0.00$) or including only non-PII ($\chi 2 = 36.53, p<0.00$).

63. Martin, *supra* note 37; Martin, *supra* note 2.

Figure 8: Trust rating for storage duration by qualifier – using an auditor led consumers to still trust even if stored up to a year (all else being equal).



3. *Institutional Trust*

First, respondents' institutional trust online—the degree to which they agreed with the statement "[i]n general, I trust websites online"—was diminished with the mere description of secondary uses of consumer data. For each survey run as described in Table 5, the average trust online was -19.5 to -22.6 as compared to a null condition of +12.4 (when respondents are asked without having to judge the vignettes). The results illustrate that institutional trust is negatively impacted by secondary uses of data *when the consumers are merely informed about the use of data.* This could also be because the secondary uses of data were, on average, deemed not appropriate from Survey 1.

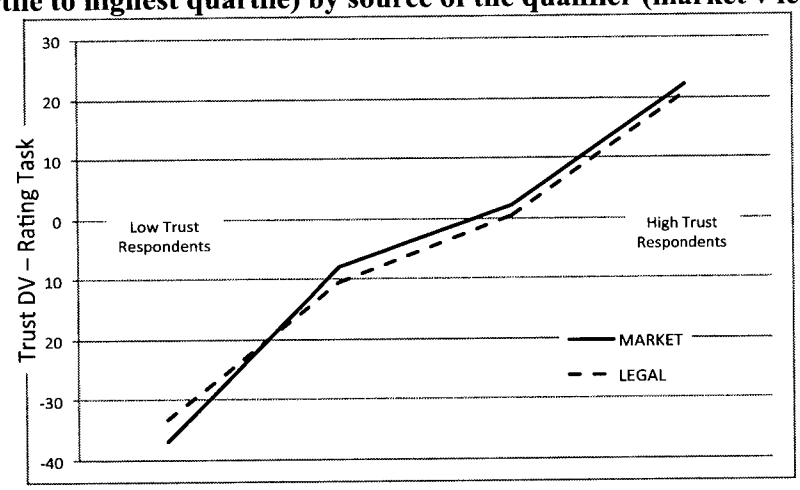
In addition, respondents' institutional trust in websites impacts the effectiveness of governance policies. To identify high- and low-trusting respondents, I split the sample into quartiles based on the rating of the institutional trust question. Respondents in the top 25% were categorized as high trusting and respondents in the lowest 25% were used in the analysis as low trusting respondents. Table 7 includes the coefficients for the regression of the trust rating task on the vignette factors for each subsample. Secondary use within the general exchange (benefiting the greater good) has a bigger impact on the trust rating for low trusting respondents. On the other hand, the introduction of low general exchange uses (e.g., lead generation) has a larger impact on trust of high trusting respondents.

Table 7: Coefficients for Secondary Use Factors (from Vignette) for High Trust (top 25% of respondents) and Low Trust (bottom 25%) Respondents

	High Trust Respondents N = 260	Low Trust Respondents N = 269	
Generalized Exch Use			
Academic Research Use	+9	+20	($\chi^2 = 28.14$, $p<0.00$)
Credit Security Use	+14	+26	($\chi^2 = 22.88$, $p<0.00$)
Reciprocal Exch Use			
Consumer Prod Use	+3	+4	($\chi^2 = 1.7$, $p=0.19$)
Lead Generation Univ Use	-15	-7	($\chi^2 = 19.31$, $p<0.00$)

In addition, the impact of using a legal mandate (the governance mechanism is through compliance to regulation) versus market demand (the qualifier is a competitive advantage) is tested by comparing the trust rating of scenarios across two distinct samples of the survey. The results show that respondents find no difference in trust if a qualifier is implemented in compliance with a regulation versus in response to competitive forces. Figure 9 illustrates the different trust ratings for low trusting and high trusting respondents (by quartile) for both market demanded and legally required qualifiers and the respondents did not differentiate the source of the qualification.

Figure 9: Trust rating for each type of trust respondents (lowest quartile to highest quartile) by source of the qualifier (market v legal).



C. Discussion Study 2

Typical secondary uses of information negatively impact both consumer trust in a firm and institutional trust online. However, justifying the flow of information based on benefits to the overall system holds promise. Secondary use within a generalized exchange has a significant positive impact on consumer trust; changing the type of secondary use to a generalized exchange has a larger impact on trust than any governance mechanism included. In terms of possible policies to govern data flows for trust, auditing was found to be a significant improvement on consumer trust compared to adequate notice. Finally, whether the governance mechanism is due to legal requirements or market demands does not impact trust, meaning an industry or market solution may be as effective as a regulatory protection.

IV. STUDY 3: EXPERIMENT

Study 1 measured whether respondents differentiated, and positively judged, secondary uses of consumer data within a generalized exchange versus a reciprocal exchange. Study 2 then tested the importance of those secondary uses of information to consumer trust while taking into consideration possible governance mechanisms—e.g., duration of storage, specialized data broker, auditing practices, etc. Study 3 now examines the importance of secondary uses of information, governance mechanisms (notice versus auditing), and institutional trust on the behavior of

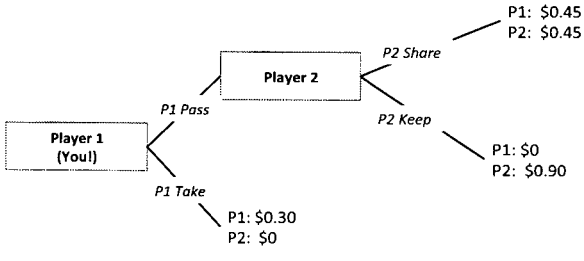
consumers.

In order to further test the finding that the secondary uses with a low generalized exchange score are a breach of consumer trust, I sought to measure the impact of secondary use of consumer data for marketing on the trust *behavior* or a consumer's willingness to engage. Here I utilized the "Trust Game" to measure trust in a firm.[64] The respondent is assigned to be one player (Player 1) and plays the game online with a 'website' (Player 2) designed with particular attributes. Player 1 must decide to become vulnerable to Player 2 by passing the initial amount of money and trusting Player 2 will share the proceeds back.

Participants were told they would play four rounds with the same partner, and each participant made four separate decisions. Each round of the scenario occurred in two stages as shown in Figure 10. Player 1 was endowed with $0.30 at the start of each round. Player 1 then made the first decision and could pass $0.30 or take $0.30. If Player 1 chose "Take,", they earned $0.30, Player 2 earned $0, and the round ended. If Player 1 chose "Pass" (Trust), the amount of money grew to $0.90, and Player 2 decided whether or not to share the $0.90 with Player 1 ($.45 for each). In each round, Player 1 indicated their choice.

The respondent was assigned to be Player 1 and would decide whether or not to trust Player 2 by passing the endowed/initial amount. The outcome was binary (0/1) as the respondent could only pass or not pass to Player 2. The experiment measures actual trust behavior rather than a trust judgment or trust intent. Standard controls from the previous surveys were used.

Figure 10: Diagram of Trust Game Experiment to Measure Propensity to Trust as Shown to Respondents



64. Vital Anderhub, Dirk Engelmann, & Werner Güth, *An Experimental Study of the Repeated Trust Game with Incomplete Information*, 48 J. ECON. BEHAV. & ORG. 197, 197–216 (2002); Joyce Berg, John Dickhaut, & Kevin McCabe, *Trust, Reciprocity, and Social History*, 10 GAMES & ECON. BEHAV. 122, 122–42 (1995).

A. Design Study 3

American participants (*N=1,014*) were recruited from Amazon Mechanical Turk. Each participant received $1.00 for taking the survey regardless of the outcome of the experimental game. In addition, respondents would receive a bonus of up to $0.50 based on the results of the experiment. In order to test the impact of changing the secondary use (high and low generalized exchange) and qualifier (notice or audit) utilized, a 2x2 design was employed as depicted in Figure 11. Respondents were assigned to one condition for the description of Player 2. The descriptive statistics of each condition subsample is in Table 8.

Figure 11: Possible backgrounds for Player 2 (respondent was assigned to one condition)

	Low Generalized Exchange Use	High Generalized Exchange Use
Notice Qualifier	Condition 2 In the course of his other work, Player 2 provides users' information to a data broker that collects user behavior (browsing, purchases, searches, etc.) to target ads and generate leads. Player 2 always makes sure his practices are included in a privacy notice.	Condition 4 In the course of his other work, Player 2 provides users' information only to a data broker for fraud prevention or academic research. Player 2 always makes sure his practices are included in a privacy notice.
Audit Qualifier	Condition 1 In the course of his other work, Player 2 provides users' information to a data broker that collects user behavior (browsing, purchases, searches, etc.) to target ads and generate leads. Player 2 always makes sure his practices are approved in a privacy audit by an accounting firm.	Condition 3 In the course of his other work, Player 2 provides users' information only to a data broker for fraud prevention or academic research. Player 2 always makes sure his practices are approved in a privacy audit by an accounting firm.

B. Results Study 3

Table 8: Sample Descriptive Statistics for Study 3

Secondary Use: Qualifier:	Null	Low General Audit	Low General Notice	High General Audit	High General Notice
	Condition 0	Condition 1	Condition 2	Condition 3	Condition 4
N	202	210	206	180	216
% Age Over 35	43%	40%	38%	48%	38%
% Male	61%	55%	57%	67%	67%
Trust Online	9.31	15.30	6.85	14.52	16.18
Privacy Important	69.37	75.15	75.23	73.59	70.47

The impact of using information for security (high generalized exchange) as compared to marketing (low generalized exchange) remains positive with 65% passing to Player 2 in the initial round (Initial % Passed $ in Table 8) for the security condition versus 58% for the marketing condition (both using the auditor) which is consistent with the factorial vignette survey findings in Study 2. Interestingly, the switch to adequate notification rather than using an auditor does not impact the percent of respondents that initially trust to 61% (compared to 65%).

Institutional trust matters to a consumer's willingness to engage with a stranger. Figure 12 depicts the percent of respondents who pass money to Player 2 in round one. Respondents who self-describe as having greater institutional trust online are more willing to trust Player 2 across scenarios: from 62% (low trust) to 78% (high trust).

For the governance mechanisms, being audited is an improvement for all respondents but is a larger improvement in trust for those with greater institutional trust. In other words, auditing is particularly useful in improving trust for those with high institutional trust. Finally, the impact of using consumer data for security (rated as good for the community) over to generate leads (rated as not good for the community) is equally important for all respondents equally.

C. Discussion Study 3

The findings extend the work in Studies 1 and 2 by illustrating the importance of institutional trust to a consumer's willingness to engage with a new market actor online. Respondents with high institutional trust were significantly more likely to trust Player 2 (78%) over those with low institutional trust (62%). Further, the governance mechanism of using an

auditor to ensure trustworthy behavior was more effective for those respondents with high institutional trust: 76% of respondents with high institutional trust were willing to trust Player 2 when they are subject to an auditor compared to only 57% willing to trust Player 2 when they are only required to give adquate notice.

Figure 12: Percent who trust Player 2 in Round One for Respondents with Low to High Institutional trust.

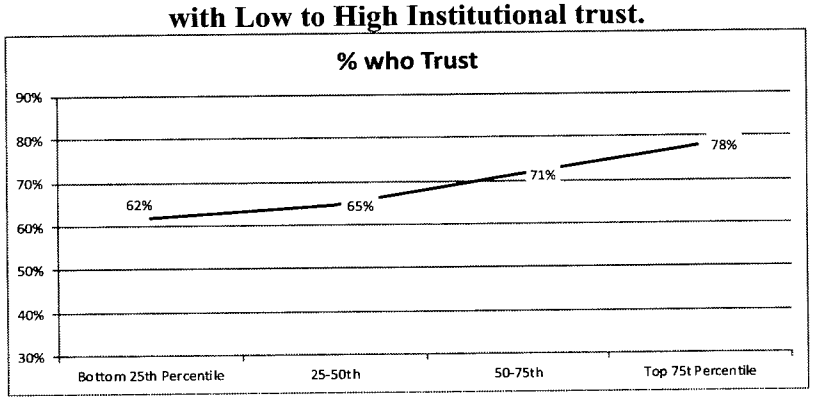


Figure 13: Percent who trust Player 2 for Low and High Trusting Respondents by governance mechanisms.

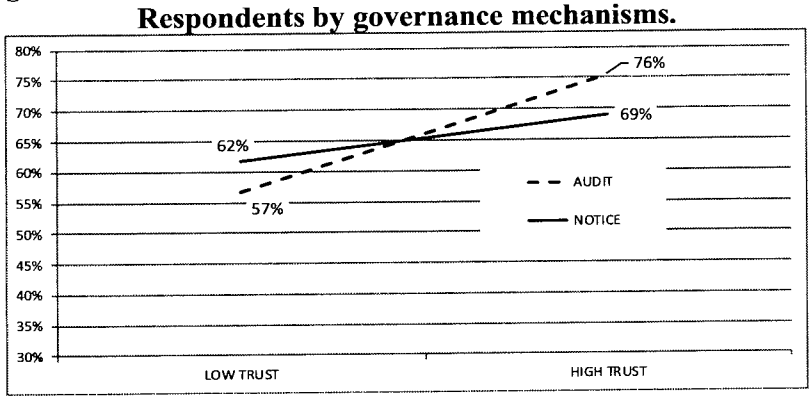
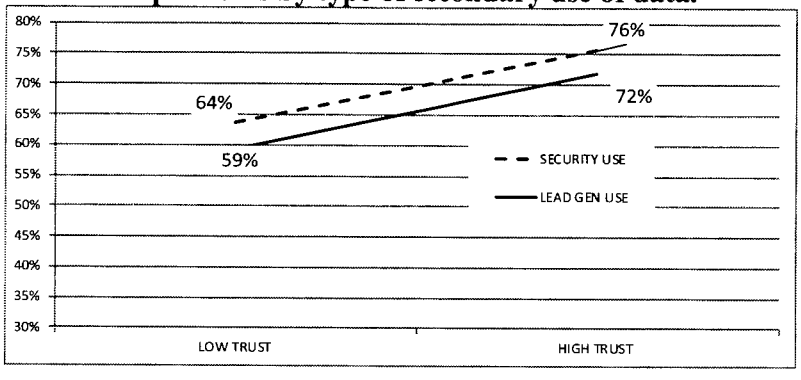


Figure 14: Percent who trust Player 2 for Low and High Trusting Respondents by type of secondary use of data.



V. DISCUSSION AND CONCLUSION

Over these studies, I found the following:

Respondents find secondary uses of consumer data more appropriate if within a generalized exchange (academic research) or within a reciprocal exchange (product search results) or both (credit security). This is contrary to a general assumption that individual have no expectation of privacy post disclosure.[65] Secondary use of information can be justified outside a simple quid-pro-quo reciprocal exchange with the consumer. Secondary uses within a generalized exchange (e.g., credit security or academic research) rather than outside any generalized exchange (marketing) impacts trust more than any governance mechanism such as changing from notice to an audit. In other words, secondary use is more important to trust than any attempts to govern the information flow.

In general, a specialized data broker focused on a limited number of uses of information reinforces the trustworthiness of firms using data within a generalized exchange.

Interestingly, considering the focus on notice and choice in the U.S., using privacy notices is the least effective governance mechanisms of those included here whereas being subject to an audit was as effective as using only non-PII in improving trust. By being subject to an audit, data brokers were still deemed trustworthy even when storing information for a year.

In regard to institutional trust, while firms that use consumer data within a generalized or reciprocal exchange are trusted more than firms who use data to place ads, overall the use of consumer data for secondary uses

65. Kirsten Martin, *Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms*, BUS. ETHICS Q. (forthcoming).

decreases institutional trust online. Institutional trust online impacts a consumer's willingness to engage with a specific online partner in a trust game experiment as well as amplifying the effectiveness of auditing as an effective governance mechanism to increase consumer trust.

These three studies reinforce the need to understand how individuals judge the secondary uses of consumer data as trafficked online and animates a new focus on the role of respecting privacy expectations in institutional trust. The results have implications for governing privacy.

A. Institutional Trust and Privacy Violations

This paper presents results that should animate how we think about penalizing privacy violations by firms. Until now, privacy violations—or the inappropriate collection, sharing, and use of information outside privacy norms—is measured by a breach of a privacy notice or the possible harm to a consumer.

The arguments and findings herein suggest that privacy governance should also be focused on ensuring institutional trust online. The mere description of secondary uses negatively impacted consumer institutional trust online. And institutional trust is important online not only theoretically due to the structure of the online markets (anonymous data traffickers exchanging consumer data with the consumer at an information disadvantage), but Study 3 illustrates how important institutional trust is to have a consumer engage with a new market actor online.

Regulating for institutional trust would require punishing privacy violators not only for any tangible harm to an individual but in order to maintain the integrity of the online market. The Security Exchange Commission (SEC) regulates insider trading "because insider trading undermines investor confidence in the fairness and integrity of the securities market"[66] in a manner similar to the regulation and prosecution of corruption in politics, bribing in foreign markets, and even cybersecurity incidents. Each are investigated and punished to maintain institutional trust in the market and not to right a wrong done to a particular person.

Importantly, this shift to justify regulating privacy-violating behavior and associated punishments based on institutional trust and integrity of the online market would alleviate the problem of identifying specific harms needed to punish privacy violations.[67] In addition, policies would then focus on the need for information flows to support the integrity of the online

---

66. U.S. Sec. & Exch. Comm'n, *Insider Trading*, INVESTOR.GOV, https://www.investor.gov/additional-resources/general-resources/glossary/insider-trading (last visited Jan. 3, 2019).

67. Calo, *supra* note 26, at 1135–42.

market.[68]

Institutional trust promotes greater participation in generalized exchange systems,[69] yet consumers currently lack trust in online advertising firms, and 74% of online consumers takes steps to limit access to their information through obfuscation or anti-tracking mechanisms.[70] Not surprisingly, calls for firms who collect, store, and aggregate consumer information to act as fiduciaries[71] captures the need for firms to actively cultivate consumer trust in order to maintain and use consumer information.[72] With more scrutiny on tracking firms as information fiduciaries via regulators and consumers, identifying what uses and limitations are considered appropriate will help tracking firms match consumer preferences and give guidance to what information fiduciary should do to foster trust.

This paper offers an additional mechanism for regulating privacy to maintain institutional trust online. The online environment has the markers of a market where generalized institutional trust is important to market actors. If privacy violations hurt not only interpersonal trust between a consumer and a firm but also institutional trust online, then privacy would be governed similar to insider trading, fraud, or bribery to protect the integrity of the market rather than only an individual. Punishment for a privacy violation would be set to ensure bad behavior is curtailed and institutional trust is maintained rather than to remediate a specific harm to an individual.[73]

---

68. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1012–15 (2014).

69. Toshio Yamagishi & Karen S. Cook, *Generalized Exchange and Social Dilemmas*, 56 SOC. PSYCHOL. Q. 235, 245 (1993); Takahashi, *supra* note 23, at 1106–07.

70. Richards and Hartzog rightly see obfuscation as fostering distrust. But it is the fault of the institutions and firms for not being trustworthy. Richards & Hartzog, *supra* note 5, at 1208; MARY MADDEN, PEW RESEARCH CTR., THE STATE OF PRIVACY IN POST-SNOWDEN AMERICA (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ [https://perma.cc/JQ39-BTE4]; Finn Brunton & Helen Nissenbaum, *Vernacular Resistance to Data Collection and Analysis: A Political Theory of Obfuscation*, 16 FIRST MONDAY 1, 7 (2011). *See generally* HELEN F. NISSENBAUM & FINN BRUNTON, OBFUSCATION: A USER'S GUIDE FOR PRIVACY AND PROTEST (2015).

71. *See generally* Richard R. W. Brooks, *Observability & Verifiability: Informing the Information Fiduciary* (Working Paper, 2015). *See also* Richards & Hartzog, *supra* note 25 at 457.

72. Consumer data brokers and aggregators as having fiduciary duties is not without criticism. *See* Jane R. Bambauer, *The Relationships between Speech and Conduct*, 49 U.C.D. L. REV. 1941, 1950–53 (2016).

73. One downside of institutional trust or regulations specifically is that actors are not able to build trusting relationships. "Indeed, financial regulation and governance concerns impersonal or system trust and thus involves strategies to constrain agents' behavior to reduce risks and uncertainty, acting as functional substitutes for interpersonal or relationship trust." Nicole Gillespie & Robert Hurley, *Trust and the Global Financial Crisis*, *in* ADVANCES IN TRUST RESEARCH 193 (2013).

B. Secondary Use of Data

Previous work on privacy in public has mistakenly viewed individuals as relinquishing privacy expectations post-disclosure as to who has access to data and how information is used.[74] In the law, the plain view and third party doctrines equate even possible disclosure to others to individuals having no expectations of privacy.[75] However, here consumers differentiate types of secondary uses of information and deemed the majority of uses as inappropriate—even after disclosure. Most uses studied here are lower on both scales than using data to place ads—the standard bearer justifying secondary use of data online. Further, the average degree the secondary uses were deemed appropriate was negative (judged not appropriate). While uses can be justified outside the standard reciprocal exchange, the majority of the uses are deemed neither good for the consumer nor society. Individuals have strong privacy expectations as to how information is used even after the disclosure of information.

In addition, the results offer a meaningful typology for secondary uses as along two scales: as within a reciprocal exchange and as within a generalized exchange. The typology is significant in predicting if the secondary use is deemed appropriate or not. Such judgments are critical for regulations such as the European Union's General Data Protection Regulation (GDPR) which relies upon "legitimate interests" of consumers and firms to justify gathering and using consumer information without consent.[76]

This typology of secondary uses is also meaningful in predicting if consumers trust data brokers in the study. How information is used is more impactful on consumer trust than any other governance mechanism such as deleting data, having a specialized data broker, auditing the firm, hiring a professional data scientist, etc.

The findings have implications for public policy and practice. The flow of information online need not only be justified in a simple quid-pro-quo

---

74. Professors Martin and Nissenbaum have conducted a series of studies to show how individuals have nuanced privacy expectations about their data after disclosure and when in "public." *See* Martin & Nissenbaum, *supra* note 3; Kirsten Martin & Helen Nissenbaum, *Measuring Privacy: Using Context to Expose Confounding Variables*, 18 COLUM. SCI. & TECH. L. REV. 176 (2017).

75. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 565 (2009); Monu Bedi, *The Fourth Amendment Disclosure Doctrines*, 26 WM. & MARY BILL RTS. J. 461, 461 (2017).

76. This finding fits with Beales and Muris's argument that notification is not necessary for sharing information for the good of the context such as banking or education as well as the GDPR's concept of legitimate interest: such sharing is well within the privacy expectations of individuals when interacting within a particular, defined context. J. Howard Beales & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 133–34 (2008); Overview of the General Data Protection Regulation (GDPR), *supra* note 28.

exchange with the consumer but could also be justified as necessary or appropriate for the online context within a generalized exchange. This opens up additional legitimate flows of information for firms and places less pressure on firms to justify why the collection of information is benefiting the consumer specifically. However, the majority of secondary uses cannot be justified as within a general exchange (benefiting the broader community) or a reciprocal exchange (benefiting the consumer directly). Uses of information that are not beneficial to the individual or necessary for the context were still judged inappropriate, violations of privacy, and as decreasing both interpersonal and institutional trust. These findings suggest that some uses of consumer data—deemed well outside either a generalized or reciprocal exchange—would be candidates for being outside minimum standards of acceptable market behavior. And the study suggests that either regulation or industry self-regulation could be valid governance mechanisms.

C. Governance Mechanisms

Consumers express concern about who has access to and later uses information about their activities online,[77] and regulations on data processors—those data brokers aggregating and using consumer data—have arrived.[78] While adequate notice is a popular regulation of privacy in the U.S.,[79] notice was the least effective governance mechanism at engendering trust compared to using an auditor, hiring a professional data scientist, utilizing a review board, and keeping anonymized data. This finding is in keeping with the scholars who find privacy notices as a mechanism for distrust[80] and find notices to be so ambiguous as to be ineffective.[81] For governing privacy for consumer trust, these alternative governance mechanisms are worthy of further examination either within private or public ordering.

Relatedly, each governance mechanism offered was equally effective at engendering consumer trust in a firm whether by legal mandate or due to competitive forces. But specialized data brokers do enhance the

---

77. Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ [https://perma.cc/JQ39-BTE4].

78. Overview of the General Data Protection Regulation (GDPR), *supra* note 28.

79. As noted by FTC Commissioner Edith Ramirez, "[c]ompanies should be more open, clear, and transparent about their data practices so that consumers can . . . exercise greater control." Mike Orcutt, *FTC Chairwoman: We Must Not Give Up on Privacy*, MIT TECH. REV. (Oct. 10, 2016), https://www.technologyreview.com/s/602474/ftc-chairwoman-we-must-not-give-up-on-privacy/?utm_campaign=add_this&utm_source=twitter&utm_medium=post [https://perma.cc/6Q6U-WY9G].

80. Martin, *supra* note 55, at 193.

81. Marotta-Wurgler, *supra* note 55, at 5. *See also* Martin, *supra* note 37, at 220.

trustworthiness of firms that keep secondary use of data within a generalized exchange. One area for a possible competitive advantage with data brokers is to become more specialized based on the types of appropriate secondary uses of consumer data as measured in studies.

However, secondary use of information is still the elephant in the room for firms worried about trust. In many ways, the addition of governance mechanisms, such as an audit or including a review board, is akin to the saying "putting lipstick on a pig": there is only so much that can be done in terms of governance to achieve consumer trust with secondary uses of consumer data that are deemed to be inappropriate and privacy violations. The majority of popular secondary uses by data brokers are well outside the legitimate interests of consumers.

CONCLUSION

This paper explored how privacy governance should also be framed as protecting a larger market or institution. In doing so, I suggest two paths forward. First, we should look to justify legitimate information flows and secondary uses of information as not only reciprocal exchanges which are good for the consumer, but also as generalized exchanges which are good for the context or institution. Second, privacy violations should be framed as detrimental to market integrity and institutional trust, and pursued similar to violations such as insider trading, bribery, and corruption to thereby maintain consumers' institutional trust and engagement online.