Opening Statement of Senator John McCain
Before
Permanent Subcommittee on Investigations
Hearing On
Online Advertising and Hidden Hazards
to Consumer Security and Data Privacy

May 15, 2014

Thank you, Mr. Chairman. I appreciate you and your staff's cooperation in conducting this important bipartisan investigation. As a longtime advocate for consumer's rights and Internet security, I believe that consumer privacy and safety in the online advertising industry is a serious issue and warrants this Subcommittee's examination.

With the emergence of the Internet and e-commerce, more and more commonplace activities are taking place on the Internet, which has led to major advances in convenience, consumer choice, and economic growth. These advances have also presented novel questions concerning whether consumer security and privacy can be maintained in the new technology-based world. We will examine these issues today specifically in the context of online advertising, where vast data is collected and cyber criminals exploit vulnerabilities in the system and use malware to harm consumers.

As we discuss this complex subject, it's important to keep in mind the following 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, whose representatives are here with us today, have a responsibility to help protect consumers from the potentially harmful effects of the advertisements they deliver. Deciding who should bear responsibility when an advertisement harms a consumer can be a technical and difficult question. But, it can't continue to be the case that the consumer alone pays the price when he visits a mainstream website, doesn't even click on anything, but still has his computer infected with malware delivered through an advertisement.

At the same time, online advertising has become an instrumental part of how companies reach consumers. In 2013, online advertising revenue reached a record high of $42.8 billion, surpassing for the first time revenue from broadcast television advertising, which was almost $3 billion less. With the continuing boom in mobile devices, online advertising will become even more lucrative in years to come.

With this hearing, we'll outline the hazards consumers face through online advertisements, how cyber criminals have defeated the security efforts of the online advertising industry, and what improvements could be made to ensure that consumers are protected online and the Internet can remain a safe, flourishing engine for economic growth.

Hazards Facing Consumers

Make no mistake, the hazards to consumers from malware in online advertising are something even a tech-savvy consumer cannot avoid. It is not a matter of simply avoiding shady websites or not clicking on advertisements that look suspicious. For example, in February of this year, an engineer at a security firm discovered that advertisements on YouTube served by Google's ad network delivered malware to visitors' computers. In that case, the user didn't need to click on any ads; just going to YouTube and watching a video was enough to infect the user's computer with a virus. That virus was designed to break into consumers' online bank accounts and transfer funds to cyber criminals. A similar attack on Yahoo in December 2013 also did not require a user to click an advertisement to have his computer compromised.

A consumer whose bank account was compromised by the YouTube ad attack has little recourse under the law as it currently stands. Of course, if an affected consumer managed to track down the cyber criminal who placed the virus, he (or relevant law enforcement agencies) could take legal action against that wrongdoer. But cyber criminals today are normally part of sophisticated professional criminal enterprises, often overseas. Tracking them down is exceedingly difficult—even for professional security specialists. A consumer has essentially no chance whatsoever of recovering funds from cyber criminals.

How can it be that cyber criminals can sneak malware into advertisements under the noses of the most technologically advanced companies in the world? Cyber criminals employ clever tricks to evade the current security procedures used by the online advertising industry. One of those key security procedures is scanning, essentially having a tester visit a website to see if a virus downloads to the test computer. Just as normal online advertisers can target their advertisements to run only in specific locations, cyber criminals can also target by location to avoid scanning. For example, if a cyber criminal knows that the facilities responsible for scanning ads are clustered around certain cities, they can target the malicious advertisement to run in other areas so that the scanners will not see it.

Cyber criminals have used even simpler techniques to bypass security. When law enforcement raided the hideout of a Russian cyber-criminal network, they found calendars marked extensively with U.S. federal holidays and three-day weekends. These cyber criminals were not planning Fourth-of-July picnics, of course; they were planning to initiate malware attacks at times when the security staffing at the ad networks and websites would be at their lowest ebb. Just this past holiday season on Friday, December 27, 2013—two days after Christmas and four days before New Year's Eve—cyber criminals hacked into Yahoo's ad network and began delivering malware-infected advertisements to consumers' computers. The malware seized control of the user's computer and used it to generate "bitcoins", a digital currency that requires a large amount of computer power to create. Independent security firms estimate that around 27,000 computers were infected through this one malware-laden advertisement.

Vulnerabilities Exploited by Cyber Criminals

The result of these cyber-criminal tactics has been countless attacks against consumers online. One major vulnerability in online advertising is that the advertisements themselves are not under the direct control of online advertising companies like Google and Yahoo. Those companies choose not to directly control the advertisements themselves because sending out all of those image or video files would be more expensive. Instead, online advertising companies have the advertiser himself deliver the ad directly to the consumer. While it is cheaper for the companies in the online advertising industry to operate in this way, it can lead to greater hazards for consumers. Malicious advertisers can use their control over advertisements to switch out legitimate ads and put in malware instead. The tech companies who run the online advertising industry frequently do not know when such a switch occurs until after the ad is served. Because those companies don't control the advertisement, their quality control processes are frequently purely reactive, often finding problems after they arise instead of before.

As the online advertising industry grows more and more complicated, a single online advertisement for an individual consumer routinely goes through five or six companies before ultimately reaching the consumer's computer. That fact makes it easier for the various companies in the chain to disclaim responsibility when things go awry.

One instance where that issue was apparent was the attack on Major League Baseball's website in June 2012. In that case, the malicious ad appeared to be for luxury watches and was displayed as a banner at the top of the MLB webpage. The ad was shown to 300,000 consumers before being taken down. In the aftermath of that attack, it was still unclear what entity was responsible for delivery of the malware. One security analyst noted at the time that "the lack of transparency and multiple indirect relationships" in online advertising made assigning responsibility for the attack virtually impossible.

The Complexity of Online Advertising

One way to get an idea of how complicated the online advertising world and online data collection can be is to take a look at what happens when a consumer actually visits a website where advertisements are served by third-party ad companies.

When a user visits a website, that website instantaneously contacts an online advertising company to provide an advertisement. That ad company in turn contacts other Internet companies who help collect and analyze data on the user for purposes of targeting advertisements to him. Each company can, in turn, contact other companies that profit from identifying users and analyzing those users' online activities. Ultimately, hundreds of third-parties can be contacted resulting from a consumer visiting just a single website.

Using special software called "Disconnect", the Subcommittee was able to detect how many third-party sites were contacted when a user visits particular websites. These contacts are represented in a chart. In this first example, we see what happens when a user visits the website of an ordinary business that does not depend heavily on advertising revenues. In this case, our example is TDBank, a company whose website provides online banking services for its existing

customers and, more importantly, not to generate income from people visiting the site. For that reason, it does not need to derive a large amount of revenue from online traffic and advertisements.

As you can see, a few third parties were contacted. By contrast, when a consumer visits a website that depends much more heavily on revenue from advertising—based on the number of people who visit their website—the number of third-parties can be enormously higher. For example, this video shows what happens when a consumer visits TMZ.com, a celebrity gossip website.

And, just to make that point even more clear, here are TDBank and TMZ side-by-side.

What these examples illustrate is that consumers generally do not understand the vast, complicated industry that has arisen to analyze their online movements for the purposes of delivering ads online. The websites themselves often don't have relationships with all of the third-parties who are contacted when visitors go to their site, and they often don't know many or all of the advertisers who actually show ads to their visitors.

Even the less complicated aspects of online advertising have proven vulnerable. A number of prominent, popular websites have suffered serious attacks through their own direct sale of advertising space to Internet advertisers. Cyber criminals will often register domain names and email addresses that closely mimic legitimate businesses in order to fool personnel tasked with advertising security. In 2009, *The New York Times* sold Internet space to someone posing as a representative of the phone company Vonage. That supposed representative of the company ran legitimate advertisements on the *Times'* website for several weeks. Then, on a Friday, the legitimate advertisements were replaced with malware-laden advertisements. It took the *New York Times* several days to identify and fix the problem.

Finally, another problem in the current online advertising industry is the lack of meaningful standards for security. The two primary regulators of online advertising are the Federal Trade Commission and self-regulatory groups like the Digital Advertising Alliance and Network Advertising Initiative. The self-regulatory groups have not been active in generating effective guidance or clear standards for online advertising security.

On the privacy side, those self-regulatory groups have worked to respond to concerns of online advertising abuses, but actual enforcement of the privacy-related self-regulatory codes of conduct appears to be lacking in some cases, where even after wrongdoing is detected by academic groups or unrelated security companies, the self-regulatory organizations seem slow to react.

For example, in March 2010, an online advertising company called Epic Marketplace began to engage in "history sniffing", a practice whereby a company can determine a consumer's previous online behavior by examining how the user's browser displays hyperlinks. Through that practice, Epic Marketplace could deduce that users had visited pages relating to, among other things, fertility issues, sensitive medical information, disability insurance, credit problems, and personal bankruptcy. Epic Marketplace then used that information for the purpose of

targeting advertisements to those users about those intensely personal issues. Epic Marketplace was a member of a self-regulatory group, the Network Advertising Initiative (NAI), when Epic's behavior came to light. NAI had not discovered Epic's behavior beforehand. Ultimately, Epic Marketplace remained an NAI member and was merely subjected to additional auditing requirements. The fact that a business engaging in such anti-consumer privacy practices could remain a member in good standing suggests that consumers cannot truly rely on a self-regulatory body to guarantee that their information is private and secure.

On the government side, the FTC has brought a number of enforcement actions against companies involved in online advertising for "deceptive" practices pursuant to their authority under Section 5 of the FTC Act. Those cases all involve some specific misrepresentation made by a company rather than a failure to adhere to any general standards. Thus, the easiest thing a company can do to avoid FTC enforcement is not to make specific promises about data privacy or security that could trigger a "deceptive" practices case. The FTC can also bring actions against "unfair" practices, though it has yet to bring any such cases against online advertising companies.

Fixing the Vulnerabilities in the Online Advertising Industry

So, where do we go from here? How can we fix the problems currently facing the online advertising industry and limit the risk of abuse of consumers' privacy and security? First, we must recognize the threat we face. Cybersecurity is a very real and increasing problem, and malware attacks in online advertising are just one technique used by cyber criminals to accomplish objectives ranging from financial gain or disruption of services to industrial espionage. Those attempting to exploit the Internet for criminal purposes are certainly the most culpable, and ensuring law enforcement has the necessary authorities and capabilities to hold criminal actors accountable is an essential element to effective deterrence.

We must also look at the security practices implemented by online advertising companies. Currently, commercial actors have limited incentives to develop and institute security measures for fear of becoming the liable party if something goes wrong. Regulators—both those in government and the self-regulatory bodies in the online advertising industry—need to collaborate to offer guidance on industry best practices for reducing risks. This review is needed to provide greater clarity on what is required of advertising companies to ensure consumer safety, and who should be held responsible when an advertisement harms consumers. This effort appears to be partly underway—just last week, with this hearing on the horizon, several online advertising companies, including Google and Yahoo, announced a new initiative called Trust in Ads that has as its goal the protection of consumers from malicious online advertisements and deceptive practices. The fact that the industry appears to be taking the problem seriously is a step in the right direction, but more needs to be done to protect consumers online.

Some of the advertising companies worry that sharing data and cooperating on security with some companies but not others would raise concerns that they are acting anti-competitively. Recent guidance issued by the Department of Justice and the Federal Trade Commission seemed to clarify that the antitrust laws do not stand in the way of sharing cyber threat information. If

there is any lingering uncertainty about the applicability of that guidance to the online advertising context, the DOJ and FTC should make clear that information sharing of online advertising malware threats is not anticompetitive. It is also long past time for legislation allowing for timely and effective information-sharing.

On the question of consumer privacy, there are some guidelines on how much data can be gathered on Internet users and how that data can be used, but these approaches—including verbose privacy notices, "do not track" efforts, and "notice and choice" procedures–have only been partially effective.

A new approach to preventing abuses of consumer data and privacy may be necessary. A few years ago, I introduced "The Commercial Privacy Bill of Rights" with then-Senator Kerry. While updates will be necessary, it provides a framework for how to think about these issues moving forward—one that includes basic rights and expectations consumers should have when it comes to the collection, use, and dissemination of their personal, private information online, and specificity in prohibited practices; a clarified role for the FTC in enforcement; and a "safe harbor" for those companies that choose to take effective steps to further consumer security and privacy. That legislation also envisions a role for industry, self-regulators, and stakeholders to engage with the FTC to come up with best practices and effective solutions.

Consumers deserve to be equipped with the information necessary to understand the risks and to make informed decisions in connection with their online activities. Today, one thing is clear. As things currently stand, the consumer is the one party involved in online advertising who is simultaneously both least capable of taking effective security precautions and forced to bear the vast majority of the cost when security fails. For the future, such a model is not tenable. There can be no doubt that online advertising has played an indispensable role in making innovation profitable on the Internet. But, the value that online advertising adds to the Internet should not come at the expense of the consumer.

Once again, I want to thank the Chairman for agreeing to hold this important hearing and the witnesses for appearing before the Subcommittee today. I look forward to their testimony.

# # #