Responses of Federal Trade Commission Daniel Salsburg to Questions Submitted for the Record

Hearing on "Reforming the Electronic Communications Privacy Act"
Senate Committee on the Judiciary
September 16, 2015

Questions from Chairman Grassley

1. The Commission's statement for the record describes a series of types of cases that would be affected in the future if there is no mechanism to compel the disclosure of content from providers—including cases involving anticompetitive and deceptive business practices, consumer protection, and other fraud enforcement actions. Can you describe these, and other, scenarios in more detail, including how often these types of enforcement actions arise?

The Commission's testimony recommended that ECPA reform legislation include a mechanism that would enable civil law enforcement, using judicial process and approval, to seek a court order requiring that a target's provider produce content when the target has failed or refused to provide the content directly to the Commission. The Commission's testimony noted that this authority would be necessary in cases against fly-by-night scammers — especially those based abroad — as well as cases against targets that refuse to respond to the agency's CIDs or discovery requests.

The Commission frequently targets complex consumer frauds that are causing substantial injury to the public and in which the targets have an incentive to hide their involvement in the fraud, destroy incriminating records, and hide or deplete assets. In such cases, the Commission will typically seek temporary restraining orders. For instance, in FY2014, the Commission sought temporary restraining orders in 20 of the 50 federal court consumer protection actions it filed. Moreover, in numerous instances, the Commission has sued foreign defendants who may seek to evade their discovery obligations. For example, in 2014, the Commission filed 10 federal court actions against foreign defendants.

Even in future cases that do not concern consumer fraud – such as competition matters involving alleged conspiracies in which the defendant fails or refuses to produce internal documents – content that the defendant stores with a cloud service provider may be evidence that is central to the enforcement action.

2. Please provide any additional thoughts that you might have on the issues raised by the hearing, including but not limited to expanding on your testimony, responding to the testimony of the other witnesses, and/or anything else you did not have a chance to respond to that was discussed at the hearing.

Thank you for soliciting the FTC's views on ECPA reform. As the federal agency responsible for protecting the privacy and security of consumers' data, we have carefully considered the proposed legislation. The Commission has developed a multifaceted approach to protect consumers' privacy and security: (1) enforcement of a wide range of statutes, including the Fair Credit Reporting Act, Childrens Online Privacy Protection Act, and Section 5 of the FTC Act, (2) policy development that provides guidance to companies on best practices they should adopt to enhance privacy and security, and (3) outreach to consumers on how to protect their personal information and mitigate the risk of identity theft. In addition to protecting consumers' privacy and security, protecting consumers from fraud is also an extremely important part of our agency's mission. ECPA reform can help strike the appropriate balance between civil law enforcement interests and the need to protect customers' and subscribers' privacy so long as it: (1) exempts previously public commercial content that advertises or promotes a product or service, (2) exempts content when the customer or subscriber consents to the release of the content to the government, and (3) provides civil enforcement agencies with the ability to seek a court order requiring a provider to produce a target's content when the target has refused or failed to produce the content directly to the agency. As the Commission explained in its testimony, a target should have no reasonable expectation of privacy with respect to government access to previously public commercial content and the consensual release of content. And, a judicial mechanism for other content that a target fails or refuses to produce to the government would provide appropriate privacy safeguards so long as it requires a civil enforcement agency to first seek the content directly from the target, and then to seek a court order with notice to the target.

Questions From Ranking Member Leahy

1. **You testified that it no longer makes sense to provide less privacy protection to emails that are more than 180 days old and to emails that have been opened. The Electronic Communications Privacy Act currently requires the government to obtain a warrant before compelling the disclosure of email less than 180 days old. 18 U.S.C. § 2703(a). Is the FTC seeking the authority in civil investigations to obtain email, regardless of age, from providers without a warrant?**

Recent ECPA reform proposals would require the government to obtain a criminal warrant in order to compel a provider to produce a customer's email content. Because the FTC is a civil agency without authority to seek a criminal warrant, this sweeping prohibition would prevent the Commission from compelling the production of all email content – even messages in which a customer had no reasonable expectation of privacy with regards to law enforcement access. For instance, a spammer that sends a million messages touting a get-rich-quick scheme or a cure-all remedy has no reasonable expectation of privacy in the content of its spam, but the Commission would be foreclosed under ECPA reform proposals from seeking this content from a provider. These proposals also would require a criminal warrant to obtain email content even when a customer consents to having the FTC obtain the content directly from its provider. For instance, if a victim deleted a message from a target and wanted to authorize the FTC to obtain a copy of the message directly from the victim's provider, the FTC would not be able to do so under proposed ECPA reform legislation. The legislative proposals should include exceptions for previously public commercial content that advertises or promotes a product or service and for content with the consent of the customer or subscriber.

ECPA reform should also include a judicial mechanism that would permit civil law enforcement to obtain a court order compelling a provider to produce electronic content such as email when efforts to obtain the content directly from the target fail. Although the FTC has not proposed a specific judicial mechanism, such a mechanism should require appropriate judicial oversight and due process to protect the privacy rights of the target.

There is no reason for treating content differently based on the length of time it has been in electronic storage. Recent ECPA reform proposals appropriately remove this distinction by imposing a single standard for content held by remote computing service or electronic communications service providers. Thus, if a target fails or refuses to produce relevant email, regardless of its age, the Commission should be able to seek a court order, with notice to the target, demanding that the target's provider produce the content.

2. **In a prior committee markup of the ECPA Amendments Act, the Judiciary Committee added a provision making clear that agencies can continue to issue subpoenas to corporations for the contents of their employees' email. This recognizes that corporations do not have the same privacy interests as individuals. How important is this corporate email provision to your agency?**

Virtually all businesses use email as a communication method. For this reason, emails among a target's employees frequently provide important evidence of a target's law violations, the scope of injury, and identity of victims. ECPA reform efforts should preserve the Commission's ability to obtain this vital form of evidence.

Questions from Chairman Lee

1. **The FTC is the nation's chief privacy protection agency. The ECPA Amendments Act is the most important and popular consumer privacy bill before Congress, and it has been for many years now. It has over 290 cosponsors in the House and 23 Senators have joined me as cosponsors in this chamber.**

   - **Why is it so difficult for the FTC to endorse a bill that would codify protections that everyone here agrees reflect users' reasonable expectation of privacy?**

The Commission supports ECPA reform, but has commented on specific ways in which recent legislative proposals could be improved. The FTC brings a unique perspective to the ECPA reform process. The FTC is the civil enforcement agency charged with protecting consumers from unfair methods of competition and unfair or deceptive acts or practices. The FTC also has extensive experience in consumer privacy enforcement. Its enforcement actions have addressed practices offline, online, and in the mobile environment. The FTC also works to protect consumer privacy through other tools such as conducting studies and issuing reports, hosting public workshops on a wide range of issues, including the Internet of Things and Big Data, and developing educational materials for consumers and businesses. In all of its privacy work, the Commission aims to protect consumers' personal information and ensure that consumers have the tools necessary to make effective choices about their privacy while at the same time taking advantage of innovative products and services offered in a dynamic marketplace.

Successful ECPA reform requires finding the appropriate balance between protecting privacy and enabling civil law enforcement to obtain the evidence needed to protect the public.

The Commission's testimony highlighted two forms of content that recent ECPA reform proposals would prevent the FTC from obtaining even though customers would have no reasonable expectation of privacy with respect to government access to the content – previously public commercial content that advertises or promotes a product or service and content when the customer has consented to the government obtaining the content.

The Commission's testimony also explained the need to create a judicial mechanism to allow civil law enforcement to obtain content in some circumstances. As more and more content moves from local storage to cloud-based storage, the FTC is likely to encounter situations in which scammers refuse or fail to turn over relevant data stored in the cloud, thereby making it difficult for the FTC to protect consumers. In those instances when a target fails or refuses to

produce content directly to a civil enforcement agency, the agency should be able to seek a court order, with notice to the target, that would direct the target's provider to produce the content directly to the agency.

- **If the FTC can't – without reservation – endorse a bill that's supported across the ideological spectrum, and that merely seeks to codify the status quo as it exists today, doesn't that raise questions about the FTC's credibility to represent the views of consumers on privacy issues?**

The FTC supports the goals of ECPA reform, but believes that current legislative proposals can be modified in ways that both protect consumers' privacy and enable the FTC to continue to perform its critical consumer protection and competition missions in the future when most business data will be stored with third parties. The Commission has worked for almost 20 years to ensure that consumers' privacy is protected; we have brought hundreds of cases to protect consumers' privacy, published detailed reports on a range of privacy issues, and produced valuable consumer education and business guidance. The Commission remains committed to protecting consumers' privacy. We also seek to ensure that the FTC is able to perform its role as a civil law enforcement agency.

2. **The SEC's proposal to compel a third-party provider to disclose all of the content of an email account (going back who knows how far) rather than going to the company or individual directly and asking for only the relevant emails should raise important privacy concerns.**

- **Wouldn't such discovery would result in a lot of unrelated personal material being produced to the SEC and other agencies like the FTC, including medical, financial or attorney-client communications that are wholly unrelated or wholly protected in civil litigation between the parties?**

Long-standing administrative and judicial procedures are capable of addressing the risk that unrelated personal data or privileged material would be improperly accessed if the Commission obtained access to a target's content. As an initial matter, the Commission does not seek unrelated or privileged materials in its investigations. Moreover, there are several procedural safeguards that significantly decrease the likelihood that the Commission would obtain such information. For example, the FTC's internal review process for civil investigative demands (CIDs) requires that they pass through several layers of review before they are ultimately issued by a Commissioner. Once issued, the recipient has several opportunities to seek to narrow the scope of the CID, ranging from a meet and confer requirement contained in the Commission's CID rules to more formal opportunities to object to the CID's scope. The judicial mechanism sought by the FTC to obtain content from a target's provider would include further safeguards by requiring a civil law enforcement agency to seek a court order from a neutral judge with notice to the target. The target would have an opportunity to appear before the judge and explain any concerns about the production of irrelevant personal or privileged materials. If the court were to find that an order directing the provider to produce material was likely to result in the production

of privileged materials or materials that were not likely to lead to the discovery of admissible evidence, it could limit or deny the order altogether.