Questions for the Record -- Ranking Member Thune
Hearing: Protecting Personal Consumer Information
From Cyber Attacks and Data Breaches
March 26, 2014

To Chairwoman Ramirez:

Question 1:

In your testimony, you reference "geolocation information" as a rapidly emerging technology. The FTC has also referred previously to "precise geolocation data," for instance in a 2012 Commission report, proposing to protect the privacy of sensitive data including "precise geolocation data."

In the 2012 report, the FTC recommended that, before any firm could collect, store or use such data, it would be required to "provide prominent disclosures and obtain affirmative express consent before using data in a manner materially different than claimed at the time of collection." This sounds reasonable in certain circumstances. However, the Commission did not define the term "precise geolocation data." The Commission does advise that geolocation data that cannot be reasonably linked to a specific consumer would not trigger a need to provide a consumer protection mechanism, and further advises that if a firm takes steps to de-identify data, it would not need to provide this mechanism. However, because the FTC does not define relevant terms, I have heard that there is some concern for how practitioners in the mapping and surveying fields can comply with the guidance. Specifically, some stakeholders are concerned that a private firm would need to get a citizen's approval before developing mapping for an E-911 and emergency response management system.

A. What does the FTC consider to be "precise geolocation data"?

Precise geolocation data includes any information that can be used to pinpoint a consumer's physical location. For example, many mobile applications ("apps") collect a user's longitude and latitude coordinates, which allows them to translate a user's exact location on a map. It does not include general location data, such as a consumer's zip code, city, or town. In the context of the Children's Online Privacy Protection Act (COPPA), the statute and the Commission's COPPA Rule require parental consent for the collection of geolocation information sufficient to identify street name and name of city or town.

B. When mapping for an E-911 or emergency response management system, what level of de-identification is needed? Does a company need to secure everyone's prior approval, or else redact from the map every citizen for whom they did not get prior consent, when mapping for an E-911 or emergency response management system?

In its 2012 Privacy Report, the Commission set forth a privacy framework that calls on companies to incorporate privacy by design, simplified consumer choice, and increased transparency into their business operations. It is important to note that the framework

is a voluntary set of best practices designed to assist companies as they operationalize privacy and data security practices within their businesses. It neither imposes new legal obligations, nor is it intended as a template for law enforcement.

The framework calls on companies to offer an effective consumer choice mechanism unless the data practice is consistent with the "context of the interaction" between the consumer and the company. Under this approach, whether a company should provide choice "turns on the extent to which the practice is consistent with the context of the transaction or the consumer's existing relationship with the business, or is required or specifically authorized by law."[1] Mapping for an E-911 or emergency response management system would generally fall within the context of the interaction, and therefore companies that collect and use of geolocation information for these purposes do not need to provide a consumer choice mechanism.

C. I understand the Commission received significant public comment on this issue from engineers, architects, planners, surveyors, mappers and the Federal Geographic Data Committee, which represents federal mapping agencies. Can you tell me what the FTC's thinking is on this issue, and what its plans are to address the stakeholders' concerns?

When members of the geospatial industry collect addresses, parcel information, or other geolocation or survey data that is tied to public land records, this practice would generally fall within the "context of the interaction" standard. As any consumer who has purchased a house knows, public land record data is collected, used, and linked to specific consumers as a matter of course in connection with real estate transactions as well as property tax assessments and similar purposes. Accordingly, companies that collect and use this data for these purposes would generally not need to provide a consumer choice mechanism.

[1] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 38-39 (Mar. 2012).

Questions for the Record – Senator Ayotte
Hearing: Protecting Personal Consumer Information
From Cyber Attacks and Data Breaches
March 26, 2014

To Chairwoman Ramirez:

Question 1:

Earlier this year, the FTC testified before the Senate Banking Committee on safeguarding consumers when there is a security breach. What precisely triggers notification? There are 46 different state laws. In your opinion, what should be the threshold warranting a notification? Since the combination of certain types of personal information is more sensitive than each piece individually, what type of information being breached should warrant a notification to consumers?

It is important for both consumers and businesses that the trigger for breach notification is balanced. We want to ensure that consumers learn about breaches that could result in identity theft, fraud, or other harm so they can take steps to help protect themselves, but we do not want to notify consumers when the risk of harm is negligible, as over-notification could cause consumers to become confused or to become numb to the notices they receive.

Consumers should be given notice when information is breached that could be misused to harm consumers. At a minimum, companies should notify consumers of a breach of Social Security numbers because this information can be used to commit identity theft, even if not paired with an individual's name and address. Similarly, an account username and password can be used to gain access to an account, even if the thief does not have the name of the account holder. Additionally, in the event of changing technology or business models, the FTC should be able to exercise rulemaking authority to modify the definition of personal information.

I am happy to work with the Committee as it considers legislation on this important matter.

Question 2:

You testified regarding your important work in civil law enforcement against unfair or deceptive acts in data security practices. Is it safe to assume that you believe the Commission has existing authority to pursue enforcement actions against private businesses that fail to adopt reasonable data security practices?

Yes. The Commission has authority to challenge companies' data security practices that are unfair or deceptive under Section 5 of the FTC Act, and we have used this authority to settle 52 data security cases to date. In addition, Congress has given the FTC authority to bring data security enforcement actions against non-bank

financial institutions under the Gramm-Leach-Bliley Act, against consumer credit reporting agencies under the Fair Credit Reporting Act, and against websites and online services directed at children under the Children's Online Privacy Protection Act.

The Commission has called for data security legislation that would strengthen its existing authority. For example, we currently lack authority under Section 5 to obtain civil penalties, an important remedy for deterring violations. Likewise, enabling the FTC to bring cases against non-profits, which have been the source of a number of breaches, would help ensure that whenever personal information is collected from consumers, entities that maintain such data take reasonable measures to protect it.

Question 3:

What additional tools do law enforcement need to share information about ongoing threats and attacks with the private sector?

Information sharing is an important part of the fight against those who attempt to exploit consumers' personal information. Information exchanges such as Information Sharing and Analysis Centers (ISAC) enable companies to pool information about security threats and defenses so that they can prepare for new kinds of attacks and quickly address potential vulnerabilities. ISACs may also share information with law enforcement agencies, and vice-versa. The FTC is considering, at the request of members of Congress, the formation of an ISAC to enable retailers to share information. We have begun consulting with other ISACs and industry groups to explore the formation of such a group.

Questions for the Record – Senator Fischer
Hearing: Protecting Personal Consumer Information
From Cyber Attacks and Data Breaches
March 26, 2014

To Chairwoman Ramirez:

Question 1:

In your testimony, you state that "having a strong and consistent national requirement would simplify compliance by businesses while ensuring that all consumers are protected." Do you believe preempting state laws in favor of a strong national requirement would benefit, not harm, consumers?

I support a federal data security and breach notification law that would preempt state law, but only if such a standard is sufficiently strong and the states are given the ability to enforce the law. If a consistent nationwide standard came at the expense of weakening existing state legal protections for consumers' information, I would not support the law.

Question 2:

Would a uniform federal data breach notification law enforced by the Commission, as well as states attorneys general, provide a significantly greater level of protection for consumers than currently exists?

While the majority of states have data breach notification laws, few have specific laws requiring general data security policies and procedures. Breach notification and data security standards at the federal level would extend notifications to all consumers nationwide and create a level playing field so that businesses operating in numerous states can apply one standard. A federal law could create uniform protections for all American consumers.

Question 3:

Many different players in the Internet ecosystem increasingly collect and store the same or similar information. Should they all be subject to the same standards for data security?

All companies that collect and handle sensitive consumer information should be required to implement reasonable data security measures. We believe that reasonableness is the appropriate standard because it allows a company flexibility to develop a data security program based on factors such as the sensitivity and volume of consumer information it holds; the size and complexity of its data operations; and the cost of available tools to improve security and reduce vulnerabilities. The

Commission has emphasized a process-based approach to data security that includes designating an individual or individuals responsible for data security; conducting risk assessments; designing a security program to address risks, including administrative, physical, and technical safeguards; and adjusting the program to address changes.

Question 4:

In your written testimony, you express concern about data security legislation's ability to keep pace with technology. Would a "reasonableness" standard help address that concern because what is reasonable today may not be reasonable tomorrow as technology evolves?

That is correct. The Commission's reasonableness standard and emphasis on a process-based approach to data security encourages companies to reevaluate and adjust their programs periodically in light of changes to the types of information they collect as well as changes in the marketplace, including changes in technology.

Additionally, we support federal data security and breach notification legislation that would, among other things, authorize rulemaking under the Administrative Procedure Act to give the Commission the flexibility to implement the statute by making changes when appropriate. For example, this authority should include the authority to modify the definition of personal information in response to changes in technology and changing threats.

Question 5:

You mention in your testimony that the data security provisions of both the Fair Credit Reporting Act and the Children's Online Privacy Protection Act rely on a "reasonableness" standard. Should comprehensive federal data security legislation also be subject to a reasonableness standard?

Yes. A reasonableness standard would ensure that companies have strong protections in place to protect consumer information as well as flexibility when developing and implementing any data security program.