June 2013 | Finance Issue

LawPracticeTODAY
THE MONTHLY WEBZINE OF THE ABA LAW PRACTICE DIVISION

ETHICS

Engage in Cyber Security—The Power and Responsibility is Yours

By Avery M. Blank

You are your own best shield against cyber-attacks. Government, businesses and individuals can provide cyber security. The inadequate attempts of government to implement comprehensive cyber security measures and the missions of Internet companies like Google and social networks like Facebook, which promote openness and accessibility, suggest that the individual should not rely on other entities to protect his or her personal information.

A recent survey out from the University of Southern California's Center for the Digital Future suggests that young adults may be particularly vulnerable to cyber-attacks. The survey indicates that Millenials (ages 18-34) are more willing than older age groups to share their personal information online, especially if they get something in return, like coupons or deals. While their online behavior may suggest otherwise, young adults are still concerned with others having access to their personal data.

Definition of "Personal Information"

The terms "personally identifiable information (PII)" and "personal information" are often used interchangeably. The National Institute of Standards and Technology defines "personally identifiable information (PII)" as:

any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as a name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

The Mission of Internet and Social Networking Businesses: Openness and Accessibility

Google's mission is to "organize the world's information and make it universally accessible and useful." Facebook says its purpose is to "give people the power to share and make the world more open and connected."

The principles of accessibility, informativeness, and openness stem from and contribute to a democratic society that is informed and has access to information. President Jimmy Carter wrote, "Access to information is a crucial element in the effort to reduce corruption, increase accountability, and deepen trust among citizens and their governments." Also, access to information helps empower citizens to challenge ideas and constructs.

Google and Facebook fulfill their respective missions by helping people answer all sorts of questions and stay connected with family and friends. However, the product of some noble missions can invite ignoble missions of others. Accessibility and openness of information can lead to the misuse of information. People can use information that we have put online to capture other unique personal information and, ultimately, engage in identity theft or fraud.

Facebook developed the Facebook Immune System (FIS), an allegedly successful defense to spam and other cyber-scams. Also, Facebook says its privacy settings "allow users to shield personal information from public view." Researchers from the University of British Columbia believe an attack on a Facebook account is still possible. These researchers note that "socialbots," software that poses as a human, can still infiltrate a Facebook account and ultimately access personal information. In fact, these researchers conducted a vulnerability study in which they were able to steal, through the use of socialbots, 250 gigabytes of personal information from Facebook's users. In an email to the author, Fred Wolens, a spokesperson for Facebook, said that Facebook uses multiple systems to combat attacks by socialbots and that the company is " constantly updating these systems to improve their effectiveness and address new kinds of attacks….We have serious concerns about the methodology of the research by the University of British Columbia and have shared these with them."

Google and its applications and Facebook are not isolated from each other or other electronic infrastructure, but rather are part of an electronic ecosystem that is highly interconnected. People can hack into Google accounts, find information related to financial accounts, and then hack into online financial accounts. Mat Honan, a writer for Wired.com (a technology news website), had his Google and Twitter accounts compromised by a hacker who was able to use reverse engineering with financial information provided by Amazon customer service.

Government's Insufficient Attempts to Fully Protect its Citizens

TELECONFERENCES & MEETINGS

The Best and Most Ethically Compliant Cloud Services
June 11, 2013 | LPM Members Rate $109 | Use Code **TSUMLPM**

Bad Check Fraud: You Could Avoiding Being Duped
July 2, 2013 | LPM Members Rate $109 | Use Code **TSVMLPM**

ABA/LPM ANNUAL MEETING
August 8-10, 2013 | San Francisco, CA

LPM BOOK SPOTLIGHT

LTRC

As it is not a good idea to rely solely on businesses to protect your personal information, neither should you rely on government to help protect your personal information. The U.S. government has made various recent attempts to get companies to share information and report breaches to help improve cyber security.

In October 2011, the Securities and Exchange Commission published guidelines that required public companies to disclose cyber security risks and cyber incidents. Disclosure of this type of information would help investors make educated spending decisions. These are guidelines, however, and so are not mandatory.

Earlier this year, President Barack Obama signed an executive order to protect critical infrastructure from cyber-attacks. The order provides for cyber security information-sharing and "the development of a framework to reduce cyber risks to critical infrastructure." The order, however, excludes "commercial information technology products or consumer information technology services."

Many telecommunications companies and industry observers criticized this exemption for companies like Google and Facebook from the executive order. For example, Marcus Sachs, Vice President of National Security Policy at Verizon Communications Inc., said that "e-mail is critical" and that "the Internet '[is] the lifeblood of cyberspace.'" The Internet is an ecosystem, and Stewart Baker, a former U.S. Department of Homeland Security official, notes that technologies provided by companies like Google and Facebook "play a vital role in the total security picture."

In February, the same month President Obama signed the executive order, the Cyber Intelligence Sharing and Protection Act (CISPA) was reintroduced in the U.S. House of Representatives. CISPA again passed the House in April and now heads to the Senate, where it died last year due to an outpouring of privacy concerns. The proposed federal law permits the sharing of information between government and certain private companies with the purpose of helping the government investigate cyber threats and bolster cyber security. TechNet, a lobbying organization that represents companies like Google, Facebook, Apple, Yahoo, and Microsoft, supports the legislation. Joel Kaplan, Vice President of U.S. Public Policy at Facebook, admitted that "[o]ne challenge we and other companies have had is in our ability to share information with each other about cyber-attacks" and that CISPA would make it easier for them and other companies to "receive critical threat data."

The federal government has enacted more than 50 statutes that address various aspects of cyber security, but no comprehensive legislation is in place. Over 40 cyber security-related bills have been introduced in the 112th Congress. In the 111th Congress, more than 60 cyber security-related bills were introduced. None of these bills passed. As a result, no major cyber security legislation has been enacted since 2002.

Your Mission: Engage in Cyber Security

The government may never be able to fully protect us from cyber-attacks. You should not wait for protection from either government or businesses. You are your own best protection from cyber-attacks. You are capable of taking the basic steps, such as not sharing personal information or anything that can be linked to personal information, protecting accounts with proper security measures (e.g., using complex and frequently changing passwords), and notifying the appropriate party if a breach has occurred so the entity can take the necessary steps to remedy the breach. For more information on how to (better) protect you and your personal information from cyber-attacks, consult websites like the U.S. Department of Homeland Security, OnGuardOnline.gov, and Ready.gov.

Attorneys also can become involved in government cyber security policy. Attorneys are trained in advocacy. You can advocate as an individual, on behalf of your business, or work with an association to help shape government cyber security policy. Make it your mission to protect against cyber-attacks and enlist the power of your advocacy to promote better cyber security policy.

LPT

ABOUT THE AUTHOR

Avery M. Blank *is an attorney and works for the University of Maryland Center for Health and Homeland Security.*