Consumers: The Missing Piece in a Piecemeal Approach to Privacy

Clark D. Asay

Attorney, Wilson Sonsini Goodrich & Rosati
650 Page Mill Road
Palo Alto, CA 94306
cdasay@stanfordalumni.org

Abstract

Under the current US regime, consumers have inadequate knowledge and control regarding how companies disclose their personal information to third parties. Consisting of industry-specific and state laws, ad hoc FTC enforcement, and self-regulation, this piecemeal approach to privacy leaves consumers in most cases with little actual knowledge about who will receive their information and how they will use it. In order to address this problem, this paper proposes a federal law that would require companies to provide consumers with notice describing in detail the intended third party recipients and their proposed uses, and a choice as to whether or not the company may disclose the personal information to such third parties. The law would be backed with a private right of action.

Introduction

In order to participate in the commercial world, consumers must often disclose vast amounts of sensitive personal information into a marketplace of data exchange they neither understand nor control. In a recent study, for instance, sixty-seven percent of consumers surveyed felt that they have lost all control over how companies collect and use their personal information.[1] Unlike other industries such as law, banking, and the medical professions, which provide ethical requirements of confidentiality with respect to clients' information, consumers enjoy no such safeguards. Concerns regarding who other than the initial recipient may have access to personal information, and how they will use it, naturally result.

The United States approaches this dilemma with a mix of legislation and self-regulation. On the legislation front, Congress has implemented a number of sectoral laws designed to address specific industries and their handling of consumer's personal information. The Federal Trade Commission (FTC) plays a role in enforcing these laws as well as monitoring privacy issues under Section 5 of the FTC Act. In addition, some states have enacted laws governing the handling of personal information. In terms of self-regulation, some commercial actors have developed and implemented "best practices" to help protect consumer privacy.

At least one key component significantly lacks in this piecemeal regime, however: consumers' power to police their own information. While the current US regime in certain cases provides consumers with some notice and choice regarding third-party disclosure of their personal information—typically as part of a blanket opt-in/opt-out approach—such notice and choice remains deficient because the consumer receives little to no information about who specifically will receive their information and how they will use it. To help bridge this gap, this paper proposes federal legislation that would require companies to provide consumers with notice and choice regarding the specific third party recipients and their intended uses. The law would also provide consumers with a private right of action to enforce their rights under the law.

The paper proceeds as follows: it first examines the current US approach to the issue of third-party disclosure, and highlights the problem that, even in the typical best-case scenario, consumers remain uninformed about who specifically will have access to their information and how they will use it. The paper then goes on to propose a system of notice and choice that would give consumers actual knowledge with respect to third-party disclosure, as well as a means to prevent such disclosure and use in the first place. The paper concludes by examining the proposal's advantages and potential drawbacks.

The Current US Regime

The most important aspects of both the legal and self-regulatory components of the US regime governing consumer personal information and third party disclosure are set forth below.

[1] Turow, J., King, J., Hoofnagle, C.J, Bleakley, A. and Hennessy, M. 2009, Americans Reject Tailored Advertising and Three Activities that Enable It. Available at SSRN: http://ssrn.com/abstract=1478214.

Sectoral Laws

Unlike Europe and many other parts of the world that have adopted comprehensive privacy legislation, the US has adopted several sectoral laws that target specific industries and types of personal information. Consequently, if a company does not fall within that specific industry, or if the type of personal information covered by the law is not involved, the sectoral law does not apply to either the entity or the information.

For instance, the Health Insurance Portability and Accountability Act ("HIPAA") only applies to "covered entities" (e.g., health plans, health care providers, health care clearinghouses and, in some cases, business associates of the same) that have access to a person's protected health information.[2] The Fair Credit and Reporting Act ("FCRA") covers entities that compile or use "consumer reports" (i.e., information regarding a person's credit, character, reputation, personal characteristics, or mode of living).[3] The Gramm-Leach-Bliley Act ("GLBA") limits itself to "financial institutions" (i.e., entities significantly involved in financial activities as defined under the Act) that handle non-public financial information.[4] And the Children's Online Privacy Protection Act ("COPPA") covers operators of commercial websites and online services directed to children under the age of 13, or such entities that knowingly collect personal information of children under the age of 13. [5]

A number of these industry-specific laws require covered entities to provide forms of notice and choice to affected persons before disclosing those persons' covered information to third parties. COPPA, for instance, requires affected entities to post an online privacy policy depicting how they collect, use, and disclose personal information, and to give the parents of children a choice as to whether the child's personal information may be disclosed to third parties.[6] The GLBA similarly requires notice to be provided about an affected entity's collection, use and disclosure practices, as well as an opt-out of some sharing of personal financial information with non-affiliated third parties.[7] HIPAA requires covered entities to use protected health information only for purposes of treatment, payment, or operations; otherwise, the covered entity must obtain specific opt-in authorization that details the information to be disclosed, the purposes of disclosure, and the entity to which disclosure will be made. Under HIPAA, consumers have a right to receive an accounting of the third-party disclosures of their personal information.[8]

Finally, under FCRA, users of consumer reports must give the subjects of such consumer reports notice and the opportunity to review the information in them when and if such user takes an adverse action based on that information.[9]

In terms of privacy, several problems arise with this sectoral approach. Perhaps most obviously, the laws only cover certain types of information and entities, thus leaving many other types of sensitive information and business entities unaccountable. Furthermore, with the exception of HIPAA, while the laws do require some amount of notice and choice before the covered entities may disclose the information to third parties, this notice and choice comes in the form of a blanket opt-in/opt-out approach. Consequently, the consumer does not actually know specifically who will receive their information and how such third parties will use it, thereby leaving the consumer with little or no control over their information. Last, with the exception of FCRA, none of these statutes include a private right of action, so consumers must rely on either the FTC or state attorney generals to protect their interests under the laws.

The FTC

In addition to helping enforce these sectoral laws, the FTC regulates privacy issues through Section 5 of the FTC Act. Under this Act, the FTC investigates and brings actions against companies that engage in "unfair" or "deceptive" trade practices. "Unfair trade practices" are defined as commercial conduct that (i) causes (or is likely to cause) substantial injury to consumers (ii) that consumers cannot reasonably avoid themselves, and (iii) without offsetting benefits to consumers or competition.[10] "Deceptive trade practices" are defined as commercial conduct that includes false or misleading claims, or claims that omit material facts.[11] With respect to deceptive trade practices, consumer injury does not need to be present; the mere fact that a company has engaged in such practices is actionable.

What constitutes a deceptive or unfair trade practice has evolved over time, ranging from implementing insufficient security measures given the sensitivity of the information involved, to companies stating certain privacy practices in their privacy notices while not actually following them.[12] However, to date the FTC has not brought deceptive or unfair trade practice actions against companies for failure to give notice and choice to consumers regarding disclosure of their information to third parties.[13] The FTC has brought actions against companies for failure to abide

[2] FTC. 2009. Summary of the HIPAA Privacy Rule. Available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
[3] 15 U.S.C. § 1681a.
[4] FTC. 2009. In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act. Available at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus53.shtm.
[5] FTC. 2009. Drafting a COPPA-Compliant Privacy Policy. Available at http://www.ftc.gov/coppa/.
[6] *Id.*
[7] FTC, *supra* note 4.
[8] FTC, *supra* note 2.
[9] FTC. 2009. Notice to Users of Consumer Reports: Obligations of Users Under FCRA. Available at http://www.ftc.gov/os/2004/11/041119factaapph.pdf.
[10] Swire, P., and Bermann, S. 2007. Information Privacy, 70. York, Maine: International Association of Privacy Professionals.
[11] *Id.*
[12] *See* FTC. 2009. Enforcement Cases. Available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.
[13] *Id.*

by their stated practices regarding third party disclosure,[14] but none of the actions to date make clear that notice and choice are necessary in the first place.

Furthermore, even if it is likely that a company collecting sensitive personal information and disclosing it to third parties without notice and choice would eventually incur the FTC's displeasure, if current trends held true such FTC enforcement would still not achieve the ideal level of notice and choice: that the consumer receive notice and choice similar to what is called for in HIPAA (i.e., identification of specific third parties and their intended uses), rather than as part of a blanket opt-in/opt-out regime that in fact provides consumers with little real information. Providing this type of notice and choice would go a long way in instilling confidence in consumers regarding where their information resides, who has it, and how such third parties are using it. Requiring companies to be more accountable may also prevent abuse.

State Law

State law also provides little reason for comfort from a consumer perspective. California's "Shine the Light Law", for instance, theoretically gives consumers greater control over their information by requiring covered companies to disclose their information-sharing practices to consumers, and, upon request, to provide consumers with a list of companies with which they have shared the consumer's information for marketing purposes.[15]

However, such laws are not widespread; at the time of this writing, California is the only state to have adopted such a law.[16] Utah has adopted laws requiring certain companies to disclose to consumers what types of information they may disclose to third parties, but the laws say nothing about consumer choice in the matter.[17] Furthermore, even under the California law, if companies provide the consumer with an opt-out or opt-in, then such companies are exempt from the rest of the law and need not disclose to consumers the companies with which the party shared their information.[18] Last, even if the consumer somehow obtained access to the list of companies with which the initial company shared the information, the law does not provide any recourse to the consumer, i.e., consumers have no legal right to require that the third party stop using or disgorge their information.

Most states do not even go so far as to require that companies develop privacy policies, let alone requiring informed notice and choice. California does require online companies to post a privacy policy indicating their information and disclosures practices.[19] Connecticut also requires a privacy policy to be posted in the event that an entity collects social security numbers.[20] However, neither of these state statutes require notice and choice about the specific third parties to be included in the privacy policies. Under state law, then, consumers remain uninformed about who actually will receive their information and how specifically the third parties may use it.

Self-Regulation

Aside from the legal regime, self-regulation also constitutes an important mechanism in the US by which companies attempt to regulate privacy issues themselves. Because consumers have become increasingly wary of providing their personal information to companies for fear of theft, misuse, or, simply, the unknown, many companies have responded by developing and adopting privacy "best practices," joining privacy "seal" programs such as TrustE,[21] or joining privacy alliances such as the Online Privacy Alliance ("OPA").[22]

In general, such alliances and seal programs require the companies to abide by certain principles. In terms of personal information and privacy, these principles typically require companies to provide consumers notice when disclosing personal information to third parties for purposes other than for which the company collected the information, and choice regarding such disclosure in the form of an opt-in or opt-out.

Two clear drawbacks to the self-regulation approach become obvious: adequacy and enforcement. That is, given companies' self-interest in retaining flexibility with respect to the personal information, it is unclear that a self-regulatory approach gives companies the right set of incentives to provide consumers with adequate protection and control. Furthermore, the self-regulation approach relies primarily on companies regulating their own behavior.

And, as with the other pieces of the US regime, even if companies do abide by these so-called "best practices," these best practices regarding notice and choice do not live up to their namesake. A best practice from the consumer's point of view would include consumers receiving notice and choice regarding who specifically is receiving their information and how that company will use it, rather than merely a general notice that unidentified third parties may in the future receive and use their personal information in manners similarly unknown.

---

[14] *See* FTC. 2004. Gateway Learning Settles FTC Privacy Charges. Available at http://www.ftc.gov/opa/2004/07/gateway.shtm.

[15] Privacy Rights Clearinghouse. 2004. California's "Shine the Light" Law Goes into Effect Jan. 1, 2005. Available at http://www.privacyrights.org/ar/SB27Release.htm.

[16] Privacy Rights Clearinghouse. 2009. Fact Sheet 4(a): California's "Shine the Light" Law. Available at http://www.privacyrights.org/fs/fs4a-shinelight.htm#10.

[17] *See* National Conference of State Legislatures. 2009. Selected State Laws Related to Internet Privacy. Available at http://www.ncsl.org/default.aspx?tabid=13463#isp.

[18] *See supra* note 15.

[19] *Id.*

[20] *Id.*

[21] *See generally* http://www.truste.com/.

[22] *See generally* http://www.privacyalliance.org/.

The Proposal

The realities of the current system thus seem less than inspiring: With the exception of protected health information under HIPAA, even in the best case scenario when notice and choice are given, consumers must either opt-out or withhold their consent, or, in the event that they opt-in or fail to opt-out, they remain without specific information about who will have access to their information and how such third parties will use it. Eventually, consumers may become aware of who, in fact, does have their information through an array of e-mails, marketing, and other contacts they receive, but they remain in the dark about how those third parties received their information in the first place, and how they may otherwise use the information. Furthermore, they have no legal means to force the party to disgorge their personal information or prevent further disclosure. This scenario hardly inspires confidence.

To help combat this problem, this paper proposes a federal law that would require companies to provide notice and choice to consumers that describes the intended third party recipients and their uses, as well as providing consumers with a private right of action to protect their interests under the law. The specifics of the proposal follow.

Definitions

Before proceeding to the law's mechanics, a few key definitions are necessary.

Personal Information. The proposed law would only apply to "personal information" that companies collect and propose to disclose to third parties, and not aggregated or anonymized information. What constitutes personal information is not as straightforward as it might seem. For instance, the EU Directive defines "personal data" quite broadly, in a manner that may include information that a company arguably would not be able to use to actually identify a person:

> '[P]ersonal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[23]

Under one interpretation of this definition, it may not even be necessary to be able to identify the person from the related information, so long as the information is related to an identified person in some way.

Other laws, such as the California data security breach act, define personal information as the name of an individual in combination with one of a number of other types of sensitive information (e.g., credit card number).[24] Such laws limit the relevant law's scope by requiring not only personal information (e.g., a name), but also highly sensitive information that, when improperly disclosed and combined with an individual's name, may pose a direct financial or security threat to the person.

This paper takes a position in between these two extremes and defines personal information similarly to how the US Executive Branch has defined it:

> Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.[25]

This definition has the advantage of avoiding the excessive breadth of the European definition, remaining consistent with how other important players in the US already define personal information, while achieving the definition's primary goal: to limit the law's application to that information which is linked or could readily be linked to an identifiable person.

Disclosure to Third Parties. Not all disclosures to third parties would trigger the law's effects. For instance, disclosing the information to third parties that perform services solely on behalf of the original recipient of the information (and do not use the information for their own purposes or for purposes other than for which the information was originally collected) would be exempt from the law. The law would only apply when and if the original recipient disclosed the personal information to the third party for a secondary use of the information, i.e., a use beyond the purposes for which the personal information was originally submitted.

Consequently, if a consumer submitted personal information to a company, and the submission was made for the purpose of disclosure to and use by specific third parties, then the law would not apply. However, if a consumer submitted personal information to a company for a specific purpose, and the company disclosed that information to a third party to process it solely on its behalf

[23] Article 2 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data. Available at http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_28.

[24] Brelsford, J. 2003. California Raises the Bar on Data Security and Privacy. Available at http://library.findlaw.com/2003/Sep/30/133060.html.

[25] *See* http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf. *See also* U.S. Department of Commerce, Office of the Chief Information Officer. 2009. Electronic Transmission of Personally Identifiable Information. Available at http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/PROD01_008240#P46_1812.

(i.e., not for the third party's own use), but for a use other than the reason the consumer initially submitted the information, then the law would apply.

This limitation is important in order to avoid interrupting the flow of information necessary to achieve the consumer's purposes in disclosing their personal information in the first place. Hence, so long as the information is being used as the consumer intended, the law's effects remain dormant. Once companies begin to explore the possibility of using the personal information outside of the original intent, however, the law would apply.

The Mechanics

The law would require at least the following elements: a privacy policy requirement stating a covered entity's privacy practices, detailed notice and choice at the point of disclosure, and a private right of action to enforce the law.

Privacy Policy. Currently only a few states require privacy policies by law. Although most major companies do develop and post privacy policies, they typically do so in order to protect themselves. An outright privacy policy requirement with consumer protections in mind is thus important in order to protect consumers. Consequently, the law would require each company that collects personal information to develop a privacy policy and to present the consumer with the privacy policy at the point of collection.

This requirement does several things. First, by requiring companies to develop a privacy policy, it forces at least some companies to take into account privacy issues that they may otherwise ignore. Second, it provides an easy forum in which companies can provide consumers with the notice and choice elements discussed directly below.

Notice. The law would further require that the privacy policy disclose specifically what covered third parties, if any, will have access to the personal information and how they will use it.

If the company would like to add additional third parties to the list after it gives the initial notice, it will need to provide the consumer with additional notice and choice (as described more fully below) before proceeding. In that way, the consumer will have a complete list and understanding of what covered third parties have their personal information and how they use it.

Note that the law would cover companies that had initially received the personal information from other companies, i.e., if a company received the personal information legally from another third party, but then desired to further disclose it to another third party, it would need to provide the consumer with notice and choice before doing so.

One complication naturally arises with this additional required notice: if the company has no means by which to contact the person (i.e., the personal information does not include contact information such as email or telephone, or such information is out-of-date), then the company has no means by which to provide the notice. However, rather than have the default favor the company (i.e., permission to proceed), the default should instead favor the consumer (i.e., no permission to further disclose the information).

Choice. Following notice, the consumer should have a choice as to whether the company may disclose their personal information to such third parties. This could be done in a blanket manner (i.e., all companies on the list are either acceptable or not), or the company could allow the consumer to pick and choose which third parties are acceptable to disclose to.

If and when companies wish to disclose a consumer's personal information to additional third parties not listed in the initial notice, then, as briefly mentioned above, the company would need to provide the consumer with additional notice and choice regarding whether the company may disclose the consumer's personal information to such third parties. The company would need to provide the consumer with a reasonable means by which to respond to the notice (e.g., e-mail, regular mail, or telephone).

As with notice, often companies may not have contact information for the persons whose consent they wish to obtain. Or, if they do, it may be out-of-date, or the person may not respond. However, this proposal contends that this should remain the company's problem rather than becoming the consumer's and that, if the company attempts to provide the consumer with notice and choice, and the consumer does not respond within certain period of time (e.g., thirty days of such notice), then the company must abandon its intention to further disclose the personal information.

Private Right of Action. A major issue with many of the sectoral laws, the FTC Act, state laws, and company self-regulation is that the consumers themselves have no means by which to enforce the laws, or, in most cases, to hold companies accountable that fail to live up to any best practices they purport to have adopted.[26] Instead, in most cases consumers must rely on the limited resources of the FTC and state attorney generals to keep companies honest, or, simply, rely on companies' own goodwill.

The proposed law would thus include a consumer private right of action to enforce the law against companies that fail to comply with its provisions. Statutory damages for grossly negligent or willful violations would also be included, at levels significant enough to make companies wary of failure to comply.

If a company illegally obtained someone's personal information and did not use it in a manner that would be immediately obvious to the consumer (e.g., direct marketing), then a consumer's ability to enforce the law against such entity may be rather limited. However, because the consumer could enforce the law against any entity that did ultimately contact or market to a consumer, and to which the consumer had no prior relationship (and

[26] One exception may be if the company makes certain promises in its privacy policy, that privacy policy is deemed to be part of a contract with the consumer, the company breaches that contract, and the consumer successfully brings a breach of contract claim. However, damages would be limited to contract remedies without any statutory relief.

thus for which the consumer had obviously not given consent), companies anywhere along the chain of information distribution would be wary of accepting information if a company along that chain failed to legally obtain the information and could not demonstrate to the party that it had done so.

In addition to the consumer's private right of action, the FTC and state attorneys general would have the ability to enforce the law.

Relationship to Other Laws. The proposed law would only affect other sectoral and state laws to the extent that its provisions impose more rigorous standards on companies. Other aspects of such laws, such as the Safeguards Rule of GLBA and the Security Rule of HIPAA, would remain unaffected. The proposed law would not preempt state law, so states could choose to impose stricter requirements.

An Analysis

The proposed law certainly poses certain challenges and, it may be argued, potential drawbacks. Most obviously, the law may hamper commercial activity between companies by regulating the free flow of information between them, limiting especially certain industries (e.g., advertising), and increasing companies' costs in order to comply with the law. Furthermore, some may view this approach as paternalistic and question whether consumers actually prefer the current or a more limited approach.

Indeed, the law's requirement of specific notice and consent in each instance may seem overwrought. Companies would need to spend vast amounts of time and resources retraining and possibly increasing staff, reworking their IT procedures and systems, and, in some cases, reforming their business models. Some industries in particular, such as advertising, rely on rapid inter-company exchanges of data in order deliver more relevant content to consumers and may, consequently, be severely restricted in how they share and obtain consumer data. In such cases, arguably the proposed law would actually harm consumers because they may receive less relevant advertisements.

Furthermore, requiring notice and choice in every instance may prove more cumbersome than beneficial to some consumers. Arguably, simply providing consumers with general notice and choice—often already done but not mandated in all cases—would instill the same sense of trust and confidence that the proposed law intends, and thus could supplant the current proposal with less hassle.

However, even if the process of notice and choice is cumbersome to some consumers, little reason exists to believe that the constant influx of marketing from third parties to whom the consumer has no prior relationship is not even more problematic for the same consumers. Some consumers would almost certainly prefer the informed notice and choice.

Furthermore, the mere fact that companies may incur increased costs in order to comply with the law is not reason enough to dismiss the proposal, especially if the current system is unfair to consumers and the proposed law strikes a better balance. And simply because some business models are based on an older system of personal information exchange is not reason enough to maintain the old system if such system presents significant deficiencies and an alternative provides significant benefits.

As argued throughout, the proposed system would provide significant advantages over the current regime's deficiencies. It would provide consumers with actual knowledge regarding what third parties a company intends to provide their personal information, rather than a general knowledge that provides little real information. Consumers' choice thereby becomes informed to the extent they choose to scrutinize the notice and exercise their choices.

This informed notice and choice, in turn, would bolster consumer confidence given consumers' enhanced ability to control the fate of their personal information. The private right of action coupled with the possibility of statutory damages would make this control actionable and real. With such pieces in place, the prevailing sense of consumer helplessness would almost certainly diminish, and the marketplace would benefit as a result. Indeed, in some cases these new controls may prevent actual malfeasance with respect to consumer information because a cost-benefit analysis under the new law will force some entities to consider privacy issues that previously they could afford, literally, to ignore.

Conclusion

Under the current US approach, consumers have little real choice regarding to whom companies may disclose their personal information and how such third parties may use it. Even in the typical best-case scenario, when consumers are given notice and choice, such notice and choice remains less than ideal because consumers do not receive sufficient information upon which they can make informed choices.

This proposal sets forth a remedy to this issue by requiring companies to develop privacy policies that provide consumers with detailed notice and choice regarding third-party disclosure and use. Such a law would increase consumer trust, confidence, and control in a world that they necessarily participate in, but often at the whims of a largely unaccountable private sector. This law seeks to change that balance.