First Monday, Volume 18, Number 12 - 2 December 2013

PEER-REVIEWED JOURNAL ON THE INTERNET

Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online

by Kirsten Martin

Abstract

The goal of this paper is to outline the laudable goals and ultimate failure of notice and choice to respect privacy online and suggest an alternative framework to manage and research privacy. This paper suggests that the online environment is not conducive to rely on explicit agreements to respect privacy. Current privacy concerns online are framed as a temporary market failure resolvable through two options: (a) ameliorating frictions within the current notice and choice governance structure or (b) focusing on brand name and reputation outside the current notice and choice mechanism. The shift from focusing on notice and choice governing simple market exchanges to credible contracting where identity, repeated transactions, and trust govern the information exchange rewards firms who build a reputation around respecting privacy expectations. Importantly for firms, the arguments herein shift the firm's responsibility from adequate notice to identifying and managing the privacy norms and expectations within a specific context.

Contents

Introduction
Privacy online, second exchanges, and transaction costs
Why notice and choice fails
Possible remedies for privacy online
Developing a privacy reputation: Privacy in practice
Implications for practice and research
Conclusion

Introduction

> In January, 2011, Facebook introduced Sponsored Stories to advertisers and users. When users liked an advertisement, mentioned a company in a post, or checked–in at a business, the user's profile and picture were sent within an advertisement to all the user's Facebook friends linked on Facebook within the normal posts in the user's News Feed without their knowledge. By April, 2011, a lawsuit was filed contending that Facebook violated the privacy expectations of users and did not give users a way to opt out of the advertising program. Facebook noted that the idea of Sponsored Stories had been included in their online user notices (Carter, 2011; Cheng, 2011; Kravets, 2012).

When online, as in the situation with Facebook above, notice and choice is the dominant mechanism to respecting privacy. Notice and choice constitute a particular mechanism to govern transactions online, where Web sites and users agree to the terms of the privacy notice and users' consent before continuing the transaction. Current tactics to addressing online privacy focus on Fair Information Practices (FIP) as a way to allow for the contemporaneous disclosure of information and respect of privacy norms while online. While definitions and applications of FIP vary (Culnan, 1993; Rubinstein and Good, 2013), notice and choice are seen as core to FIP (Beales and Muris, 2008), and FIP has become synonymous with how firms protect privacy with stakeholders (Bowie and Jamal, 2006; Culnan and Armstrong, 1999; Culnan and Williams, 2009; Peslak, 2005). The Federal Trade Commission's reliance on FIP, and notice and choice in particular, serves as

a source of guidance for self–regulation within the industry [1]. Solove and Schwartz (2011) succinctly summarize notice and choice: "As long as a company provides notice of its privacy practices, and people have some kind of choice about whether to provide the data or not, then privacy is sufficiently protected" (see also Sloan and Warner, 2014). Firms can then be judged based on how well they conform to notice and choice principles (*e.g.*, Williams, 2006), and respondents' concern for FIP is equated to a concern for privacy (Smith, *et al.*, 1996; Smith, *et al.*, 2011; Stewart and Segars, 2002; Malhorta, *et al.*, 2004).

Notice and choice embody laudable goals as a mechanism to govern information exchanges online with the ability to incorporate societal values, normative expectations, and dominant privacy approaches tailored for each transaction. Notice and choice, as a tactic to respect privacy online, focuses on users to fully understand the terms at the point of the exchange, and thereby attempts to empower individuals in a free market (Nissenbaum, 2011) and to give control to consumers (Whittington and Hoofnagle, 2012). Enforcement of adequate notification is cheaper, easier, and more popular than alternatives [2]. In addition, notice and choice can be viewed as consistent with privacy scholarship by allowing for heterogeneity in privacy expectations — each exchange develops a particular set of rules governing how, when, why, and where information is used. Shopping online, talking in the break room, and divulging information to a doctor are governed by the information norms of their social context, and non-uniform privacy notices allow these terms to fit within a given context.

Yet, these information exchanges between users and Web sites appear to fail in regards to the privacy expectations of users. Where users have become empowered in shifting many transactions online — such as looking for a car, finding a mortgage, or buying a pair of jeans with additional pertinent information, lower switching costs, and greater competition — individuals feel incompetent and impotent when it comes to privacy online as concerns surrounding privacy increase. Of surveyed Web sites, 61 percent transmitted identifying information to at least one outside Web domain, and 45 percent transmitted identifying information to at least four additional organizations online (Angwin, 2011); yet a majority of users (68 percent) have stated that they *never* approve of being tracked online (Turow, *et al.*, 2009). Users perceive themselves to be left without a real choice since the alternatives are not apparent as companies regularly "stack the deck to make certain choices easier, more obvious, [and] more likely to occur" (Tene and Polentsky, 2012). Consumers, therefore, see a monolithic "Big Data" actor online that stubbornly collects and consolidates their data — not only are consumers not fully aware, but they also lack the power to choose otherwise (Brunton and Nissenbaum, 2011).

In response, individuals have attempted to pull out of this information exchange and obfuscate their behavior using tools such as CacheCloak, donottrack.us, Bit Torrent Hydra, TOR, Disconnect, and TrackMeNot, which work to allow users to reap the benefits of a Web site without passing identifiable information to the Web site and tracking companies (Brunton and Nissenbaum, 2011; Empson, 2013; Mayer and Narayanan, 2010). Such small acts of rebellion against the current notice and choice approach are the 'canaries in the coalmine' of misaligned governance mechanisms and the associated social frictions. Rather than declare privacy to be dead, these market signals should be seen as an early opportunity to adjust the governance strategy using more alert, entrepreneurial firms.

While considerable agreement exists that transparency and choice has failed (Nissenbaum, 2011), notice and choice within FIP remains popular as a mechanism to govern information exchanges online. The goal of this paper is to analyze when and why notice and choice fails to adequately respect privacy expectations online in order to identify alternative governance structures to support mutually beneficial relationships around privacy online. As argued below, the online environment merely typifies the boundary conditions of notice and choice — where privacy approaches relying on explicit contracts in a simple market through informed consent cease to be useful. High information asymmetries, moral hazard risks, and a complicated and dynamic system of tracking render relying on explicit contract agreements to govern privacy norms online untenable.

A range of governance structures exist to guide such online transactions (Williamson, 1986; Coase, 1937). After first understanding the factors driving the failure of notice and choice to successfully govern information exchanges online, the second portion of the paper outlines two paths to remedy the problems with privacy online. First, tactics including legislation, industry best practices, and privacy enhancing technologies can be understood as ameliorating frictions in the current notice and choice governance structure. Second, as noted by transaction cost economists and explored here, the environment described calls for a shift from a contract–governed exchange to a focus on brand name and reputation outside the current notice–and–choice mechanism. The shift from focusing on notice and choice governing simple market exchanges to relying on credible contracting, where identity, repeated transactions, and trust govern the information exchange, rewards firms who build a reputation around respecting privacy expectations. Importantly for firms, the firm's responsibility shifts from adequate notification to identifying and managing the privacy expectations within a specific context. A consequence–based approach, privacy in practice, is offered as an alternative framework to make sense of privacy online and draws on a stream of privacy scholarship moving away from notice and choice (Sloan and Warner, 2014; Barocas and Nissenbaum, 2009; Beales and Muris, 2008). This shift away from notice and choice has direct implications to management: firms take on a larger role in managing the privacy expectations of users rather than rely on users to shoulder the responsibilities of determining privacy expectations online.

Privacy online, second exchanges, and transaction costs

In addition to the many commercial exchanges online [3], where a user exchanges money for goods or services, a second exchange occurs. In this second exchange, the user provides information in the form of search terms, clicks on a Web page, browsing history, or demographic information in exchange for "value such as high quality services and personalized offers or discounts" [4], or for just the privilege of interacting with that website or application [5]. While money does not change hands, both the users and the website receive benefits within this second transaction.

In fact, this second exchange has taken on greater prominence with the focus on notice and choice as the remedy to privacy concerns online. In effect, the Web site's notice and the associated user consent constitute the explicit agreement that governs a handoff when an individual relinquishes their information and the Web site agrees to abide by the terms of the written privacy notice. Users and Web sites thereby agree as to how, when, why, and where the users' information is gathered, shared, and used, and the rules or norms governing the use of information are based on the privacy notice when this second exchange takes place.

Transaction cost economics suggests analyzing transactions or exchanges based on the relative cost of making transactions for both parties. Transaction costs are the costs to initiate, carry out, and possibly terminate an agreement, consisting of *ex ante* pricing, bargaining, and decision costs as well as *ex post* enforcement costs (Coase, 1937). *Ex ante* pricing costs include drafting, negotiating, and safeguarding (Williamson, 1979) as well as the costs to identify pricing, parties, and product [6]. For the online user, *ex ante* costs become the time and cost required to *identify* all Web sites and tracking parties involved, their approaches to handling information, and the benefit (if at all) of handing over information. In other words, the time and money necessary to identify relevant parties and privacy options online, to incorporate possible contingencies in an online environment, and to write findings into an explicit contract increases the costs of bargaining and decisions online. *Ex post* costs occur after the signing of the contract or after users give consent by engaging with the privacy policy online. This includes the ability to (a) identify a problem; (b) enforce and penalize the offending party; and, (c) switch to an alternative provider if the explicit contract is broken. These transaction costs are also called "get together costs, decision and execution costs, information costs" (Ellickson, 1989) or simply, the cost of communicating (Cooter, 1982) [7].

Key to transaction cost economics is minimizing costs in comparison to alternatives. Each transaction can be governed by a range of structures or mechanisms: *e.g.*, in a spot market, with a handshake, with a written contract, within a firm, by a government, in a long–term and trusted relationship, etc. Transaction cost economics is a comparative analysis and moves towards the possibility of private ordering, where "exchange partners attempt to work through and perfect trading relations in a self–help way" to realize the mutual advantage (Williamson, 2002) [8]. In other words, getting the governing structure right is not only relative to alternatives, but it also takes time and patience.

When private ordering is done successfully, both parties are treated fairly and realize benefits in the solution. Transactions, when aligned with a governance structure and working correctly, provide order, relieve conflict, and support mutually beneficial solutions (Williamson, 2002; van Oosterhout, *et al.*, 2006). In fact, "gains from the trade are *conditional* on getting the governance structures right" (Williamson, 2002, emphasis added). In other words, successful private ordering should appear to be fair and mutually beneficial with happy exchange partners. Opportunistic behavior by either party adds friction to the exchange, thereby making the transaction more costly than alternative alignments (Williamson, 2002).

Misalignments regularly occur when the chosen governance mechanism does not adequately govern the underlying exchange. For example, if a house were purchased (the transaction) based solely on a handshake (the governance structure), multiple failings would probably follow: buyers could walk away from agreements, sellers could change their minds after buyers sell their current house, buyers could make deposits on multiple houses, etc. The transaction is not fatally flawed, but the misalignment of the governance structure of a handshake may cause one party to be at a disadvantage. Transaction costs help explain why individuals do not optimally solve problems and conflicts (Schwab, 1989), and transaction costs, for Coase, drive the ability to the successful private ordering of harms.

Currently, many firms get it wrong with online privacy. Over 68 percent of Americans reject all tracking online (Turow, *et al.*, 2009), yet 87.5 percent of Web sites examined allow third–party tracking cookies on their Web site (Ayenson, *et al.*, 2011). Most importantly, the current and measurable discontent surrounding respecting privacy online is a temporary market inefficiency that is resolvable through private ordering. The burden has been on the user with disproportionate costs (McDonald and Cranor, 2008; Marotta–Wurgler, 2011), little bargaining power, and questionable procedural and interactional fairness without voice in the process (Brunton and Nissenbaum, 2011). While the failings of notice and choice have been documented, when and why informed consent fails to adequately respect privacy online has not been addressed. Identifying the cause of the misalignment of the governance mechanism will support outlining possible remedies.

Why notice and choice fails

Identifying the impediments to successful private ordering will provide a roadmap to potential remedies and alternative structures. Notice and choice can be useful, but "it is not clear that it should serve as the golden rule for privacy design in all cases" (Spiekermann and Cranor, 2009). Notice and choice, as an explicit contract between the primary website and the Internet user, works in certain circumstances similar to other explicit contracts: (a) where the relevant information is understood by all parties; (b) when the contract is enforceable in that the harms are detectable and reparations are possible; and, (c) when the environment is stable with low uncertainty to allow for transactions to continue with low costs (Coase, 1937). Each requirement is examined below in regards to the online environment.

1. Information asymmetries

Information asymmetries exist when one party is privy to information about a transaction not available to another. Information asymmetries may impact *ex ante* costs when one party is not being able to identify the quality of the product or service (Akerlof, 1970) or is not able to identify an appropriate market price (Coase, 1937). In addition, information asymmetries may exist around identifying the parties in the transaction. In Coase's (1937) famous example, a farmer and a rancher owned land next to each other and were easy to identify as transaction partners. Yet, transactions may occur where parties are not known to each other with an associated cost of *finding* the transaction partner.

For example, a buyer of a used car may not have access to the car's history or current working condition and, therefore, would be unable to accurately assess the quality of the product (Akerlof, 1970). In addition, the buyer may be in a small town and not have access to the used car market to assess an appropriate price even if given information on the car. Both types of information asymmetries add costs to the transaction. In the case of the used car purchase, the buyer historically bears the brunt of the cost (Akerlof, 1970). Information asymmetries can lead to parties feeling 'duped' or tricked in the exchange as information may become available or knowable after the transaction is complete. In the used car purchase, for instance, the car may break down a year later or the buyer may find a competitor's lower price.

In terms of online privacy statements, organizations are limited in effectively communicating to consumers how information flows even when individuals do read privacy notices. Policies are byzantine (Hull, *et al.*, 2011) in their attempt to capture a complicated flow of information to include data aggregators, ad networks, and third party tracking companies (Barocas and Nissenbaum, 2009). Even the difference between primary websites and third–party companies is fuzzy (Cooper and Tschofenig, 2011). Users struggle to understand the complicated system of online tracking with a network of technologies and actors working in concert to track user behavior across Web sites and across sessions. The problem does not lie solely with the complicated environment, as individuals struggle to take in long written contracts with accuracy (Calo, 2013) [9]. At the time Sponsored Stories was introduced, Facebook's privacy policy was 5,830 words and the portion pertaining to Facebook's Sponsored Stories was "buried in a Help Center page, not connected by any link with the Privacy Policy of Statement of Rights and Responsibilities page." [10]

Privacy scholar Helen Nissenbaum (2011) summarizes this tension as the *transparency paradox*, wherein the more that information is shared through notice statements, the less understandable those notice statements are for authentic consent by the user. In other words, explicit privacy statements will not be both accurate and understandable given the complicated system of tracking and surveillance online. This paradox is found in practice: instead of helping consumers limit tracking, tools to detect online tracking were more likely to cause confusion and, at times, accomplish the opposite of what the user intended (Loftus, 2011). The user has little information about the quality of the firm's information management tactics, the degree to which the Web site abides by the user's privacy expectation, the market price for comparison, or all the third parties relevant to the exchange of information. The situation is fraught with high information asymmetries where the primary Web site has access to a disproportionate amount of relevant information that is unknowable by the users.

2. Enforcement

Enforcement costs occur after the agreement has been reached and include the cost to identify a problem, adjust the contract, and institute reparations or switch exchange partners. Without the ability to enforce an agreement, one party may be seen as particularly vulnerable and needing additional protections. In the case of the exchange of information online, users are at a disadvantage to be able to identify (1) any violation; (2) the responsible party for that violation; or, (3) the steps to fix any violation of a notice and choice agreement.

First, users are limited in identifying if and when a breach of the contract may have occurred, as violations to privacy statements are not obvious even to experts (Mitchell and Mayer, 2012). When a defective product is purchased from a large brick–and–mortar store, the consumer can identify the problem and return the product in order to be compensated — even months later. However, detection and reparations are exceedingly difficult and time consuming online. Even if information has obviously been leaked to third party tracking companies, which Web site allowed the leakage is difficult, if not impossible, to ascertain. The issue of information leakage is widespread (Mayer, 2011), where information expected to remain in one location or within one context is later leaked to additional parties or used in a novel way. Such information leakage is a violation of the prevailing privacy norms within the context. Out of 85 Web sites analyzed, 45 percent transmitted identifying details (Angwin, 2011) — a real concern as only three pieces of data are needed to identify 87 percent of the population: gender, zip code, and birthday (Sweeney, 2000). In the case of

Facebook's Sponsored Stories, users had to be notified by recipients that their preferences were being broadcast as the information leak was not immediately obvious to the user.

Second, enforcement is difficult with notice and choice agreements as many of the relevant and responsible actors are not party to the actual agreement. Beacons, Web bugs, cookies, and flash cookies are used by tracking companies to follow users' online activities. The actors and flow of information online are obscure with many indirect, third–party organizations involved (Barocas and Nissenbaum, 2009). Even organizations with the best of intentions to notify users struggle to communicate complicated and changing policies which, given the large network of actors in the online space, may conflict with the policies of their online partners such as ad networks, third–party organizations, and user–generated applications (Brunton and Nissenbaum, 2011).

Third, while switching exchange partners is possible, *e.g.*, a user could switch from one travel site to another, violations of the privacy agreement are not retractable. In other words, once the information is leaked — either to a third party or to friends as in Sponsored Stories — the user cannot demand that the information be 'unleaked'. *Ex post* costs include identifying infractions to the contract as well as negotiating possible remedies to the infraction. However, there is no 'undo' button online as the information quickly moves from the primary site to the network of tracking organizations. Even if the Web site is identified as disclosing information to a third party, the user has little recourse as the data is quickly sold to large data aggregators and networks. Enforcement of explicit contracts online is costly for the user because: (a) the explicit agreement is between the primary website and the user where third parties are violating the agreement; (b) detection is difficult; and, (c) reparations are not feasible for the user. Without adequate enforcement mechanisms, users are not given the ability to enforce the contract — either through reparations or exit — which is necessary for successful private ordering and fair exchange.

3. Uncertainty

In addition to the cost to discover relevant prices and to negotiate and conclude the contract, transaction costs include the cost to identify necessary changes to the contract [11]. While "all complex contracts are unavoidably incomplete" (Williamson, 2002), maladaptation occurs when parties are not able to adjust in a cost–efficient way based on new information (Williamson, 1975, 1986; Hoofnagle and Whittinger, 2012). Explicit contracts work best when the environment is stable with few material changes in the foreseeable future for all parties.

The online environment is uncertain, where the future possibilities around the flow of information are difficult to predict. New technological capabilities introduce the problem of unknown, future information leakage where information expected to remain in one location or within one context is later leaked to additional parties or used in a novel way (Mayer, 2011). The use of cookies gave way to flash cookies which were followed by super and *uber* cookies (Jackson, 2011; Mayer, 2011; Tene and Polentesky, 2012). Similarly, behavioral tracking was followed by browser finger printing, device fingerprinting, and history sniffing. Each successive innovation brings increasingly persistent tracking capabilities with new information being gathered by new actors. Privacy policies change frequently in order to incorporate technological upgrades and novel privacy measures, which renders keeping abreast of the most recent version a herculean task for users (Wurlgler, 2010; Hull, *et al.*, 2011; Barocas and Nissenbaum, 2009).

Summary

With the current notice and choice approach, once the information exchange occurs, the information is deemed public, owned, or fairly gathered by the Web site with only those norms or expectations explicitly written in the agreement governing the exchange. Web sites are in a state where 'anything goes' (Nissenbaum, 2004), leaving little guidance to make sense of the inevitable novel technological capabilities and changes to information technology. In relying on explicit notice and choice to govern privacy expectations, the Web sites take a "Schillerian" approach where "what is not forbidden is allowed" [12]. In fact, the only affirmative responsibility of Web sites is adequate notification (Calo, 2013).

Notice and choice as the sole mechanism to address privacy fail where similar explicit contracts fail: where the environment renders the transaction costs of the exchange too high. High information asymmetries, enforcement costs, and uncertainty combine to make the online environment hostile to effective explicit contracting.

Possible remedies for privacy online

Privacy agreements governed by notice and choice fail to adequately address privacy expectations online, leaving two approaches to ameliorate privacy concerns. First, the existing approach to privacy online could be modified to possibly resuscitate notice and choice as a mechanism to govern information exchanges online. Second, a new governance mechanism for the information exchange would shift to focusing on brand name and reputation with credible contracting and trust to govern the exchange. Both approaches are explored below.

Adjustments within the existing notice and choice approach

Small, mutual adjustments of behavior to resolve social frictions should be expected in a market. Stability in private ordering is possible "through discriminating alignment, where by transactions (which differ in their attributes) are aligned with governance structures (which differ in discrete structural ways and display different adaptive capacities) so as to effect an economizing result" (Williamson, 2002). In other words, potential remedies should provide a harmonizing effect (Williamson, 1981).

In his famous examination of the market for lemons in the used car industry, economist Akerlof (1970) provides four options to realign a transaction with the governance structure: (1) increase the ability to identify quality; (2) add guarantees; (3) provide licensing practices; and, (4) focus on brand name and reputation. The first three work within the existing notice and choice approach and attempt to relieve some of the frictions in the exchange: information asymmetries, enforcement issues, and uncertainty [13].

First is the ability to **identify quality** for users' attempts to remedy the information asymmetries around the pricing mechanism. For example, the browser add-on "Terms of Service; Didn't Read" (TOS;DR http://tosdr.org) analyzes privacy policies of online services and summarizes the analysis in a grade for the policy. A grade of "Class E" (on a scale from A to E) would include a service that takes credit for users' content, indemnifies the service for any claims, and does not really delete content a user thinks is deleted. TOS;DR highlights the important differences in the privacy policy of telecommunication and online services so that users can incorporate the particular policies into their decision to use the service. Similarly, recent work on privacy seals (Hann, *et al.*, 2008) and privacy labels (Kelley, *et al.*, 2009) propose to reduce the information asymmetries online for the user by offering meaningful information about the privacy policy in an easily digested format. In an experimental study through a Future Privacy Forum 2009 initiative, Professor Cranor examined privacy nutritional labels in order to standardize privacy notices online. Certificates or seals give an immediate signal to the user as to the quality with mixed results in practice (Hann, *et al.*, 2008), and a labeling mechanism by which a Web site's match to a user's desired privacy expectations has been proved successful in experimental studies (Aquisti and Varian, 2005; Aquisti and Grosslags, 2005; Aquisti, *et al.*, 2011).

Second, **guarantees** of the product or service serve to shift the risk and responsibility from buyer (Internet user) to seller (Web site) in an attempt to assuage concerns about uncertainty. Users do not have the knowledge or power to explicitly call for particular contingencies with rapidly changing actors and tracking capabilities (Brunton and Nissenbaum, 2011), and a trend in privacy scholarship calls to shift the burden from users to business (Tene and Polenetsky, 2012; Martin, 2012). The focus with privacy online has been on the users to choose wisely, thereby placing the burden on individuals to decide when to share information. Rather than focus on 'don't tell' as the main remedy, law scholar Peppet (2010) proposes focusing instead on 'don't ask' or 'don't use' to change the flow of information and place the responsibility on Web sites rather than users. Similarly, the proposed 'undo button' and the right to be forgotten (Rosen, 2012; U.S. White House, 2012) as well as treating changes to privacy policies as a change in the Web sites' trademark (Ohm, 2013) place a burden on the Web site to uphold their policies and adds to the cost of retaining data [14].

Third, Akerlof suggests **licensing practices or industry best practices** to guide behavior and aid in enforcement within notice and choice. The FTC's "Do Not Track" report and commonly accepted practices are seen as attempts to recommend industry best practices. Within regulation, the Commercial Privacy Bill of Rights Act of 2011 further pushes enforcement to the FTC. Recommendations at the browser level, such as adding tracking protection or the voluntary conformance to standards supplements work with the Better Business Bureau to highlight best practices within a notice and choice approach. Similarly, the application "Clueful" scans applications on smartphones and shows which application are "not malicious" in conforming with the best practices defined by the company (Perez, 2013b).

Table 1: Approaches to fixing privacy online.

Governance mode	Possible amelioration	Attempts to fix (Problem online)	Continuing hurdles
Explicit contracts & transaction focus	Identify quality through seals, Use TOS;DR	Information asymmetry	Transparency paradox (Nissenbaum, 2011)
	Licensing practices or industry best practices	Enforcement	Identifying breaches of contract
	Guarantees	Uncertainty	Technological instability with data retention and

			possible second use
Laws and regulation/Government focus	Limits in data access and use	"Anything goes" (Nissenbaum, 2004) Schillerian approach (Solove and Schwartz, 2011)	Inability to innovate with outdated regulations. Loss of trust between parties by relying on regulations.
Trust and reputation/Relationship focus	Focus on privacy in practice with firms increasingly responsible for privacy norms of information exchange		Identifying evolving privacy expectations and contexts

Alternative modes of governance

The frictions around privacy online are not easily ameliorated. Nissenbaum's concept of a transparency paradox shows that revealing more information to a user is not necessarily a fix to information asymmetry. Specifically, relying on better notification within a simple exchange does not resolve how to fully explain the current and possible secondary uses of information while not overwhelming the user. Further, the nature of information sharing and leakage online is fundamentally different than, for example, purchasing a defective bike from Target. While parallel service examples exist which are not 'returnable' — such as a wedding reception — breaches online remain difficult to identify in a timely manner to make consumer decisions. When the environment for an exchange is inhospitable to governance through an explicit contract, conflicts arise, solutions are not mutually beneficial, and transaction costs are high. Alternative governance structures may be necessary to create stable relationships rather than attempt to modify the existing reliance on notice and choice within a simple market exchange.

Outside the current notice–and–choice mechanism, a focus on **brand name and reputation** shifts the exchange away from the one–shot dilemma governed by an explicit contract to a long-term relationship or repeated transactions governed by trust (Kollock, 1994), credible contracting (Williamson, 2002), or implicit rules (Akerlof, 1970).

Market for rubber and rice. Kollock (1994) provides a useful parallel example of a market with evolving governance structures in his comparison of the original markets for rice and rubber. The market for rice had low information asymmetries and minimal uncertainty surrounding the transaction for both buyer and seller. The quality of the rice was known immediately to both parties by feel of the rice, and the conditions for use were stable after the transaction. Furthermore, competitors were available in the market. Such an environment is more closely aligned with typical economic context for explicit contracts: where information is readily and easily attainable by both parties and switching costs are low, the trade can be performed in an anonymous exchange governed by an explicit agreement. In such a situation, reputation matters little (Kollock, 1994).

However, in the market for rubber, the information about the product was *not knowable* at the time of sale, as time was required to ascertain the quality of the rubber. Yet, exchanges in such an environment with high information asymmetries and uncertainty still prevailed. According to Kollock, the exchange of rubber survived not through a spot market, or with a simple exchange governed with an explicit contract, or through blind trust in the seller, or with an elaborate governance structure. Instead, the exchange of rubber shifted to one "with personal, long term exchange relationships between particular buyers and sellers" [15] which allowed for the development of fairness and trustworthiness within relationships (Kollock, 1994). In doing so, parties with a reputation for trust realized a competitive advantage by decreasing the costs to correctly price the product and for enforcement. In the case of rubber, "the possibility of repeated exchanges means commitment can be used as a response to the risks that derive from information asymmetry" [16]. The governance structure shifted to be better aligned with the attributes of the transaction.

For online privacy, many may desire a market that is similar to that of rice, where information is known, enforcement is possible, and uncertainty is minimal. However, the current market is closer to that of rubber, where identity and reputation matter. Transaction cost economists recognize the important "difference between generic transactions with faceless buyers and sellers who exchange standard goods at equilibrium prices versus exchanges where identities matter and continuity of the relationship has significant costs and consequences" (Williamson, 2002).

Parties are in a bilateral dependency when asset specificity and contractual hazards render parties "vulnerable" (Williamson, 2002, quotes in original). And when parties are vulnerable, the simple market gives way to credible contracting where identity and continuity is important (Williamson, 2002) to allow reputations to develop. Credible contracting, within transaction cost economics, offers parties mechanisms for information disclosure and verification, specialized dispute mechanisms, penalties, etc. to account for the increased vulnerability through asset specificity, contracting hazards, and information asymmetries.

Requirements for brand and reputations to develop. For brand and reputation to effectively govern a particular transaction type, identity, repeated transactions, and preferences become important. First, rather than the faceless buyers and sellers in the simple spot market, identity matters in a bilateral dependent relationship in order for brands and reputations to develop. The need to identify an opportunistic or defrauding firm renders opportunism or fraud unprofitable (Coase, 1988). Second, repeated transactions offers incentives to firms to modify their behavior and align the quality and price of the product with the desires of the buyer. The frequency of repeated transactions increases the efficacy of reputation effects as well as the incentives to incur cost of any specialized internal governance (Williamson, 2005). Within long–term relationships, such as in the market for rubber, repeated transactions take on the form of continuity of the particular relationship poor performance can put future transactions at risk. However, reputational effects put additional transactions at risk with third parties; poor performance can put transactions at risk with other parties. Third, relying on brand and reputation requires signals from the consumer that are then indicated in prices and quality. These signals, in the form of voice, are as important as the ability to exit in private ordering [17]. For example, buyers of rubber needed to explain to sellers their criteria for value; and online users and firms need a mechanism to voice their preferences.

In situations such as the market for rubber described above, reputations are built over repeated transactions through a continuous relationship, where the identities of the parties are known. In addition, institutional trust can develop through societal norms, professionalism, or a network of buyers and sellers. For example, diamond dealers in New York City are embedded in a close–knit community of merchants where the cost and consequences of fraud or opportunism are magnified by the number of future transaction affected (Williamson, 1993). Rather than lose one customer, a fraudulent dealer of diamonds or rubber could lose all future business within that network. Therefore, **rather than trust in a particular dealer, customers have trust in the network** to identify fraudulent or opportunistic dealers (Coase, 1988) and exact punishment in the form of voice and exit to serve as incentives for firm behavior (Williamson, 2005).

This institutional trust in a network (Williamson, 1993) would be a viable option for privacy online. Users and Web sites are plagued with the problem of identity and continuity — users have trouble identifying transgressions online and associating them with a particular Web site; Web sites have little incentive to modify their approach to privacy when the cost and consequences center on losing a single user. Within credible contracting, vulnerable parties need mutual confidence from a collective organizing structure (Williamson, 2002), and without the general social norms to govern privacy online, parties will need to rely on the institutional trust in a network [18].

Akerlof's suggestion to rely on brand and reputation could work online by creating a network that identified Web sites, allowed brands and reputations to develop based on feedback of users and experts, and gave users and Web sites a mechanism to signal preferences at a fine grain level. Similar to Angie's List (angieslist.com — "reviews you can trust" for local merchants) or Trip Advisor (tripadvisor.com — reviews for hotels and travel), users would have a mechanism to check on the reputation of a Web site in meeting privacy expectations before entering into a transaction.

This online network around privacy in the form of a Web site would parallel Kollack's rubber merchants and Williamson's diamond dealers by increasing the cost and consequences of fraud and opportunism. Rather than focusing on continuity within a single relationship, a Web site would risk discontinuing the relationships with a larger group of users on the network with a bad review or reputation. In addition, the site would provide signals to the Web sites for the preferences of users and allow practices of Web sites to be accessible to users.

Within the online economic environment, where parties are vulnerable in the exchange, reputation (Akerlof, 1970), trust (Kollock, 1994), and credible contracting (Williamson, 2002, 2005) become critical. In fact, trust is more likely in situations, such as the rubber market, where information asymmetries introduce significant risks rather than in the rice market where information is available with lower risk (Kollock, 1994). As noted by Kollock, "risk creates a breeding ground not only for trust but for exploitation as well" [19].

The shift from focusing on notice and choice governing simple market exchanges to relying on credible contracting where identity, repeated transactions, and trust govern the information exchange rewards firms who build a reputation around respecting privacy expectations. Importantly, firms must now understand the evolving privacy expectations of uses for different contexts rather than rely upon adequate notification. Fortunately, privacy scholarship has already identified how users develop privacy expectations within particular contexts, and the associated tactics for firms to meet privacy expectations are outlined below.

Developing a privacy reputation: Privacy in practice

Similar to the market for rubber, privacy scholarship reinforces the need to develop rules and expectations within a particular relationship rather than rely on adequate notification through an explicit contract. Online "transactions are governed by norms", and both users and business must conform to those norms (Sloan and Warner, 2013). A growing body of research has focused on privacy as being contextually defined, thereby examining privacy norms within a specific set of relationships or contexts (Nissenbaum, 2004, 2009; Solove, 2002, 2006; Martin, 2011, 2012; Sloan and Warner, 2013). Contextual approaches view privacy expectations as the developed rules about when, why, and how information is exchanged within a particular community or relationship.

More specifically, irrespective of notice and choice, individuals consider the consequences of the use and misuse of information for a particular information exchange to identify the appropriate set of privacy rules and expectations for that context [20]. This rule–utilitarian approach — whereby rules and norms are developed with the costs and benefits to the many stakeholders in mind (Mill, 1863; Gustafson, 2008; Armstrong, 2004) — explains how individuals develop privacy norms within particular relationships. The privacy expectations are developed and evolve within a community for a particular purpose, and individuals take into consideration the consequences of a rule in developing such privacy norms and expectations.

A shift from explicit contracts to informational norms also changes the responsibility of the firm from adequate notification to supporting the cost–benefit analysis of privacy rules. For privacy online, a rule–utilitarian approach would suggest that Web sites and users develop privacy expectations taking into consideration the benefits and costs of a particular practice. The rules would not necessarily be grounded in written contracts, and the Web site would take on the burden to manage these norms and expectations as the firm is in the best position to do so given their knowledge and power in the relationship.

Privacy in practice in scholarship

This pragmatic, rule–utilitarian model is part of a general cross–disciplinary trend to identify privacy rules based on the consequences within a particular relationship or context rather than conformance to an explicit contract. Within information systems, the 'privacy calculus' suggests that individuals assess outcomes as a result of providing information (Culnan and Armstrong, 1999; Dinev and Hart, 2006; Li, *et al.*, 2010). Consumers perform a risk"benefit analysis (Malhorta, *et al.*, 2004) which can be internalized into a privacy norm (Xu, *et al.*, 2009). Individuals are then seen as trading information in exchange for specific benefits (Westin, 2003) as well as considering expected harms (Calo, 2013). Similarly, privacy pragmatists (Westin, 2003) are defined as those individuals willing to permit the use of their information (a) if they are given a rationale and tangible benefit; and, (b) if they sense that safeguards are in place to prevent misuse [21]. This negotiation is also framed as the willingness–to–sell versus the willingness–to–protect information online in experimental studies (Acquisti and Grosslags, 2005).

Within public policy, the Federal Trade Commission (FTC) considered a consequences–based model that attempts to identify specific harms in order to develop privacy norms to deemphasize notice and choice as a goal (Beales and Muris, 2008). While critics find this particular rule–utilitarian approach too focused on economic and physical harms, as well as being reactive to harms that have been established rather than prescriptive [22], this harm–based model — and not notice and choice — served as the basis of the FTC's popular Do Not Call List (Beales and Muris, 2008) by allowing for different rules to govern different contexts.

This pragmatic approach is found within legal scholarship with the use of tort law on issues of privacy. Privacy through tort law is positioned against property approaches to privacy, including FIP and the current notice–and–choice approaches (Bambauer, 2012) [23]. Tort law focuses on broader societal interests and is a more pragmatic approach to privacy in that the rules are constructed with consequences in mind (Calo, 2011). For example, an examination of consequences guides rules around frictionless sharing (McGeveran, 2012), Facebook and Google (Tene and Polonetsky, 2012), and the use of utility bills for credit worthiness (Bambauer, 2012). In addition, Solove (2002) explicitly takes a pragmatic approach to conceptualizing privacy by allowing the privacy norms to develop within a particular context rather than residing as an objective definition outside a particular situation.

Finally, privacy as contextual integrity (Nissenbaum, 2004, 2009) places the concept of negotiated privacy norms at the forefront in a conceptual framework. Within privacy as contextual integrity, rules about how information flows within specific contexts constitute expectations of privacy, and these rules are developed based on the potential harms and benefits to the context and the individuals in the context. As Nissenbaum notes, privacy norms should "define and sustain essential activities and key relationships and interests, protect people and groups against harm, and balance the distribution of power" (Nissenbaum, 2010). Similarly, privacy as a social contract within business ethics builds on Nissebaum's theory and suggests specifically that privacy norms are developed with consequences in mind (Martin, 2012).

Privacy in practice is not synonymous with assuming that individuals *relinquish privacy* in order to gain something in return as with privacy as a commodity or the privacy paradox or some readings of a privacy calculus, privacy as a second exchange, and privacy pragmatists. In other words, individuals can be mistakenly seen as giving up some measure of privacy to benefit from a transaction (*e.g.*, customizing products, using electronic health records, or having books suggested online) rather than negotiating over the privacy norm itself [24]. Instead, actors within a context negotiate what the privacy rules will be while

retaining every expectation of privacy. More specifically, the very function of privacy norms is developed within a context using the cost–benefit analysis [25].

Privacy in practice analysis

A rule–utilitarian approach, as described above, shifts the focus from controlling information as property towards identifying the mutually beneficial, implicit rules developed within specific situations or contexts. **Importantly for firms, managing privacy in practice shifts the firm's responsibility from adequate notice to identifying and managing the cost–benefit analysis within a specific context**. Figure 2 illustrates the theoretical relationship between harms and benefits governing privacy in practice. Privacy scholarship suggests that individuals who develop privacy rules consider the magnitude of the harm, the probability of the harm being realized, and the expected benefits of sharing information. The concepts are briefly explored below to illustrate how a pragmatic approach to privacy in practice would be researched in the future.

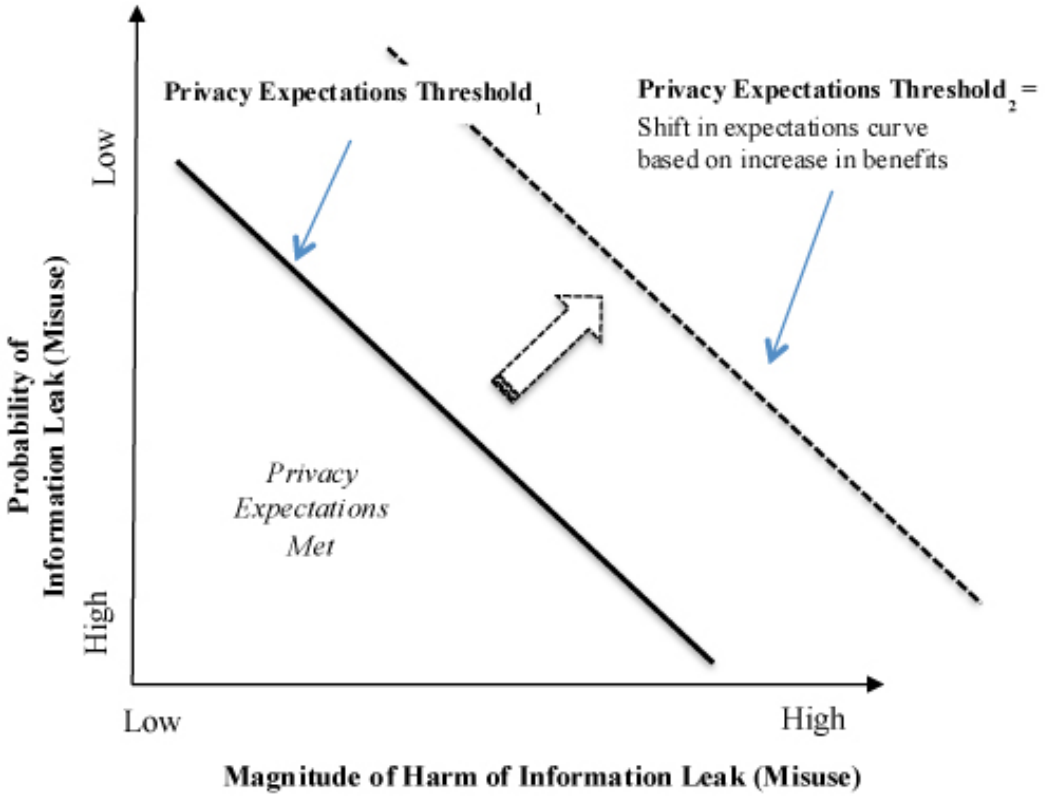

Figure 1: Privacy in practice.

Magnitude of potential harm. Traditionally, privacy rules develop to limit the potential harm that occurs from the misuse of information. Prosser (1960) famously outlined four types of harms that are still used to explain individual harms from privacy violations: intrusion, disclosure of embarrassing facts, placing information in a false light, and appropriation. Less quantifiable harms are more difficult to systematically address such as embarrassment and humiliation (Solove, 2006), the inhibition of an individual based on how others might react and judge (Nissenbaum, 2004), and reputational and breaches of trust (Bambauer, 2012). Calo (2013) views these more–difficult–to–quantify–harms as subjective: just as assault is apprehension of battery, individuals can be harmed by the *perception* of observation as largely an apprehension of unwanted information driven injury. For example, the harm caused by Facebook Sponsored Stories would fall under Calo's subjective harm category as individuals would have difficult attributing monetary damages to harm from discrimination, lost jobs, lost companionship, etc. Tene and Polonetsky (2012) summarize the incorporation of potential harms in developing privacy rules for a particular context by suggesting the question, "does information flow harm users, interfere with self–determination, or amplify undesirable inequalities in status, power, and wealth?" [26]

Probability of information leak. The potential harms outlined above are not a certainty; harms are realized when information is used in a new manner or accessible to new people. The possibility of harm from an information exchange is a function of the degree that the information exchange is protected from misuse,

such as improper use, unauthorized use, and unauthorized access (Smith, *et al.*, 1996; Malhorta, *et al.*, 2004). For example, a users' name, e–mail, and address details were sent to application developers for Google's Android without the knowledge or choice of the user and without even a request from the developers (Tung, 2013). Similarly, photographs posted to a select group of friends can be resent widely thereby escaping the assumed boundaries of the picture's context (Hill, 2012).

The probability of an information leak varies by the context. Showing a picture to a friend within a house carries a lower chance of information leakage compared to posting a picture on a social network site. Similarly, encrypted data is highly protected with low probability of information being leaked. Within privacy scholarship, maintaining anonymity lessens the degree an individual is identifiable and increases the degree to which their actions are protected. For example, one who is perfectly anonymous need not worry about their actions (Solove and Schwartz, 2011) and enjoys the benefits of being in a protected environment. Within law and information technology scholarship, k–anonymity is used to identify the number of factors to include in a record in order to maintain the degree of anonymity required for a particular situation (Sweeney, 2000). In other words, k–anonymity describes the level of difficulty in identifying individuals, where k represents the number of individuals to whom a pattern of data fits. Detailed data tends to lower the value of k (Spiekermann and Cranor, 2009; Sweeney, 2000). Solove and Schwartz (2011) note that true anonymity has become a myth — with data becoming quickly re–identified (Sweeney, 2000). Instead, the ability to identify should be thought of as a continuum with fully anonymous and fully identified being at two ends of a continuum.

While the use of anonymity as a proxy for privacy is flawed (Smith, *et al.*, 2011), the desire to be *obscure* or hidden from view remains a driver of privacy expectations and protects information from possible leaks. Rather than focus only on identifiability, individuals online and off–line search for a state of obscurity where it is "unlikely that the observation would lead to the deduction of all relevant bits of information necessary to comprehend our actions or utterances" (Hartzog and Stutzman, 2010). For example, individuals actively manage an optimal level of obscurity within particular relationships to protect their actions from leaking to outsiders. The key to obscurity is keeping relevant information away from those it was not intended or avoiding information being leaked.

		Possible Harm from 2nd Use of Information	
		Low	High
Degree of Obscurity	Low	'Public' Information – easily accessible and inconsequential	Vulnerable Information – Sensitive information and easily accessed or attributed to an individual
	High	Over-Protected/Inefficient Information – valuable information that could be more accessible or less obscure	Secure Information– valuable, potentially harmful information which is hidden from view or secondary use.

Figure 2: Relationship between harm and obscurity.

Meeting privacy expectations. Greater potential harms require greater protections to decrease the possibility of harms being realized as depicted in Figure 1. Obscurity and potential harm are related in that an increase in obscurity is necessary with greater potential harms in order for a norm to be seen as meeting privacy expectations. An individual could share innocuous information with a friend using encryption software with a low potential harm and high obscurity. Similarly, an individual could write their social security number on a piece of paper and leave it on the counter of the grocery store. Sensitive data, with an increase in potential harm, requires more protection in the form of obscurity or information friction in order to meet privacy expectations and not feel threatened. In Figure 1, an increase in potential harm requires an increase in obscurity to remain within privacy expectations, and an increase in potential harm on the horizontal access without additional obscurity could cause a scenario to move outside privacy expectations. Likewise, a decrease in obscurity for the same potential harm also moves the norm to outside privacy expectations. For example, medical records, names of rape victims, and the U.S. President's logistical plans are considered potentially harmful if leaked and warrant additional protections so that individuals do not feel threatened and privacy expectations are met. Similarly, privacy research focusing on privacy concerns rather than privacy expectations focus primarily on this 'threat of harm' analysis (Smith, *et al.*, 1996; Smith, *et al.*, 2011).

Benefits of disclosing information. Individuals do not only focus on privacy concerns and, all things being equal, individuals take into consideration the benefits or utility of the information exchange when assessing privacy expectations. Beales and Muris (2008) outline the many reasons why individuals' expectations of

privacy are met even when sharing sensitive data. Individuals disclose seemingly sensitive information to decrease the overall risk of fraud, facilitate credit–granting decisions, locate individuals, monitor official conduct, and protect people from predators (Beales and Muris, 2008). In a similar analysis, the use of utility bills to supplement credit reports for credit decisions may benefit the poor who have good payment histories and may not have any credit scores (Bambauer, 2012). The cost–benefit analysis requires careful analysis within a particular context. Bambauer illustrates the complicated analysis around privacy rules where the benefits of a right to be forgotten must be weighed against the possible harms in allowing domestic violence perpetrators to cleanse their records (Bambauer, 2012). Importantly, these benefits are not only monetary — in fact, monetary payments of information disclosure are of no significance when the information captured is deemed relevant to the context (Li, *et al.*, 2010). Individuals recognize the non–monetary benefits to sharing information, such as an interest in being able to associate (Swire, 2012) as well as to share information in order to develop relationships and personalities (Nissenbaum, 2004).

Implications for practice and research

Given Figure 1, firms have multiple tools at their disposal to move a scenario within privacy expectations: (1) make the exchange more obscure thereby decreasing the probability that the information will be leaked; (2) decrease the possible harm that could come from a leakage by enacting 'do not use' rules that limit the use of data; and, (3) increase the benefit of the information exchange for the individual and the larger community to ensure the purpose of the information is understood. **All three options — increasing obscurity, decreasing harm, and increasing benefits — work to ensure that the information exchange is within privacy expectations without relying on notice and choice.**

1. Decrease harms. Specific 'do not use' policies help decrease the potential harm of information sharing (Bambauer, 2012; Peppet, 2010) such as antidiscrimination policies. By limiting the potential harm for individuals and the community through 'do not use' policies, firms effectively make meeting the privacy expectations of users more likely given Figure 2. The threat of unraveling, "when decisions to disclose are seen as a signal and shift the expectations of disclosure for everyone else" (Peppet, 2010), specifically harms those outside the immediate exchange. For example, if enough job applicants voluntarily submit to a drug test, then the default changes from no drug test to taking a drug test, and those that do not submit to a drug test are then seen to be hiding something. Similar problems exist in health insurance and preexisting conditions, employment and intent to become pregnant, and more recently, potential new hires and access to their Facebook account [27]. Along these lines, the World Economic Forum's report focuses on limiting the use of information rather than how information is collected in their report on rethinking personal data [28].

2. Increase obscurity. A number of tactics are available to make information less likely to be leaked while still disclosing information. Floridi (2006) uses the concept of information friction to describe the degree to which information is protected in a given situation. For example, hospitals with separate rooms for each patient would have greater friction than hospitals with only a curtain between patients. Information friction can be physical, technological, or social and captures the difficulty by which others can gather the relevant pieces of information or the degree to which information can leak out of a desired context. Both obscurity and friction capture the range that an individual and their relevant information are accessible and understandable to outsiders or *could become* accessible and understandable to others [29]. Separate, non–linked databases add to the obscurity of the information for Hartzog and Stutzman (2010), would add to the information friction of the situation for Floridi (2006), and make the individual less threatened in Figure 1. Similarly, having a conversation on an encrypted phone would add to both obscurity and friction. As summarized by a technology writer John Biggs, in a perfect world, individuals would be "susceptible to brute force attacks and social engineering, perhaps, but little else" (Biggs, 2012). While the world is not perfect, firms can move closer to the ideal by increasing user obscurity. For example, famil.io (a photo–sharing application) and Path (a social network site) are designed to limit sharing by default, making the product less prone to information leakage (Lunden, 2013; Perez, 2013a). Similarly, Apple introduced a robust approach to obscuring voice data whereby information is aggregated and then identifiers are deleted from the data (Etherington, 2013). The approach allows Apple to customize their product and improve their service while obscuring the data of users making leakage less probable.

3. Explain the benefits. Explaining the possible uses of the data to users has proven to be effective in meeting privacy expectations. U.S. Census response rates improve when the purpose of the questions is explained for society — but interestingly not merely when the benefit to the immediate individual is explained (Martin, 2006). Individuals regularly share information when it is known to benefit either themselves or others: sharing information between doctors is useful for the individual users (Martin, 2012) and disclosing information to credit bureaus is useful for the larger economic community (Beales and Muris, 2008).

While much maligned, tracking cookies are capable of capturing detail to improve users' experience online (Bambauer, 2012), and targeted advertising online is more effective than traditional advertising which "enables companies to offer consumers choices that better satisfy their preferences" (Beales and Muris, 2008; Beales, 2010). Finally, location tracking is useful for research purposes to track happiness, obesity, and traffic planning (Hotz, 2011). Within privacy research, explaining how monitoring is related to the job positively impacts perceptions of employee monitoring (Alder, *et al.*, 2007). And while 68 percent of

Americans reject tracking (Turow, *et al.*, 2009), targeted advertising is more acceptable if useful in matching the context and industry of the Web site (Goldfarb and Tucker, 2011).

Business has a role in ensuring their stakeholders do not feel threatened by developing privacy norms and expectations that are within the privacy expectations of the context. For example, privacy by design is an approach to respecting privacy that focuses on designing the technology — in this case, the Web site — with a particular set of privacy expectations embedded in the design (Rubinstein and Good, 2013). As noted by privacy scholar M. Ryan Calo, "You can write a lengthy privacy policy that few will read, or you can design the Web site in a way that places the user on guard at the moment of collection" [30]. Not only should the website be designed with the particular privacy norms in mind, but those value–laden design decisions should be clear to users through icons, cosmetic changes to the Web site, and reminders so that the user is 'nudged' (Acquisti, 2009) in directions of the agreed–upon norms.

Implications for privacy scholarship

Privacy scholarship relies on Fair Information Practices and notice and choice specifically to judge firms (Williams, 2006) and define a respondent's concern for privacy (Smith, *et al.*, 2011). This paper has suggested an alternative approach to privacy that relies on contextually defined privacy norms, which is supported across disciplines and has implications to privacy research. Privacy norms will depend on the context of the exchange and would need to be examined inductively within a particular practice. The privacy paradox is defined as when an individual expresses strong concerns about privacy but behaves in a contradictory way to those concerns by disclosing information (Smith, *et al.*, 2011; Xu, *et al.*, 2009). However, apparent inconsistencies between a particular practice and responses to an abstract concern about privacy may have an alternative explanation: the practice may be in line with the expectations of the contest as illustrated in Figure 1. Individuals can have a general concern about privacy while also reserving privacy expectations when disclosing information.

Second, the current governance structure — explicit contracts through notice and choice — relies on a disclosure fallacy: the belief that modifications to the information practices of a firm after disclosure are not a concern of individuals. The disclosure fallacy posits the act of disclosure as dispositive of relinquishing an interest in the use of an individual's information. However, this article suggests that individuals have an ongoing interest in how information is used beyond the initial disclosure of information. In other words, disclosure is not dispositive of relinquishing a right to privacy.

Third, as noted by Sloan and Warner (2013) in their critique of notice and choice and advocation for analyzing informational norms to govern a transaction, "merely to define a tradeoff is, of course, not necessarily to define an acceptable one" [31]. More work would need to focus on the inductive identification of privacy expectations, the normatively optimal set of privacy norms, and the gap to bridge the two points.

Finally, both Kollack and Coase suggest an additional onus on business ethics when prescribing government action. As summarized by Schwab (1989): "In our world of transaction costs, private parties do not eliminate externalities when the transaction costs of doing so exceed the benefits. Likewise, however, the costs of government intervention may exceed the benefits." Kollock also notes the problems with imposing rules and regulations to govern such exchanges. The negative consequences of an outside party giving guarantees exist because the "average level of interpersonal trust was significantly lower in the certain–quality condition compared to the uncertain–quality condition" [32]. "In fact, the more the state intervenes ... the more necessary (on this view) it becomes, because positive altruism and voluntary cooperative behavior atrophy in the presence of the state and grown in its absence." In other words, the more we have it [the state], the more we 'need' it, and the more we come to depend on it [33]. Instead, this paper illustrates an alternative governance mechanism may be a viable option to address privacy concerns online.

Conclusion

Notice and choice constitute a particular structure to govern transactions online. While aligned governance structures provide order, minimize conflict, and result in mutually beneficial solutions (Williamson, 2002; van Oosterhout, *et al.*, 2006), the current status of privacy online and the arguments here suggest that notice and choice have ceased to be viable amelioration of privacy concerns online. The existence of a misaligned structure — such as the current notice and choice regime for online privacy — is normal and expected within the messiness of a market economy. Small acts of rebellion against the current regime, such as the use of obfuscation technologies to hide from Web sites (Brunton and Nissenbaum, 2011), are the 'canaries in the coal mine' of misaligned governance mechanism and the associated social friction. Rather than be ignored, such market signals should be seen as an early opportunity to adjust the governance strategy by more alert, entrepreneurial firms (Kirzner, 1973).

In fact, theory suggests the current online environment may be an opportunity for firms to differentiate themselves in the marketplace. As Kollack notes, when the situation is correspondent and the exchange favors both parties, little chance exists for trust to develop. In other words, an increase in risk and vulnerability of one party creates an opportunity for trust. When uncertainty is low, commitment is low and exchange partners are less concerned with reputation and trust. However, "if uncertainty is high, actors will

enter into committed exchange relations with those partners who have shown themselves to be trustworthy" (Kollock, 1994). Exclusive exchange relationships are formed with higher commitment and greater trust only in an uncertain environment (Kollock, 1994). Not only are trusting relationships necessary in such an environment, an online environment is particularly fertile for such relationships to form.

Privacy online provides an example of how a Coasean analysis of an exchange can illuminate the determinants of a misaligned transaction. Rather than focus on government intervention as necessary, this paper proposed fixes to the current notice and choice governance structure as well as an alternative mechanism to guide private ordering in the development of trust, reputations, and repeated transactions. A transaction cost analysis may prove useful to addition ethical issues in business.

About the author

Kirsten Martin is an assistant professor of Strategic Management and Public Policy at the George Washington University's School of Business. She is the principle investigator on a three–year grant from the National Science Foundation to study online privacy. Martin has published academic papers in the *Business and Professional Ethics Journal, Journal of Business Ethics*, and *Ethics and Information Technology Journal* and is co–author of the textbook *Business ethics: A managerial approach*. She has written teaching cases for the Business Roundtable Institute for Corporate Ethics. Martin earned her B.S. Engineering from the University of Michigan and her MBA and Ph.D from the University of Virginia's Darden Graduate School of Business. Martin is also a member and the vice chair of the U.S. Census Bureau's National Advisory Committee for her work on privacy and the use of big data. Her research interests center on online privacy, corporate responsibility, and stakeholder theory.
E–mail: martink [at] gwu [dot] edu

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant Number number 1311823.

Notes

1. See U.S. Federal Trade Commission (2012a) "Protecting consumer privacy in an era of rapid change: Recommendations for business and policymakers", Federal Trade Commission's (2012b) "Fair information practice principles", and the White House's (2012) "Consumer data privacy in a networked world."

2. Calo, 2013, p. 1,029.

3. Over US$45B is spent annually on online retail (U.S. White House, 2012). The US$4B in digital advertising in 2010 (Hoy and Milne, 2010) will grow by 40 percent and overtake all platforms of advertising by 2016 (Olmstead, *et al.*, 2012).

4. Culnan and Bies, 2003, p. 326.

5. As noted by Culnan and Bies (2003, p. 326), "The second exchange is not new. Before customer databases existed, data from the second exchange were maintained in ledgers or in the proprietor's head".

6. Coase, 1937, note 7, p. 78.

7. This transaction is subject to the same analysis and expectations within transaction cost economics regardless of how much money changes hands. In addition, notice and choice were designed so as to replicate a user agreement or contract so a transaction cost analysis should be familiar to notice and choice advocates. In fact, the comparative analysis within transaction cost economics is particularly well–suited for this subject since the exchange of information has become the focal point of scrutiny and the current governance structure — notice and choice — has become the focal point of critiques.

8. Private ordering are the efforts of parties to the transaction to align incentives or craft governance structures that are better attuned to their exchange needs (Williamson, 2002, p. 172). For Williamson, private ordering is an alternative to public ordering which is a focus on rules of the game or constitutional economics (Williamson, 2002).

9. The average privacy policy is 2,464 words, written at the college–level, and falls somewhere between the Declaration of Independence (1,337 words) and the U.S. Constitution (4,440 words) (Coldewey, 2011).

10. http://www.wired.com/images_blogs/threatlevel/2012/05/sponsoredlawsuitfacebook.pdf.

11. Coase, 1937, p. 336.

12. Solove and Schwartz, 2011, p. 1,868.

13. Akerlof's last remedy — focusing on brand name and reputation — suggests a new governance mechanism for the information exchange which would replace relying on notice and choice and introduce trust and implicit rules to govern the exchange. This approach is addressed below.

14. This shift to the responsibility of Web sites asking for and using information is seen in surveys: 61 percent believe a law should exist to force sites to disclose what they know and 92 percent believe a right to undo should be law (Turow, *et al.*, 2009).

15. Kollock, 1994, p. 314.

16. Kollock, 1994, p. 319.

17. Williamson, 1993, p. 461.

18. Interestingly, Williamson also suggests institutional trust in a profession to mitigate vulnerability of parties and risk in the transaction as in the case of a doctor or a lawyer. Previously, only statisticians, academics, and engineers would have access to such large data sets of users and would need to adhere to a code of ethics for their given profession, thereby offering individuals the form of institutional trust suggested by Williamson (1993). boyd and Crawford (2012) note that such access to these data sets is no longer limited to professionals.

19. Kollock, 1994, p. 320.

20. Beales and Muris, 2008, p. 109.

21. Beales and Muris, 2008, p. 118, footnote 29.

22. FTC, 2010, p. 33.

23. "While privacy law scholars [preoccupied with controlling dissemination] automatically code all increases in personal data accumulation as a threat, tort scholars are open minded about the appropriate activity level so long as the activity is not posing undue risk" (Bambauer, 2012). Property–rights approaches to privacy in law are exemplified by the FIP and notice–and–choice in particular. Yet, privacy through property rights is problematic because the approach "prioritizes the autonomy and self–determinism of an information subject over competing autonomy interests of information holders and the societal interests in unencumbered information flow" (Bambauer, 2012).

24. For example, Beales and Muris (2008) frame Westin's privacy pragmatists as trading information for a clear rationale and benefits whereas Westin (2003) sees these pragmatists as giving up privacy. The difference is important as the former suggests that the privacy expectation is the result of a negotiated process (as is argued here) and privacy expectations exist after the disclosure of information. Alternatively, the latter frames privacy as a right that is purchased and given up, thereby forcing the individual to relinquish any interest going forward. Nissenbaum (2004) refers to this latter argument as the "anything goes fallacy" where privacy is mistakenly viewed as being given up in certain circumstances.

25. This is the very definition of rule–utilitarianism where social rules are developed given the consequences to various stakeholders. Rule–utilitarianism should not be conflated with simple consequentialism or act utilitarianism where a specific decision is judged given the cost–benefits analysis to the individuals. Rule–utilitarianism judges the precedent, rule, or norm being set by the consequences of the rule to a community and society.

26. Potential harm to a data subject can also be operationalized as the sensitivity of the data (*e.g.*, Beales and Muris, 2008) or as highly volatile information (Bambauer, 2012), where sensitivity is a function of the potential harm from the data's misuse. Medical records are considered sensitive due to the harm from the possible discrimination; bank records are sensitive due to the possible harm to the data subjects through fraud; sexual proclivities are considered sensitive due to the possible harm through embarrassment of the data subject. Data is not objectively sensitive and can change over time and context. For example, social security numbers are increasingly considered sensitive data as the potential for misuse and harm has increased over time (Martin, 2006). While social security numbers were once used on university identification cards and drivers' licenses, now social security numbers can be used for identity theft and fraud and considered some of the most sensitive types of data. More recently, data is considered sensitive when used to screen insurance applications, credit, and employment (Timberg, 2013).

27. For example, the state of Michigan prevents employers and schools from requiring social network site passwords (such as Facebook) from potential applicants (Kersey, 2012).

28. http://www.weforum.org/issues/rethinking-personal-data.

29. Individuals will seek obscurity both online and off–line if none is offered. Brunton and Nissenbaum explore the many types of *obfuscation* used in the online and off–line settings. Obfuscation is a tool to mitigate the impact of monitoring, aggregation, analysis, profiling, by adding noise to data to make collection

more ambiguous, confusing harder to use, and less valuable (Brunton and Nissenbaum, 2011).

30. Calo, 2013, p. 26; Tene and Polenstky, 2012.

31. Sloan and Warner, 2013, p. 14.

32. Kollock, 1994, p. 338.

33. Taylor, 1987, p. 168.

References

Alessandro Acquisti, 2009. "Nudging privacy: The behavioral economics of personal information," *IEEE Security & Privacy*, volume 7, number 6, pp. 82–85.
doi: http://dx.doi.org/10.1109/MSP.2009.163, accessed 10 December 2013.

Alessandro Acquisti and Jens Grosslags, 2005. "Privacy and rationality in decision making," *IEEE Security & Privacy*, volume 3, number 1, pp. 26–33.
http://dx.doi.org/10.1109/MSP.2005.22, accessed 10 December 2013.

George A. Akerlof, 1970. "The market for 'lemons': Quality uncertainty and the market mechanism," *Quarterly Journal of Economics*, volume 84, number 3, pp. 488–500.
doi: http://dx.doi.org/10.2307/1879431, accessed 10 December 2013.

G. Stoney Alder, Marshall Schminke, and Terry W. Noel. 2007. "The impact of individual ethics on reactions to potentially invasive HR practices," *Journal of Business Ethics*, volume 75, number 2, pp. 201–214.
doi: http://dx.doi.org/10.1007/s10551-006-9247-6, accessed 10 December 2013.

Julia Angwin, 2011. "Privacy study: Top U.S. Web sites share visitor personal data," *Wall Street Journal* (11 October), at http://blogs.wsj.com/digits/2011/10/11/privacy-study-top-u-s-websites-share-visitor-personal-data/, accessed 10 December 2013.

Melissa Armstrong, 2004. "Rule pragmatism: Theory and application to qualified immunity analysis," *Columbia Journal of Law & Social Problems*, volume 38, pp. 107–130, and at http://www.columbia.edu/cu/jlsp/pdf/Fall%202004/Armstrong381-A.pdf, accessed 10 December 2013.

Mika D. Ayenson, Dietrich J. Wambach, Ashkan Soltani, Nathaniel Good, and Chris J. Hoofnagle, 2011. "Flash cookies and privacy II: Now with HTML5 and ETag respawning" (29 July), at http://dx.doi.org/10.2139/ssrn.1898390, accessed 10 December 2013.

Jane Yakowitz Bambauer, 2012. "The new intrusion," *Notre Dame Law Review*, volume 88, number 1, pp. 205–523, and at http://scholarship.law.nd.edu/ndlr/vol88/iss1/5/, accessed 10 December 2013.

Solon Barocas and Helen Nissenbaum, 2009. "On notice: The trouble with notice and choice," *First International Forum on the Application of and Management of Personal Electronic Information*, at http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf, accessed 10 December 2013.

Howard Beales, 2010. "The value of behavioral targeting." *Network Advertising Initiative*, at http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf, accessed 10 December 2013.

J. Howard Beales and Timothy J. Muris, 2008. "Choice or consequences: Protecting privacy in commercial information," *University of Chicago Law Review*, volume 75, number 1, pp. 109–135.
doi: https://lawreview.uchicago.edu/sites/lawreview.uchicago.edu/files/uploads/75.1/75_1_Muris_Beales.pdf, accessed 10 December 2013.

John Biggs, 2012. "The privacy problem: We have met the enemy and he is us," *Tech Crunch* (5 March), at http://techcrunch.com/2012/03/05/the-privacy-problem-we-have-met-the-enemy-and-he-is-us/, accessed 10 December 2013.

Norman E. Bowie and Karim Jamal, 2006. "Privacy rights on the Internet: Self–regulation or government regulation?" *Business Ethics Quarterly*, volume 16, number 3, pp. 323–342.

danah boyd and Kate Crawford, 2012. "Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon," *Information, Communication & Society*, volume 15, number 5, pp. 662–679.
doi: http://dx.doi.org/10.1080/1369118X.2012.678878, accessed 10 December 2013.

Finn Brunton and Helen Nissenbaum. 2011. "Vernacular resistance to data collection and analysis: A political theory of obfuscation," *First Monday*, volume 16, number 5, at http://firstmonday.org/article/view/3493/2955, accessed 10 December 2013.

M. Ryan Calo, 2013. "Against notice skepticism in privacy (and elsewhere)," *Notre Dame Law Review*, volume

87, number 3, at http://scholarship.law.nd.edu/ndlr/vol87/iss3/3/, accessed 10 December 2013.

M. Ryan Calo, 2011. "The boundaries of privacy harm," *Indiana Law Journal*, volume 86, number 3, pp. 1,131–1,162, at http://ilj.law.indiana.edu/articles/86/86_3_Calo.pdf, accessed 10 December 2013.

Brian Carter, 2011. "The 7 biggest fan page marketing mistakes," *AllFacebook* (17 May). at http://allfacebook.com/7-biggest-fan-page-marketing-mistakes_b43011, accessed 10 December 2013.

Jacqui Cheng, 2011. "No opting out of Facebook turning your check-ins, likes into ads," *Ars Technica* (26 January). http://arstechnica.com/business/2011/01/no-opting-out-from-facebook-turning-your-check-ins-likes-into-ads/, accessed 10 December 2013.

Ronald H. Coase, 1988. "2. The nature of the firm: Meaning," *Journal of Law, Economics and Organization*, volume 4, number 1, pp. 19–32.

Ronald H. Coase, 1937. "The nature of the firm," *Economica*, New series, volume 4, number 16, pp. 386–405.

Devin Coldewey, 2011. "Examination of privacy policies shows a few troubling trends," *TechCrunch* (30 November), at http://techcrunch.com/2011/11/30/examination-of-privacy-policies-shows-a-few-troubling-trends/, accessed 10 December 2013.

A. Cooper and H. Tschofenig, 2011. "Overview of universal opt–out mechanisms for Web tracking," IETF draft (7 March), at http://tools.ietf.org/search/draft-cooper-web-tracking-opt-outs-00, accessed 10 December 2013.

Robert Cooter, 1982. "The cost of Coase," *Journal of Legal Studies*, volume 11, number 1, pp. 1–33.

Mary J. Culnan, 1993. "How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use," *MIS Quarterly*, volume 17, number 3, pp. 341–363.

Mary J. Culnan and Cynthia Clark Williams, 2009. "How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches," *MIS Quarterly*, volume 33, number 4, pp. 673–687.

Mary J. Culnan and Robert J. Bies, 2003. "Consumer privacy: Balancing economic and justice considerations," *Journal of Social Issues*, volume 59, number 2, pp. 323–342.
doi: http://dx.doi.org/10.1111/1540-4560.00067, accessed 10 December 2013.

Mary J. Culnan and Pamela K. Armstrong, 1999. "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Organization Science*, volume 10, number 1, pp. 104–115.
doi: http://dx.doi.org/10.1287/orsc.10.1.104, accessed 10 December 2013.

Tamara Dinev and Paul Hart, 2006. "An extended privacy calculus model for e–commerce transactions," *Information Systems Research*, volume 17, number 1, pp. 61–80.
doi: http://dx.doi.org/10.1287/isre.1060.0080, accessed 10 December 2013.

Robert C. Ellickson, 1989. "The case for Coase and against Coaseanism," *Yale Law Journal*, volume 99, pp. 611–630, and at http://digitalcommons.law.yale.edu/fss_papers/462/, accessed 10 December 2013.

Rip Empson, 2013. "Disconnect 2 brings more privacy to your browser, lets you block 2K+ sites From tracking your activity online," *TechCrunch* (17 April), at http://techcrunch.com/2013/04/17/disconnect-2-brings-more-privacy-to-your-browser-lets-you-block-2k-sites-from-tracking-your-activity-online/, accessed 10 December 2013.

Darrell Etherington, 2013. "Apple keeps anonymized voice data related to virtual assistant Siri for up to 2 years," *TechCrunch* (19 April), at http://techcrunch.com/2013/04/19/apple-keeps-anonymized-voice-data-related-to-virtual-assistant-siri-for-up-to-2-years/, accessed 10 December 2013.

Luciano Floridi, 2006. "Four challenges for a theory of international privacy," *Ethics and Information Technology*, volume 8, number 3, pp. 109–119.
doi: http://dx.doi.org/10.1007/s10676-006-9121-3, accessed 10 December 2013.

Avi Goldfarb and Catherine E. Tucker, 2011. "Privacy regulation and online advertising," *Management Science*, volume 57, number 1, pp. 57–71.
doi: http://dx.doi.org/10.1287/mnsc.1100.1246, accessed 10 December 2013.

Andrew Gustafson, 2008. "Utilitarianism and business ethics," In: Thomas Donaldson and Patricia H. Werhane (editors). *Ethical issues in business: A philosophical approach* Eighth edition. Upper Saddle River, N.J.: Pearson/Prentice Hall.

Il–Horn Hann, Kai–Lung Hui, Sang-Yong T. Lee, and Ivan P.L. Png, 2008. "Consumer privacy and marketing avoidance: A static model," *Management Science*, volume 54, number 6, pp. 1,094–1,103.
doi: http://dx.doi.org/10.1287/mnsc.1070.0837, accessed 10 December 2013.

Woodrow Hartzog and Frederic D. Stutzman, 2010. "The case for online obscurity," *California Law Review*, volume 101, number 1, pp. 1–49, and at http://www.californialawreview.org/assets/pdfs/101-1/01-HartzogStutzman.pdf, accessed 10 December 2013.

Kashmir Hill, 2012. "Internet freak–out over Google's new privacy policy proves again that no one actually reads privacy policies," *Forbes* (25 January), at http://www.forbes.com/sites/kashmirhill/2012/01/25/internet-freak-out-over-googles-new-privacy-policy-proves-no-one-actually-reads-privacy-policies/, accessed 10 December 2013.

Robert Lee Hotz, 2011. "The really smart phone," *Wall Street Journal* (23 April), at http://online.wsj.com/news/articles/SB10001424052748704547604576263261679848814, accessed 10 December 2013.

Mariea Grubbs Hoy and George Milne, 2010. "Gender differences in privacy–related measures for young adult Facebook users," *Journal of Interactive Advertising*, volume 10, number 2, at http://jiad.org/article130.html, accessed 10 December 2013.

Gordon Hull, Heather Richter Lipford, and Celine Latulipe, 2011. "Contextual gaps: Privacy issues on Facebook," *Ethics and Information Technology*, volume 13, number 4, pp. 289–302.
doi: http://dx.doi.org/10.1007/s10676-010-9224-8, accessed 10 December 2013.

Nicholas Jackson, 2011. "The next online privacy battle: Powerful supercookies," *Atlantic* (18 August), at http://www.theatlantic.com/technology/archive/2011/08/the-next-online-privacy-battle-powerful-supercookies/243800/, accessed 10 December 2013.

Patrick Gage Kelley, Joanna Bresee, and Lorrie Faith Cranor, and Robert W. Reeder, 2009. "A 'nutrition label' for privacy," *SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and Security*, article number 4.
doi: http://dx.doi.org/10.1145/1572532.1572538, accessed 10 December 2013.

Ben Kersey, 2012. "Michigan passes law to protect social network account protection bill," *Verge* (30 December), at http://www.theverge.com/2012/12/30/3817588/michigan-passes-social-network-account-protection-bill, accessed 10 December 2013.

Israel M. Kirzner, 1973. *Competition and entrepreneurship*. Chicago: University of Chicago Press.

Peter Kollock, 1994. "The emergence of exchange structures: An experimental study of uncertainty, commitment, and trust," *American Journal of Sociology*, volume 100, number 2, pp. 313–345.

David Kravets, 2012. "Judge rejects Facebook 'Sponsored Stories' lawsuit settlement," *Wired* (18 August), at http://www.wired.com/threatlevel/2012/08/facebook-settlement-rejected/, accessed 10 December 2013.

Han Li, Rathindra Sarathy, and Heng Xu, 2010. "Understanding situational online information disclosure as a privacy calculus," *Journal of Computer Information Systems*, volume 51, number 1, pp. 62–71.

Tom Loftus, 2011. "Study: Usability issues plague tools that limit online behavioral advertising," *Wall Street Journal* (31 October), at http://blogs.wsj.com/digits/2011/10/31/study-usability-issues-plague-tools-that-limit-online-behavioral-advertising/, accessed 10 December 2013.

Ingrid Lunden, 2013. "Dave Morin, CEO of Path: 'If Facebook is a Chevy, then we're a BMW'; 'Family friendly' network pushes 6M users, launches virtual goods," *TechCrunch* (21 January), at http://techcrunch.com/2013/01/21/dave-morin-ceo-of-path-says-if-facebook-is-a-chevy-then-were-a-bmw-as-family-friendly-network-pushes-6m-users-looks-to-launch-more-virtual-goods/, accessed 10 December 2013.

Naresh K. Malhorta, Sung S. Kim, and James Agarwal, 2004. "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Information Systems Research*, volume 15, number 4, pp. 336–355.

Florencia Marotta–Wurgler, 2011. "Some realities of online contracting," *Supreme Court Economic Review*, volume 19, number 1, pp. 11–23.

Elizabeth Martin, 2006. "Privacy concerns and the Census Long Form: Some evidence from Census 2000," *U.S. Census Bureau, Survey Methodology, number 2006–10*, at http://www.census.gov/srd/papers/pdf/rsm2006-10.pdf, accessed 10 December 2013.

Kirsten E. Martin, 2012. "Diminished or just different? A factorial vignette study of privacy as a social contract," *Journal of Business Ethics*, volume 111, number 4, pp. 519–539.
doi: http://dx.doi.org/10.1007/s10551-012-1215-8, accessed 10 December 2013.

Kirsten E. Martin, 2011. "TMI (Too Much Information): The role of friction and familiarity in disclosing information," *Business and Professional Ethics Journal*, volume 30, numbers 1–2, at http://faculty.cua.edu/martink/BPEJMartin2011.pdf, accessed 10 December 2013.

Jonathan Mayer, 2011. "Tracking the trackers: Where everybody knows your username," Center for Internet and Society, Stanford Law School (11 October), at http://cyberlaw.stanford.edu/blog/2011/10/tracking-trackers-where-everybody-knows-your-username, accessed 10 December 2013.

Jonathan Mayer and Avrind Narayanan, 2010. "Do not track: Universal Web tracking opt–out," *IAB Internet Privacy Workshop position paper* (5 November), at http://www.iab.org/wp-content/IAB-uploads/2011/03/jonathan_mayer.pdf, accessed 10 December 2013.

Aleecia M. McDonald and Lorrie Faith Cranor, 2008. "Cost of reading privacy policies," *I/S: A Journal of Law and Policy for the Information Society*, volume 4, number 3, pp. 541–565, and at http://moritzlaw.osu.edu/students/groups/is/files/2012/02/Cranor_Formatted_Final.pdf, accessed 10 December 2013.

William McGeveran, 2012. "The law of friction," *University of Chicago Legal Forum; Minnesota Legal Studies Research Paper*, 12–66, at http://ssrn.com/abstract=2192191, accessed 10 December 2013.

John Stuart Mill, 1863. *Utilitarianism*. London: Parker, son, and Bourn.

John C. Mitchell and Jonathan R. Mayer, 2012. "Third–party Web tracking: Policy and technology," *Proceedings of the 2012 IEEE Symposium of Security and Privacy*, pp.413–427. doi: http://doi.ieeecomputersociety.org/10.1109/SP.2012.47, accessed 10 December 2013.

Helen Nissenbaum, 2011. "A contextual approach to privacy online," *Daedalus*, volume 140, number 4, pp. 32–48, at http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf, accessed 10 December 2013.

Helen Nissenbaum, 2010. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, Calif.: Stanford Law Books.

Helen Nissenbaum, 2004. "Privacy as contextual integrity," *Washington Law Review*, volume 79, number 1, pp. 119–158.

Paul Ohm, 2013. "Branding privacy," *Minnesota Law Review*, volume 97, pp. 907–989, and at http://www.minnesotalawreview.org/wp-content/uploads/2013/02/Ohm_MLR.pdf, accessed 10 December 2013.

Scott R. Peppet, 2010. "Unraveling privacy: The personal prospectus and the threat of a full disclosure future," *Northwestern University Law Review*, volume 105, number 3, pp. 1,153–1,203, and at https://www.law.northwestern.edu/lawreview/v105/n3/1153/LR105n3Peppet.pdf, accessed 10 December 2013.

Sarah Perez, 2013a. "Private photo And video sharing service For families, Famil.io, is like a dropbox For memories," *TechCrunch* (22 March), at http://techcrunch.com/2013/03/22/private-photo-and-video-sharing-service-for-families-famil-io-is-like-a-dropbox-for-memories/, accessed 10 December 2013.

Sarah Perez, 2013b. "After getting booted from Apple's App Store, mobile privacy app Clueful returns on Android," *TechCrunch* (21 May). http://techcrunch.com/2013/05/21/after-getting-booted-from-apples-app-store-mobile-privacy-app-clueful-returns-on-android/, accessed 10 December 2013.

Alan R. Peslak, 2005. "An ethical exploration of privacy and radio frequency identification," *Journal of Business Ethics*, volume 59, number 4, pp. 327–345. doi: http://dx.doi.org/10.1007/s10551-005-2928-8, accessed 10 December 2013.

William L. Prosser, 1960. "Privacy," *California Law Review*, volume 48, number 3, pp. 383–423, and at http://www.californialawreview.org/assets/pdfs/misc/prosser_privacy.pdf, accessed 10 December 2013.

Jeffrey Rosen, 2012. "The right to be forgotten," *Stanford Law Review*, volume 64, pp. 88–92, and at http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten, accessed 10 December 2013.

Ira Rubinstein and Nathaniel Good, 2013. "Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents," *Berkeley Technology Law Journal*, volume 28, pp. 1,333–1,413, and at http://btlj.org/data/articles/28_2/1333-1414_Rubinstein&Good_11262013_Web.pdf, accessed 10 December 2013.

Stewart Schwab, 1989. "Coase defends Coase: Why lawyers listen and economists do not," *Michigan Law Review*, volume 87, number 6, pp. 1,171–1,198.

Richard H. Sloan and Robert Warner, 2013. "Beyond notice and choice: Privacy, norms, and consent," *Suffolk University Journal of High Technology Law*, at http://ssrn.com/abstract=2239099, accessed 10 December 2013.

H. Jeff Smith, Tamara Dinev, and Heng Xu, 2011. "Information privacy research: An interdisciplinary review," *MIS Quarterly*, volume 35, number 4, pp. 989–1,015.

H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke, 1996. "Information privacy: Measuring individuals' concerns about corporate practices," *MIS Quarterly*, volume 20, number 2, pp. 167–196.

Daniel J. Solove, 2006. "A taxonomy of privacy," *University of Pennsylvania Law Review*, volume 154, number 3, pp. 477–560, and at https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477%282006%29.pdf, accessed 10 December 2013.

Daniel J. Solove, 2002. "Conceptualizing privacy," *California Law Review*, volume 90, number 4, pp. 1,087–1,155, and at http://scholarship.law.berkeley.edu/californialawreview/vol90/iss4/2/, accessed 10 December 2013.

Daniel J. Solove and Paul M. Schwartz., 2011. *Information privacy law*. Fourth edition. New York: Wolters Kluwer Law & Business.

Sarah Spiekermann and Lorrie Faith Cranor, 2009. "Engineering privacy," *IEEE Transactions on Software Engineering*, volume 35, number 1, pp. 67–82.
doi: http://dx.doi.org/10.1109/TSE.2008.88, accessed 10 December 2013.

Kathy A. Stewart and Albert H. Segars, 2002. "An empirical examination of the concern for information privacy instrument," *Information Systems Research*, volume 13, number 1, pp. 36–49.
doi: http://dx.doi.org/10.1287/isre.13.1.36.97, accessed 10 December 2013.

Latanya Sweeney, 2000. "Simple demographics often identify people uniquely," *Carnegie Mellon University, Data Privacy Working Paper*, number 3, at http://dataprivacylab.org/projects/identifiability/paper1.pdf, accessed 10 December 2013.

Peter Swire, 2012. "Social networks, privacy, and freedom of association: Data empowerment vs. data protection," *North Carolina Law Review*, volume 90, number 5, pp. 1,371–1,416, at http://www.nclawreview.org/2012/10/social-networks-privacy-and-freedom-of-association-data-protection-vs-data-empowerment/, accessed 10 December 2013.

Michael Taylor, 1987. *The possibility of cooperation*. New York: Cambridge University Press.

Omer Tene and Jules Polonetsky, 2012. "Privacy in the age of big data: A time for big decisions," *Stanford Law Review*, volume 64, pp. 63–69, at http://www.stanfordlawreview.org/online/privacy-paradox/big-data, accessed 10 December 2013.

"Terms of Service; Didn't Read" (TOS;DR http://tosdr.org, accessed 10 December 2013.

Craig Timberg, 2013. "Web–connected cars bring privacy concerns," *Washington Post* (5 March), at http://articles.washingtonpost.com/2013-03-05/business/37453419_1_car-insurance-companies-new-cars-seat-belt, accessed 10 December 2013.

Liam Tung, 2013. "Google Play privacy slip–up sends app buyers personal details to developers," *ZDNet* (13 February), at http://www.zdnet.com/google-play-privacy-slip-up-sends-app-buyers-personal-details-to-developers-7000011249/, accessed 10 December 2013.

Joseph Turow, Jennifer King, Christopher J. Hoofnagle, Amy Bleakley, and Michael Hennessy, 2009. "Americans reject tailored advertising and three activities that enable it," at https://www.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf, accessed 10 December 2013.

U.S. Federal Trade Commission., 2012a. "Protecting consumer privacy in an era of rapid change" (5 March), at http://www.ftc.gov/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations, accessed 10 December 2013.

U.S. Federal Trade Commission., 2012b. "Fair information practice principles" (23 November), at http://www.gov/reports/privacy3/fairinfo.shtm

U.S. White House, 2012. "Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy," at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf, accessed 10 December 2013.

J. (Hans) van Oosterhout, Pursey P. M. A. R. Heugens and Muel Kaptein, 2006. "The internal morality of contracting: Advancing the contractualist endeavor in business ethics," *Academy of Management Review*, volume 31, number 3, pp. 521–539.

Alan F. Westin, 2003. "Social and political dimensions of privacy," *Journal of Social Issues*, volume 59, number 2, pp. 431–453.

Jan Whittington and Chris Jay Hoofnagle, 2012. "Unpacking privacy's price," *North Carolina Law Review*, volume 90, number 5, pp. 1,327–1,370.

Felicia Williams, 2006, "Internet privacy policies: A composite index For measuring compliance to the fair information practices," at http://ftc.gov/os/comments/behavioraladvertising/071010feliciawilliams.pdf.

Oliver E. Williamson, 2005. "The economics of governance," *American Economic Review*, volume 95, number 2, pp. 1–18.
doi: http://dx.doi.org/10.1257/000282805774669880, accessed 10 December 2013.

Oliver E. Williamson, 2002. "The theory of the firm as governance structure: From choice to contract," *Journal of Economic Perspectives*, volume 16, number 3, pp. 171–195.
doi: http://dx.doi.org/10.1257/089533002760278776, accessed 10 December 2013.

Oliver E. Williamson, 1993. "Calculativeness, trust, and economic organization," *Journal of Law and Economics*, volume 36, number 1, part 2, pp. 453–486.
doi: http://dx.doi.org/10.1086/467284, accessed 10 December 2013.

Oliver E. Williamson, 1981. "The economics of organization: The transaction cost approach," *American Journal of Sociology*, volume 87, number 3, pp. 548–577.
doi: http://dx.doi.org/10.1086/227496, accessed 10 December 2013.

Oliver E. Williamson, 1979. "Transaction–cost economics: The governance of contractual relations," *Journal of Law and Economics*, volume 22, number 2, pp. 233–261.

Oliver E. Williamson, 1975. *Markets and hierarchies, analysis and antitrust implications: A study in the economics of internal organization*. New York: Free Press.

Heng Xu, Cheng Zhang, Pan Shi, and Peijian Song, 2009. "Exploring the role of overt vs. covert personalization strategy in privacy calculus," *Academy of Management Proceedings* (August Meeting Abstract Supplement), pp. 1–6.
doi: http://dx.doi.org/10.5465/AMBPP.2009.44249857, accessed 10 December 2013.

Editorial history

Received 21 August 2013; revised 11 November 2013; accepted 10 December 2013.

Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online
by Kirsten Martin.
First Monday, Volume 18, Number 12 - 2 December 2013
http://firstmonday.org/ojs/index.php/fm/rt/printerFriendly/4838/3802
doi:10.5210/fm.v18i12.