



Security, Privacy and The Law

Posted at 5:18 PM on March 15, 2009 by Gabriel M. Helmer

Highlights from the IAPP Privacy Summit - March 11-13, 2009 Washington, D.C.

Between March 11, 2009 and March 13, 2009, the [International Association of Privacy Professionals \(IAPP\)](#) hosted a [Privacy Summit](#) in Washington, D.C. that featured keynote presentations from fraud expert [Frank W. Abagnale](#) and information security guru [Bruce Schneier](#). The three-day event included dozens of breakout sessions with industry experts and government officials. Here are some of the highlights:

- Frank W. Abagnale spoke at length about his life, made famous by the Spielberg movie "[Catch Me If You Can](#)." What became clear through his stories was that armed with only an agile mind, Mr. Abagnale was able to compromise a series of security and anti-fraud systems at financial institutions and other businesses. And today, according to Mr. Abagnale, it is "4000 times easier" because of the leaps made in computer technology. "Technology breeds crime. It always has. It always will."
- Bruce Schneier, a luminary in the field of information security, spoke at length about how "data is today's pollution problem" - a problem that requires a new generation of professionals fluent in technology and law to manage a new "data environmentalism."
- Peter Cullen, Microsoft's Chief Privacy Strategist and member of the Consumer Privacy Legislative Forum (now called the Business Forum for Consumer Privacy) discussed the CPLF's decision to first generate a set of self-regulatory privacy guidelines before seeking to draft a comprehensive federal privacy standard. According to Mr. Cullen, businesses "need self-regulation" and to compile what have become best practices before attempting to impose a single federal standard. "[L]egislation is only part of the puzzle" and "bad legislation [would be] worse than no regulation."
- A panel of security experts from [\(ISC\)²](#), discussed the roles of the Chief Privacy Officer and Chief Information Security Officer during incident management. The panel also outlined several essential elements of an incident response plan, including: (1) a procedure for ensuring that a breach initiates an incident response team meeting, (2) a procedure to confirm that a breach has occurred, (3) anticipation and preparation of likely scenarios, (4) draft press releases and notifications, and (5) identifying key consultants and vendors used in investigating and resolving incidents.

- Representatives from [Google](#) and [Salesforce.com](#) discussed privacy issues raised by cloud computing models that may require different types of end user licenses, policies and agreements. Key issues include: (1) selecting the cloud model that is appropriate for your needs; (2) data persistence - ensuring that there is an appropriate policy for destruction of data; (3) data centralization and security - the more data served by a single service, the more of a target it will become for those seeking unauthorized access; (4) data use - centralizing data permits the cloud provider with the ability to provide additional services, but what limits should apply to the service provider's use of that data?
- A legislative update - the consensus is that consumer protection is one of Congress' top priorities and that Congress may be moving towards authorize the FTC to regulate information security more broadly.
- Jeffrey M. Kopchick, Senior Policy Analyst for the [FDIC](#), reported that federal agencies involved in the development of federal Red Flags Rules were preparing FAQs regarding compliance with those rules that should be published in the near future. He also indicated that because banks and other financial institutions have been subject to those rules since November 1, 2008 (unlike many other companies, who will see the rules go into effect on May 1, 2009), a number of common problems have been observed by FDIC examiners: (1) confusion in identifying what accounts give rise to the risk of identity theft; (2) insufficient oversight of third party service providers; and (3) lack of internal training to teach staff how to recognize red flags and mitigate the harm from identity theft.
- Joel Winston, Associate Director of the FTC's Division of Privacy and Identity Protection, updated members on recent trends in FTC enforcement. He indicated that the FTC intends to harmonize rulemaking on information security under a single federal standard evident in the recent Red Flags Rules: requiring businesses to adopt "reasonable and appropriate procedures." Given the speed of innovation, the FTC believes that requiring "reasonable" protections is the only manner for regulation to keep pace with technology. The FTC has considered and rejected suggestions that it impose specific security tools on businesses, as some states (including Massachusetts) have done. "Technology is too fluid." For example, "encryption may not always be the perfect solution - there could be good alternatives." The FTC appears to be unwilling to extend the May 1, 2009 deadline for enforcement of the Red Flags Rules and will be expecting businesses to demonstrate good faith efforts to comply with the regulations.

<http://www.securityprivacyandthelaw.com/2009/03/articles/government-enforcement/highlights-from-the-iapp-privacy-summit-march-1113-2009-washington-dc/print.html>