MEMORANDUM

TO: ESPC

FROM: Reed Freeman
Patrick Bernhardt

DATE: May 16, 2014

RE: Senate Subcommittee Hearing and Report Regarding "Online Advertising and Hidden Hazards to Consumer Security and Data Privacy"

We write to summarize a May 15, 2014, hearing by the U.S. Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations ("Subcommittee") and a corresponding staff report entitled "Online Advertising and Hidden Hazards to Consumer Security and Data Privacy" (the "Report").

The hearing and Report focused on the risks to consumer privacy and data security posed by online advertisements, and specifically the potential use of online advertisements to deliver malware to consumers' computers. The Report contained findings and recommendations, as summarized below, and the Subcommittee heard testimony from representatives of the online advertising industry, a privacy advocacy group, the Federal Trade Commission ("FTC"), and the Digital Advertising Alliance ("DAA").

KEY POINTS:

- **Although the Subcommittee identified areas of broad concern regarding the delivery of malware through online advertisements ("malvertising"), the Subcommittee itself does not seem to be aligned around a legislative solution. There is agreement to punt the issue to the FTC (for more enforcement) and to self-regulatory bodies.**

- The FTC used this hearing to again call for enactment of a strong federal data security and breach notification law, which would include granting the FTC authority to seek civil penalties. It's possible that this call gets traction this term or next. **The issue would be whether advertisers or publishers would have secondary liability for malware they did not know about. Presumably they would, and would be responsible for potentially astronomical civil penalties, if their means of identifying and stopping malvertising were not "reasonable in the eyes of the FTC (without clear guidelines as to what's "reasonable").**

    - **Expect the FTC to redouble its law enforcement efforts in this area. They will look for malvertising and investigate advertisers, publishers and**

members of the ad-tech industry in the chain to determine whether their practices were "reasonable" in terms of stopping the malware.

- **This means that all of these companies need a written plan on how to do so in light of reasonably-anticipatable threats to the infection of malware into ads.**

REPORT FINDINGS AND RECOMMENDATIONS

The Subcommittee's key findings and recommendations from the Report for advertisers and self-regulatory groups are:

Findings:

1. Consumers risk exposure to malware through everyday activity, including viewing a page that has an infected ad on it;
2. The complexity of current online advertising practices impedes industry accountability for malware attacks;
3. Self-regulatory bodies (NAI, DAA) alone have not yet been adequate to ensure consumer security online;
4. Visits to mainstream websites can expose consumers to hundreds of unknown and potentially dangerous third parties;
5. Consumer safeguards are currently inadequate to protect against online advertising abuses, including malware, invasive cookies, and inappropriate data collection; and
6. Current systems may not create sufficient incentives for online advertising participants to prevent consumer abuses.

Recommendations:

1. FTC should enforce more than it has so far, and self-regulatory bodies should establish better practices and clearer rules to prevent online advertising abuses;
2. Strengthen security information exchanges within the online advertising industry to prevent abuses;
3. Clarify specific prohibited practices in online advertising to prevent abuses and protect consumers; and
4. Develop additional "circuit breakers" to protect consumers.

HEARING SUMMARY

The hearing began with introductory remarks from **Ranking Member Sen. John McCain (R-AZ)**, who summarized the findings and recommendations of the Report. In particular:

- He noted that the Internet has provided major benefits to consumers, but it also presents "novel questions concerning whether consumer security and privacy can be maintained in the new technology-based world."

- He expressed a "simple idea that I think everyone will agree on: **Consumers who venture into the online world should not have to know more than cyber criminals about technology and the Internet in order to stay safe. Instead, sophisticated online advertising companies like Google and Yahoo . . . have a responsibility to help protect consumers from the potentially harmful effects of the advertisements they deliver**."

- He suggested the current problem may require a new approach to preventing abuses of consumer data privacy, citing his legislation introduced several years ago, entitled "The Commercial Privacy Bill of Rights." The legislation would include:

    - Rights and expectations regarding data collection, use, and disclosure;
    - Prohibitions on specific practices;
    - A clarified role for FTC enforcement; and
    - A safe-harbor for companies that take effective steps to protect consumer security and privacy.

In additional remarks, **Chairman Sen. Carl Levin (D-MI)** emphasized the complexity of the online advertising industry and that such complexity may lead to weaknesses for cybercriminals to exploit. He also expressed concerns regarding the "vast amounts" of information created about consumers through visits to websites and indicated support for giving more enforcement tools to the FTC.

PANEL ONE: DETERMINING THE SCOPE OF THE PROBLEM

After introductory remarks, the Subcommittee called a panel of witnesses who addressed the following general issues: (1) the extent of the problem posed by malware delivered through online advertisements; (2) the current efforts by online advertising companies to protect consumers from malware; (3) whether those efforts were sufficient in light of the risks posed to consumers and the tools available to companies; and (4) the potential solutions that could enhance consumer privacy and data security.

Alex Stamos, Chief Information Security Officer, Yahoo!, Inc., and **George Salem, Senior Product Manager, Google, Inc.**, began by describing their companies' efforts to protect consumer security and combat malware. **Craig Spiezle, Executive Director, Founder and President, Online Trust Alliance**, provided information regarding the threat of "malvertising" and proposed additional solutions to the problem. During testimony and questions, the following issues were raised:

- **Panelists were divided about the extent of the problem posed by malware delivered through online advertisements**.

    - Sen. McCain emphasized the severity of the problem and repeatedly questioned the witnesses regarding whether the consumers are facing an increase in the amount of malware delivered through advertisements.

        - Alex Stamos noted that while the problem exists, online advertising constitutes only a small fraction of the malware distribution system and that "distribution is only one part of the problem."

        - **Sen. Claire McCaskill (D-MO)** agreed that this is only part of the problem, and emphasized that it is important to inform and empower consumers, who are generally unaware of online advertising practices.

    - **Craig Spiezle criticized online advertising companies for failing to coordinate with stakeholders and share information with other companies and regulators.**

    - Several Subcommittee members emphasized that the problem is made worse because consumers bear much of the costs of malware and that it could undermine consumer confidence and harm consumers directly.

- **Panelists disagreed about the sufficiency of current industry efforts to protect consumers against such risks**.

    - Industry representatives emphasized that Google and Yahoo! take a multi-pronged approach to security, including: scanning advertisements for malware, designing and implementing security protocols and tools, participating in industry groups, coordinating with security researchers and other companies, and building systems to prevent and disable malware.

    - Sen. McCain believed that companies should be engaging in more cooperation to achieve "best-practices" and that greater incentives are necessary to encourage companies to increase efforts to protect consumers.

    - Sen. Levin raised the possibility that companies could improve advertisement verification standards and develop relationships with "trusted" ad networks.

        - George Salem noted that it was often difficult to verify advertisers because cybercriminals deliberately deceive online advertising companies.

- **Panelists agreed that sharing information with other companies and government regulators could enhance security, but disagreed over other potential solutions**.

    - Panelists generally agreed that online advertising companies should share information about malware threats with other companies and potentially also with government regulators.

    - Sen. McCain and **Sen. Ron Johnson (R-WI)** would like to provide incentives to implement best-practices by providing a safe-harbor for companies that have taken certain steps.

- Alex Stamos emphasized that rather than focusing on incentivizes for online advertising companies, which already have market incentives to protect consumers, government should focus on reducing cybercriminals' financial incentives to deliver malware and commit fraud.

- Sen. Levin supported imposing a requirement on companies to provide notification of malware incidents to consumers or government agencies.

  - However, Alex Stamos noted that it would be difficult to provide notice to consumers because there is no direct relationship with the consumer or means of determining precisely who received the advertisement.

PANEL TWO: EVALUATING SELF-REGULATION AND OTHER POTENTIAL SOLUTIONS

The second panel included testimony from **Maneesha Mithal, Associate Director of the Division of Privacy and Identity Protection, Federal Trade Commission**, and **Lou Mastria, Managing Director, Digital Advertising Alliance**. The testimony and questions focused on the role that self-regulatory groups and the FTC play in protecting consumer security and privacy in the online advertising context. In particular:

- **Panelists agreed that self-regulation plays an important role in protecting consumer security and privacy**.

  - Lou Mastria reported on the substantial progress that the DAA has made in developing the Self-Regulatory Principles for Online Behavioral Advertising and subsequent frameworks for addressing multi-site data and applying the Self-Regulatory Principles in the mobile context.

  - **Maneesha Mithal called for "continued industry self-regulation to ensure that ad networks are taking reasonable steps to prevent the use of their systems to display malicious ads to consumers."**

- **Maneesha Mithal reviewed the FTC's prior enforcement actions and emphasized that online advertising companies may still be subject to liability under Section 5 if they fail to use reasonable security practices to prevent third parties from using online ads to deliver malware**.

  - Maneesha Mithal noted that "the Commission has made clear that **reasonable and appropriate security is a continuous process of assessing and addressing risks;** that there is no one-size-fits-all data security program; that the Commission does not require perfect security; and that the mere fact that a breach occurred does not mean that a company has violated the law. **These principles apply equally to advertising networks.** Just because malware

has been installed does not mean that the advertising network has violated Section 5. Rather, **the Commission would look to whether the advertising network took reasonable steps to prevent third parties from using online ads to deliver malware**."

- **Finally, Maneesha Mithal continued the FTC's calls for enactment of a strong federal data security and breach notification law, which would include granting the FTC authority to seek civil penalties**.