Written Response to US Federal Trade Commission (FTC) queries for 07 DEC 09

FTC QUESTION 1: RISKS

Original Question

What risks, concerns, and benefits arise from the collection, sharing, and use of consumer information? For example, consider the risks and/or benefits of information practices in the following contexts: retail or other commercial environments involving a direct consumer-business relationship; data broker and other business-to-business environments involving no direct consumer relationship; platform environments involving information sharing with third party application developers; the mobile environment; social networking sites; behavioral advertising; cloud computing services; services that collect sensitive data, such as information about adolescents or children, financial or health information, or location data; and any other contexts you wish to address.

Response: The FTC should develop a methodology/metrics for measuring the risk of improper use of Personally Identifiable Information (PII).

There are two areas of risk in considering the exposure of Personally Identifiable Information (PII): planned risks and unplanned risks. Planned risks are the risks associated with the intentional and agreed-to (implicitly or explicitly) sharing, collection, storage, archiving, and destruction of PII by the parties. The parties to such planned risks are the Subject of the PII, Relying Parties, and Identity Providers. Unplanned risks stem from the misuse/abuse of PII in ways not sanctioned by the agreeing parties (particularly the Subject) at the time they enter into an agreement.

Planned risks fall into the domain of contract law, and, as noted in our response to Questions 2 and 3, there is much room for improvement in the current legal regimes that cover this domain.

Unplanned risks more typically emanate from illegal activity. These are the subject of this response.
In order to properly regulate the handling of PII, it is necessary to understand the impacts of mishandling this information.

The impacts of improperly handled PII potentially include the following:

.* Physical harm (e.g., from government or rebel groups)
.* Financial harm (e.g., from governments, criminals)
.* Reputational harm
.* Duress and mental anguish (e.g., from abusive ex-partners or bullies)
.* National security.

The measurement of these impacts must consider individual data items and not merely PII as a class. To develop a proper assessment of the risk associated with each data item, an analysis of both the impact and the likelihood of worst-case scenarios must be considered. For example, certain data items that suggests an individual's ethnicity have been used to support massive genocides in various countries in the world, contributing to both physical harm and mental anguish. While the US has faced this impact only on a limited scale, storing and potentially disclosing such information does poses risks that extend beyond US borders. And because internet-attached systems are vulnerable to attack by extremist groups from anywhere in the world, a proper risk assessment must consider the consequences that extend beyond domestic borders.

Because privacy is, fundamentally, contextual, any question about privacy risk must be understood in the context of:

• The ways in which such information may be misused/abused
• The motivations of parties that may misuse/abuse such information.

The first step is to clearly enumerate the contexts in which risks of improper data handling will be measured. This set of contexts must span seemingly minor and trivial use cases to the most complex.

The second step in performing this analysis is the development of a framework to measure risk with respect to context of use and misuse.

The third step would be to measure risk within specific contexts associated with individual data items.

The fourth step is to then consider the impacts of correlation of data items, aggregated from multiple sources. In a data correlation scenario, data items that were deemed innocuous in a single, simple context may pose far greater risks. This analysis will require supplementing the measurement framework to address the additional sophistication and risks that data correlation presents.

Until we understand the impacts and likelihood of such scenarios, a rational determination of appropriate use and protections of such information cannot be determined.

FTC QUESTION 2: CONSUMER EXPECTATIONS

Original Question

Are there commonly understood or recognized consumer expectations about how information concerning consumers is collected and used? Do consumers have certain general expectations about the collection and use of their information when they browse the Internet, participate in social networking services, obtain products from retailers both online and offline, or use mobile communications devices? Is there empirical data that allows us reliably to measure any such consumer expectations? How determinative should consumer expectations be in developing policies about privacy?

Response: Recommend FTC create consumer education on risks and actions they can take to reduce exposure.

Consumers have unrealistic expectations as a result of having a limited understanding of both the risks associated with their PII and the care (or lack thereof) that it taken to protect this information.

When prompted for PII, the average consumer does not read the Terms of Service and Privacy Policies imposed by service providers – even while checking the box that states "I have read and accept" these terms. Consumers assume that the terms are reasonable because he believes that others have accepted them. He presumes that among these others are those who have read, understood, and agreed that the terms are acceptable. He further bolsters his acceptance on the fact that none of his associates who have similarly accepted these terms appear to have suffered any ill effects as a result of their acceptance. His "risk-based" model, therefore, supports his decision.

But the consumer's risk-based model is flawed because he lacks sufficient information to make an informed decision. Among the information he lacks are the following:

1. He does not understand the terms offered by the service provider (either because he has not read them or because they are not understandable to him)
2. He does not have a basis of comparison to know whether such terms are common or egregious
3. He does not understand the full exposure to which the terms subject him
4. He does not appreciate the persistance of his PII, once it has been given
5. He does not appreciate the potential for the probability of harm to increase over time.

Consumers also lack the power to compel service providers to change their terms to be more acceptable.

These information short-comings are likely to persist because consumers lack a clear champion to represent them. While there are numerous organizations taking on the mantle of protecting the consumer in this area, none have the name recognition, visibility, resources, or power to make a significant impact. It is similar to the early days of trade unions. Workers were being exploited, but they lacked a unified voice necessary to stand up to the power of large corporations.

The FTC has the name recognition, visibility, resources and power to drive improvements in the market. FTC has the name recognition and visibility to get the attention of both consumers and service providers. FTC has the resources to educate consumers on the risks associated with giving out their PII (as described in our response to Question 1). And FTC has the power to drive standardization of terms in Terms of Service and Privacy Policies that will simplify the understanding of offered terms (as described in our response to Question 3), allow for comparison of terms from one service provider to another, and create a market among service providers to compete on terms.

FTC QUESTION 3: LEGAL REQUIREMENTS, REGULATORY REGIMES, AND TECHNOLOGY

Original Question

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 1: FTC should consider regulations to resolve the market imbalance created by the lack of a legal regime to cover the ownership of PII.

There is no current Intellectual Property regime established to handle PII. Ownerhsip of PII is currently established by possession of it. There is no other standard, and mere possession fails to empower the person impacted by the distribution of his PII to protect himself.

While certain service providers may elect to restrict their disclosure of consumer PII, most holders of PII are free to do with it as they please. Furthermore, while specific regulations (e.g., HIPAA) impose restrictions on the distribution of particular data items of PII, privacy policies issued by entities subject to these regulations often compel comsumers to waive many of the rights conferred by the regulations in order to obtain service.

The problem is exacerbated by the way in which most PII is generated. It is not just a matter that much current PII is already "public" and no longer in control of its subject. Most PII is generated by a service provider (e.g., federal social security number, state drivers license, bank credit card number). Because of this, most PII is never within the sole control of its subject.

The situation is not unlike that of the environment. Little concern was given to the exploitation of air and water by business when the US was founded. Both resources were bountiful and the nation had yet to industrialize. Over time, however, expansion of the population and industrialization began using up these resources at a rate that demonstrated that they were not boundless. It became clear that such resources were limited, but the open market did not properly account for these social costs in the production costs of the industries that consumed them. To rectify this market imbalance, Congress created regulatory regimes that gave protection to these public resources.

In the area of PII, such information was originally disseminated on paper and remained on paper. Transactions occurred in person and identity was frequently established by face-to-face recognition. The "industrialization" of PII occurred when the internet fostered the digitization and allowed for both remote authentication of a consumer and the widespread distribution and correlation of PII.

While PII is not owned by the public, it suffers the same problem as the environment. The resource is not represented by a power to offset its exploitation. For a market-driven solution to exist to manage PII, an entity (or entities) needs to exist to represent the best interests of the public regarding the use of the information. Subjects represent such entities. While not the owners of the information, per se, their intersts best align with the public good. They need to be given the power of stewardship to dictate the distribution of their own PII. This could re accomplished by a new set of laws defining a new form of intellectual property. Alternatively, regulations can be promulgated under existing law to confer upon individuals the power to manage their own PII.

Response 2: FTC should promote the standardization of privacy policies.

There is a need to make privacy policies more understandable to allow consumers to know the risks that they are taking when they blithely check the box that they "have read and accept" the terms of the policy. In practice, this is seldom the case. Reasons that consumers do not read and understand these policies include the following:

1. They are lengthy, requiring a lot of time to read.
2. They are written in legalese, which makes them difficult to understand.
3. Rather than defining the consumer's privacy rights, they typically target the waiving of consumer's rights to privacy.
4. Consumers feel that they have no choice if they want a service (assuming competitor's policies are equally egregious in their treatment of PII).

Standardizatoin of privacy policies can help address this. The standardization of privacy policies would have the following benefits:

1. Make it easier for consumers to read and understand such policies.
2. Make it easier for consumers to make informed decisions about what terms they are willing to accept.
3. Facilitate the publication of educational materials (e.g., by privacy groups like EFF) that help consumers understand the impacts of various standard terms and might even include recommendations for appropriate terms.
4. Facilitate competition among service providers to provide consumer-friendly privacy policies.

Today, privacy policies are lengthy legalese documents that intimidate most consumers. As a result, consumers ignore them and just click Yes. And because no serious work has been done to assess the risks of various policies, they are unaware of the risks to which they expose themselves when they blithely accept such contracts.

Privacy policies currently include similar information that lends itself to standardization. A standardized privacy policy could provide

1. A checklist documenting what data items are collected.
2. A second section detailing to whom the information is disclosed (e.g., other departments of the same company, partner companies, third-party aggregators, third-party enterprises, government, etc.).
3. A third section detailing how the information is protected.
4. A fourth section that includes opt-in/opt-out information for releasing particular data or releasing it to particular third parties.

The Privacy Commons has already begun addressing this challenge. But the task is large and demands both policy and legal expertise to ensure that policies are both reasonable and enforceable. By providing resources to support this effort, FTC could expedite the creation of such policies and ensure their quality.