Response to FTC Questions

Proposal for December 7, 2009 FTC Privacy Roundtable Discussion

Aaron Titus, Information Privacy Director

Liberty Coalition

(202) 360-4032 x 2

aaron.titus@privacycommons.org

http://www.libertycoalition.net

About Aaron Titus and the Liberty Coalition

Aaron Titus received his JD from the George Washington University Law School, where he specialized in Information Privacy Law, and has served as the Information Privacy Director for the Liberty Coalition. Aaron is an expert in privacy breaches and their causes, having documented more than 200 breaches in detail. In conjunction with the Liberty Coalition, Aaron created National ID Watch, a free website which has documented more than 1 million Identity Exposure Reports (IXRs). Each IXR is an individualized report which tells a victim of a breach exactly what types of information were exposed, under what circumstances, for how long, who's responsible, and how to contact them.

Aaron Titus has also worked extensively on privacy policies, and is a co-founder of Privacy Commons, which is a framework of privacy policy disclosure requirements. When completed, this framework will help organizations create complete, informative, enforceable, and easy-to-adopt privacy policies. The core framework will be supplemented by additional disclosure requirements for specialized activities. For example, some of these unique activities include financial, goods-and-services, and healthcare activities. In addition, Privacy Commons will convey high-level privacy policies through simple iconography.

The Liberty Coalition is a Washington DC-based non-profit organization which helps organize, support, and coordinate transpartisan public policy activities related to civil liberties and basic rights. The Liberty Coalition works in conjunction with groups of

partner organizations that are interested in preserving the Bill of Rights, personal autonomy and individual privacy. Although the Liberty Coalition does not speak for its Partners, the 80+ Liberty Coalition Partner organizations include:

American Civil Liberties Union
Amnesty International
Arab American Institute
Center for Financial Privacy and Human Rights
Citizens Against Government Waste
Common Cause
Democrats.com
Electronic Frontier Foundation
Electronic Privacy Information Center
First Amendment Foundation
The Libertarian Party
MoveOn.org Political Action
Patient Privacy Rights Foundation
Privacy Activism
Republican Liberty Caucus

References:

Liberty Coalition: http://www.libertycoalition.net

National ID Watch: http://www.nationalidwatch.org

Privacy Commons: http://wiki.privacycommons.org

Question 3

Do the existing legal requirements and self-regulatory regimes in the United States today adequately protect consumer privacy interests? If not, what are the particular privacy interests that warrant increased protection? How have changes in technology, and in the way consumer data is collected, stored, and shared, affected consumer privacy? What are the costs, benefits, and feasibility of technological innovations, such as browser-based controls, that enable consumers to exercise control over information collection? How might increased privacy protections affect technological innovation?

Response to Question 3

Personal Information Cannot Be Property

The Intellectual Property legal regime is wholly inadequate to adequately protect consumer privacy interests, and the market does not value privacy.

The premise of personal-information-as-property is that an individual accrues ownership interest in information about himself through some operation of law. Based on that ownership right, a person has a right to exclude others from viewing, using, disseminating, accumulating, etc., or alternatively, license these rights. This under-developed premise of personal-information-as-intellectual-property has no traceable roots to other forms of intellectual property law, but has nevertheless found its way into state breach notification laws, which refer to "data owners." The privacy tort of Appropriation is, at its core, a property right. Echoes of this premise may also be found in the common expression, "Identity Theft:" The idea that an identity may be owned and stolen like property.

Reliance on a pseudo-intellectual property regime to is insufficient to protect privacy. Personal information cannot be property for several reasons. First, personal information does not fit into any existing IP category. Personal information are facts, which are not copyrightable. With few exceptions, a name and SSN can't be trademarked. An address probably does not qualify for trade secret protection, and a date of birth is certainly not patentable.

Second, accrual of ownership is problematic. Even if an imaginary intellectual property right to one's personal information existed, acquiring ownership is difficult. Under existing IP theories, an individual cannot easily accrue ownership of his own personal information, since most sensitive personal information is created by third parties. Logically, any ownership right would first accrue to the party responsible for its creation, and then must be transferred to the data subject. This would mean that one's parents would most likely "own" one's name. Mothers would "own" children's dates of birth, and credit card companies would "own" my credit card number. The government would "own" Social Security Numbers, the Post Office would "own" my address, and Verizon would own my IP address and phone number.

Third, theoretical rights are unhelpfully limited. Even if an imaginary intellectual property right existed, and the title to the rights were successfully passed to the subject of the information (the "data subject"), any title conferred must cease when the individual transfers it to another. Theoretical "licenses" would be impossible to manage or enforce.

Fourth, personal information does not behave like property. Personal information is valuable and fungible. But unlike all other forms of property, personal information is inherently inalienable. Property, once properly alienated, will not affect the former owner. The former owner of a car which has been wrapped around a tree bears no liability for the accident. However, a person can never completely avoid liability when his identity has been wrapped around a proverbial tree.

Finally, even if all of these issues were able to be overcome, treating personal information as property is a bad idea. Your identity or Data Self is a digital alter-ego: a collection of personal facts which has its own life, fallacies, and mortality. Your Data Self may enter into contracts, commit crimes, have surgery, or be kidnapped to your detriment. For the first time in human history, a person may be defined and impersonated using just a small collection of facts. In other words, Self is Data. If personal information is treated like property, then there emerges an inescapable conclusion: **If Self is Data and Data is Property, then Self may become Property**. Indeed, the term "identity theft" embodies these two notions: First, our identities are a collection of data; and second, our identities may be bought, sold, traded, lost, stolen, or damaged like any other form of property.

Current Failure of Contract Law and Market Forces

Privacy policies in the United States suffer from several deficiencies. First, they are often unsophisticated and incomplete. They often fail to address important privacy issues or fail to consider all potential parties.

Second, privacy policies are relegated to the legal department, and often fail to address or actually contradict field practices. The Higher Education industry is notorious for this- many privacy policies talk about cookies and web forms, and completely ignore the vast storehouses of personal information they keep on every student.

Third, many privacy policies waive, rather than confer, privacy rights. The healthcare industry is well-known for this practice. Many patients assume that regulations authorized by HIPPA confer a large number of protections. In reality, the protections are substantially more moderate. But the regulations allow patients to waive certain privacy rights if they are notified. And many of those are waived when they sign the privacy policy. Thus, there is a substantial expectation gap between the protections patients believe they receive, and what they actually receiving.

Fourth, many privacy policies are not easily understood or even physically accessible.

Fifth, privacy policies which strictly enumerate technologies quickly become outdated in the face of emerging technologies.

Most importantly, US courts have consistently interpreted privacy policies to be unbinding notices, rather than contracts. As a result, privacy policies generally create no enforceable rights or enforceable expectations of privacy. In this sense, privacy policies can create a false expectation of confidentiality, privacy, or even fiduciary responsibility.

Privacy Commons seeks to solve these problems. A privacy policy which conforms to Privacy Commons requirements will be complete, informative, easy to understand, and easy to adopt. Like Creative Commons, Privacy Commons seeks to identify common cultural notions of privacy, and embody them in easy-to-understand policy frameworks, with simple high-level iconography.

Privacy Commons Frameworks allow Data Stewards (Stewards), and a Data Subjects (Subjects) to create contractual duties of confidentiality through principles of offer, acceptance, and consideration. Unlike Creative Commons, which operates under intellectual property (IP) licensing law, Privacy Commons Frameworks, contracts, and policies operate under a combination of market forces, contract, and tort law. IP law alone fails to provide meaningful privacy protections because: 1. Expectations of privacy end once a data subject shares personal information, and 2. Personal information are facts, which generally cannot be copyrighted, patented, trademarked or benefit from trade secret protection.

Privacy Commons will have a set of core disclosure requirements which will be common to all frameworks. These core disclosure requirements will be comprised of Required Representations, Optional Representations, and Prohibited Representations. We don't know how large these core requirements will be, but on top of those we've identified more than ten activities which collect unique information in unique ways, with unique practices and challenges, and unique regulations.

- Goods and Services Activities: Ie, Online stores, Hotels, Brick & Mortar stores
- Healthcare Activities: Ie, Health Insurance activities and medical services.
- Financial Activities: Ie, banking,
- Legal Activities: Ie, Activities protected by attorney-client privileges.
- Education Activities: Ie, K-12, Higher education, private schools
- Social Networking Activities: Ie, Facebook, Twitter, LinkedIn
- Network Provider Activities: Ie, ISPs, Cell phone providers
- Non-Profit Activities
- Government Activities: Government Agencies, Elected representatives, and Campaigns.
- Non-Networked Activities: Locally owned Mom and Pop's store or mechanics who store information in non-digital formats.
- Personal Activities: Personal blogs and websites.

A single organization may engage in more than one activity. For example, a typical University engages in educational, financial, healthcare, network provider, non-profit, and goods and services activities on behalf of their students. Importantly, a comprehensive privacy policy must address internal business practices. *Privacy practices must match privacy policies*. The vast majority of breaches are the result of inadequate privacy practices, regardless of whether the privacy policy was adequate.

Once fully-implemented, Privacy Commons could easily be implemented through several technological means, including P3P.

Success and Failures of Breach Notification Laws

With six years of breach notification law experience, it is essential to ask, "Are they working?" My shorthand answer is "yes, sort of."

Some contend that notification laws may even be harmful, distracting and confusing. Some believe that notifications fool consumers into thinking they aren't at risk if they don't receive a notice. I agree that as currently written, breach notification laws have several shortcomings: They are noisy and contain a strong element of theater. But their success or failure should be measured in several ways:

1. Decreased Incidence of Identity Theft
2. Increased Awareness and Identity Control
3. Decreased Risk Behaviors and Incidence of Breach
4. Increased Victims' Rights

1. Decreased Incidence of Identity Theft

Q: Do breach notification laws decrease identity theft?

A: Probably not. Several breach notification laws emphasize the need to protect consumers from identity theft and other misuse of a person's Data Self. However, researchers Sasha Romanosky, Professor Rahul Telang, and Professor Alessandro Acquisti presented a well-reviewed paper which measured the change in the rate of reported identity thefts before and after data breach laws went on the books. Though drawn from incomplete FTC data, the paper convincingly demonstrates that breach notification laws have a negligible effect on reported identity theft rates. Instead, they suggest that a state's gross domestic product and general fraud rate has a much stronger correlation with ID theft.

2. Increased Awareness and Identity Control

Q: Do breach notification laws increase identity risk awareness? Consumers' control over their identities?

A: Yes, to varying degrees. A cruel irony of data breaches is that the responsible organization is the only one who knows exactly what happened, and they have the strongest incentive to hide or skew the details. Many breaches go under- or unreported,

regardless of law. Even well-intentioned organizations issue vague, incomplete, blame-shifting or liability-reducing press releases that leave victims in the dark. In order to effectively empower consumers to conduct their own risk analysis, breach notifications must contain the following elements:

- **Who**: The class of victims affected by the breach.
- **What**: A complete list of exposed information, whether objectively sensitive or not, whether required by law or not.
- **Responsibility**: Exposing party's contact information.
- **How and When**: Sufficiently detailed information about the how and when the breach occurred.
- **How Much**: Total number of people affected.
- **Sensitivity**: The objective sensitivity of the information exposed
- **Duration**: The term of the exposure in hours or years
- **Distribution**: Was it a single-point exposure (ie, printed material in a dumpster), or an infinite-point exposure (such as an online exposure)?
- **Suggested Action**: A clear statement of consumer's legal rights (or lack of rights); Concrete actions taken by the organization to fix problems, mitigate risk, or remedy harm and suggested actions for the victim.

Breach notification laws have much more lax reporting requirements than these. And although I agree that the average breach announcement is "noisy," I think it would be a mischaracterization to label them as nothing more than "noise." Even the least specific notifications build public awareness. For better or worse, most public awareness of identity risks come from news bulletins about data breaches. Although none of the announcements may put any particular individual on notice of a personal risk, these "noisy" notifications have a net positive effect of educating the population at large.

3. Decreased Risk Behaviors and Incidence of Breach

Q: Do breach notification laws decrease individual risk behavior?

A: Probably Not, but they have that potential. An effective notification must contain actionable intelligence, which means Intelligence plus Action. A person stranded

in a raft on the ocean without a patch kit or pump may gather intelligence when they see bubbles rising in the water, but they will inevitably sink without the ability to take action.

An alert is only effective when it empowers a person to act. Typical breach announcements usually do nothing to empower individuals. Effective breach notifications require both intelligence and action. If either one of these elements is missing (as is often the case), it will fail to empower victims, and may even engender apathy.

Some suggest that in the current environment of data insecurity, consumers should be on constant high alert for identity theft, even without notice of a breach. After all, one's Data Self is constantly being traded without one's knowledge or consent in IT and business environments of questionable reputes.

It's a nice thought, but not very helpful. Being on high alert all the time is essentially the same as not being on alert any of the time.

Q: Do breach notification laws encourage organizations to improve behavior?

A: Perhaps yes. The Romanosky paper found that notification laws likely encourage businesses to take more stringent safety precautions with personal information, because of the economic incentive to avoid breaches. However, the incentives to secure data do not appear to outweigh the market forces which devalue privacy. Both the Privacy Rights Clearinghouse and the OSF Data Loss Database show a steady, and perhaps even increasing number of breach incidents and lost records each year. While part of this increase may be attributable to better reporting, there is no solid indication that data breach incidents are decreasing.

4. Increased Victims' Rights

Q: Do Breach Notification Laws Create New Rights for Consumers?

A: Absolutely yes. While not the silver bullet to cure all ails, breach notification laws are an important first step at creating rights for victims of breaches. Before BNLs, nobody had the right to know whether their Data Self had been compromised. Additional regulation will be necessary to address existing and emerging identity threats.

Solutions:

1. **“Stewards,” not “Owners”**: Given the tenuous and dangerous legal basis for “owning” personal information, notification laws should replace the concept of “personal information owners” with “personal information stewards.” This change would help sharpen the distinction between Data as Self versus Data as Property, and emphasize that third parties can’t “own” a Data Self.

2. **Expand Reporting Requirements**: Breach notifications should provide actionable intelligence, including Who, What, Responsibility, How and When, How Much, Sensitivity, Duration, Distribution, and Suggested Action.

3. **Standard Measures of Risk Breach**: I suggest using Size, Sensitivity, Duration, and Distribution.

4. **Presumptive Loss**: In order to successfully sue for a breach, a consumer must 1. Become an actual victim of identity theft and suffer loss, 2. Find the identity thief, 3. Prove that the thief’s copy of their SSN or other personal information came from the breaching entity, and 4. Prove that the entity had a legal obligation to keep that information private (a rare duty). This is an unreasonable and often insurmountable burden of proof. Instead, a few states including Tennessee have adopted a small presumptive “ascertainable loss” whenever a breach occurs. These nominal damages would recognize harm to reputation, apprehension, emotional distress, and violation of selfhood. They would also help counteract the market’s failure to value privacy

5. **Require a Data Audit Trail**: Stewards of personal information should maintain standard inventory controls on personal information, recording with whom and when the personal information was shared. This data trail would be used for data audits and could help establish causation in the case of a breach.

6. **Automatic Credit Reporting**: Consumers should get an automatic notification at any activity on their credit.

7. **Comprehensive Identity Control**: Just as identity theft can take on many forms, one's identity is far more than a financial credit report.

8. **Standardized Privacy Policies**: The Privacy Commons project is currently attempting to formalize and standardize privacy policies.