

---

## **Summary of House Subcommittee Hearing on Online Privacy, Social Networking, and Crime Victimization**

---

The House Judiciary Subcommittee on Crime, Terrorism and Homeland Security held a hearing on July 28, 2010, to consider online privacy, social networking, and crime victimization. The Subcommittee heard testimony from representatives of the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service describing the nature of online crimes relating to personal information that is shared online, as well as law enforcement efforts to counter these criminal acts. Industry and public interest groups discussed the protection of personal information online as well as the tools available to consumers to maintain the privacy of their data. Members expressed concern for the level of transparency provided to consumers online and called for consistent implementation of privacy controls on social networks, the protection of teenage and younger users on such networks, and promoting the ability of federal law enforcement agencies to establish partnerships with other U.S. and international law enforcement groups to successfully investigate and prosecute complex, multijurisdictional online crimes.

The hearing was chaired by Chairman Robert Scott (D-VA). Subcommittee members in attendance included Ranking Member Louie Gohmert (R-TX), Rep. Zoe Lofgren (D-CA), Rep. Bob Goodlatte (R-VA), Rep. Mike Quigley (D-IL), and Rep. Ted Deutch (D-FL). The Subcommittee heard from the following witnesses: Gordon M. Snow, Assistant Director, Cyber Division, FBI; Michael P. Merritt, Assistant Director, U.S. Secret Service; Joe Sullivan, Chief Security Officer, Facebook, Inc.; Marc Rotenberg, President, Electronic Privacy Information Center (“EPIC”); and Joseph Pasqua, Vice President of Research, Symantec Corporation.

### **Gordon M. Snow, Assistant Director, Cyber Division, FBI**

Mr. Snow remarked that “classic” crimes such as investment fraud schemes are migrating to the Internet. He explained that criminals are using new techniques available only online to perpetrate crimes. For instance, he said perpetrators acquire access to a user’s social networking profile to exploit that user’s friends by extending “emergency” requests for money. He also said criminals often use an employee’s personal social networking account to deploy malware into an employer’s networks. He noted a rise in data mining schemes that use online forms to solicit consumer personal information for illicit purposes.

Mr. Snow noted that online criminals are increasingly organized, and often organized into transnational hacking rings that present jurisdictional and logistical challenges to law enforcement. However, he highlighted the recent success of long-standing partnerships with federal, state, local and international law enforcement, as well as not-for-profit organizations. Mr. Snow asserted that intelligence and investigative agencies could share relevant information in “real time” and with limited pre-approval requirements. Mr. Snow did not present any legislative recommendations in prepared testimony.

## **Michael P. Merritt, Assistant Director, U.S. Secret Service**

Mr. Merritt asserted that Secret Service authority is broader than that commonly understood by the public and highlighted the range of statutory authorities entrusted in part to the Secret Service, such as access device fraud, identity theft, computer fraud, and bank fraud.

Mr. Merritt described a recent significant increase in the quantity and complexity of “cyber crimes” against financial institutions, private industry, and critical infrastructure. He expressed his concern with regard to crimes involving corporate network intrusions through exploitation of employee social networking profiles, as well as the increasing level of collaboration among cyber-criminals across jurisdictional boundaries.

Mr. Merritt recommended amending criminal statutes to safeguard sensitive personally identifiable information, and additional legislative reforms to provide law enforcement with greater resources to investigate data breaches.

## **Joe Sullivan, Chief Security Officer, Facebook**

Mr. Sullivan described in detail the most recent iteration of Facebook’s privacy controls and user protections. He asserted that user-managed controls have been simplified to allow users to apply to their profiles either broad settings of general applicability (“public,” “friends only,” etc.) or to set specified controls for each shared or posted item appearing in the user profile. He noted additional protections against malicious network use, including “Report” links on Facebook profiles and content items to notify Facebook personnel of problems, hidden security algorithms to detect anomalous and suspicious behavior, and cooperation with users to provide useful information in the event of fraudulent account access and activity.

In response to questioning by Chairman Scott and Rep. Lofgren concerning Facebook’s recent changes to user privacy controls, Mr. Sullivan explained Facebook’s approach to user privacy including tools to empower users to control their privacy. Mr. Sullivan also described Facebook’s partnerships with third-party developers and web sites in response to questioning from Rep. Goodlatte, who expressed concern as to the security measures taken when Facebook shares user data with such entities. Rep. Deutch expressed his concern with access by underage users to social networking sites. Mr. Sullivan responded by noting Facebook’s efforts to protect teenagers online and to prevent underage users from accessing the site or being put at risk in the event that they access the site, such as analysis of patterns in user activity and unique algorithms to protect against “friend requests” from malicious adult users.

Mr. Sullivan presented several specific legislative recommendations to the Subcommittee. These include:

- The implementation of a national database of convicted sex offenders that includes online identifiers and is accessible to industry, as provided for by the 2008 KIDS Act;
- Investment in youth and parent Internet education programs;
- Broader access by Internet companies to hashes of known images of sexual exploitation of children;
- More resources to train law enforcement on social technologies; and
- Better cooperation between law enforcement entities in different jurisdictions.

**Marc Rotenberg, President, EPIC**

Mr. Rotenberg commented that he believes some Internet companies have often modified user privacy settings and other data access and sharing features without first obtaining users' consent. He additionally commented that privacy settings are often too difficult for the average user to understand. Mr. Rotenberg expressed support for Congress to assert oversight and impose regulations on social networks. In response to a question from Chairman Scott with regard to the strength of online privacy laws in foreign jurisdictions, Mr. Rotenberg remarked that the European Union provided a "more comprehensive" approach to privacy protection than the United States.

Mr. Rotenberg specifically recommended a revision of section 2701 of the Electronic Communications Privacy Act to limit the ability of Internet companies to disclose user data to third parties, such as application developers and external web sites, without meaningful opt-in consent.

**Joseph Pasqua, Vice President of Research, Symantec**

Mr. Pasqua noted a dramatic increase in malicious software, viruses, and spyware deployment, and relayed his company's observation that the new signatures entered into Symantec antivirus software in the past 15 months exceeded the signatures entered in the past 18 years combined.

Mr. Pasqua presented several policy recommendations. These included the following:

- Criminalize the malicious act, not the software, as software programs can often provide beneficial uses;
- Increase penalties for online crimes;
- Develop model statutes and definitions to support uniform applications in foreign jurisdictions;
- Increase public-private partnerships; and
- Enact a comprehensive federal data security and breach notice law that incorporates liability-limiting incentives for businesses to encrypt stored user data.