Protecting Privacy Online

Wednesday, April 11, 2007

South San Francisco Conference Center

2007 Summit Final Report

STATE OF CALIFORNIA

dca

DEPARTMENT OF CONSUMER AFFAIRS

What Our Partners Are Saying

"Identity theft is an equal opportunity crime. It can strike people of all ages and walks of life, and the impacts can be devastating."
Beth Givens, Director, Privacy Rights Clearinghouse

"A Notary's job is essentially to prevent fraud and help verify identity, so the National Notary Association is proud to be a part of this important event."
Timothy S. Reiniger, Esq., Executive Director, National Notary Association

"Identity thieves bombard the Internet every day, attempting to manipulate both technology and those who use it in order to obtain consumers' personal identifying information. These scams often devastate families irreparably, and those who perpetrate them must be stopped. This summit represents a very important step in that direction."
David LaBahn, California District Attorneys Association, Executive Director

"The California summits are a great forum for information about recognizing and preventing identity theft."
Gary Penrod, San Bernardino County Sheriff, California State Sheriffs' Association

Summary, Findings, and Recommendations

California Office of Privacy Protection
www.privacy.ca.gov

Contents

Overview

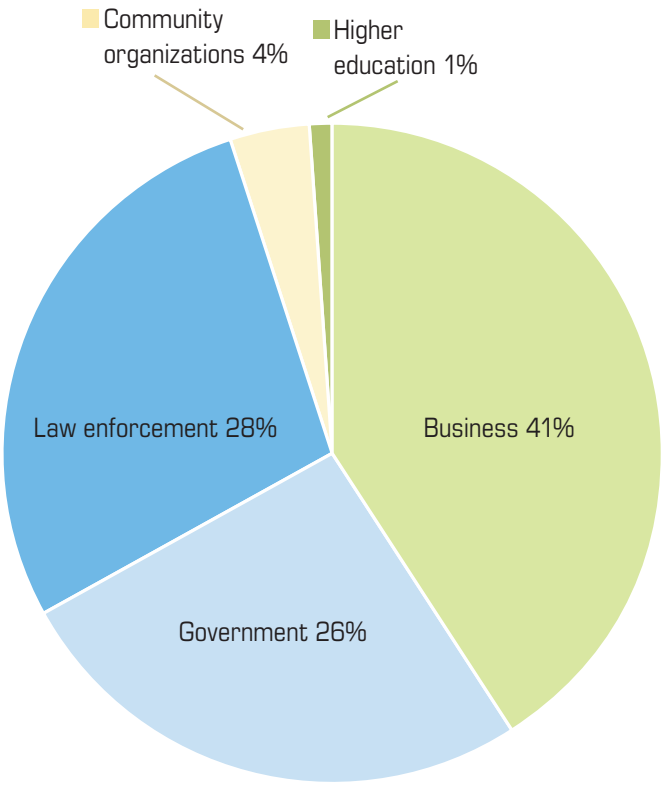
Protecting Privacy Online: A California Identity Theft Summit

More than 400 people attended the third California Identity Theft Summit in South San Francisco, where they joined with experts in exploring the privacy implications of the profound changes the Internet has made in our lives. The World Wide Web has put a universe of information at our fingertips, including, in some cases, information that we consider private. While online services offer greater convenience to consumers and cost-saving efficiencies to business and government, they also give criminals new opportunities for identity theft and other fraud. The 2007 Summit addressed the challenges of protecting privacy in the online world, from discussions of public policy issues to workshops offering practical guidance.

Like the two previous California identity theft summits, the 2007 Summit was the result of collaboration among the public, private industry, and State government. The event was presented by the California Office of Privacy Protection, the Department of Consumer Affairs, and the State and Consumer Services Agency. The Advisory Committee that helped design the Summit included representatives of leading California technology companies, privacy and consumer advocacy organizations, and experts in high-tech crime. The Summit was sponsored by Deloitte, as Gold Sponsor, and the California Victim Compensation and Government Claims Board, as Silver Sponsor.

Summit attendees represented the range of stakeholders concerned about online privacy: 41 percent were from business, 28 percent law enforcement, 26 percent government, 5 percent higher education and community-based organizations, and 100 percent consumers. Participants were able to choose among workshops on topics including protecting home computers, investigating identity theft cases, responding to privacy breaches, and earning customer trust in the online marketplace. The workshop for law enforcement offered POST-certified continuing education credit, and the one on California privacy laws offered Mandatory Continuing Legal Education credit to attorneys.

Summit participants



Findings and Recommendations

Findings

- The proliferation of personal information in digital form collected by organizations creates opportunities for identity thieves and poses risk management challenges for the organizations.
- Financial institutions and other organizations are increasingly using more robust authentication procedures to detect and prevent online fraud.
- Federated identity management, a system that allows individuals to use the same personal identification to sign on to more than one network to conduct transactions, can allow more user control of personal information and less sharing of sensitive information.
- Sensitive personal information like Social Security numbers in public records puts people at risk of identity theft, reputational damage, personal safety threats, and secondary uses.
- Some Web sites containing information from public records have policies allowing individuals to remove their personal information.

Recommendations

Based on the above findings, the California Office of Privacy Protection makes the following recommendations:

- Governments should reduce the amount of sensitive personal information in public records to the extent consistent with the original purpose for creating the record.
- The requirements of the Information Practices Act, Civil Code Section 1798 and following, should be applied to local government agencies.
- Web sites that post personal information, even when it was derived from public records, should provide individuals with a simple means of removing their information from the site.

General Sessions

Keynote Address: Identity Theft in the Digital World

Rena Mears, Global and U.S. Privacy Services Leader for Deloitte & Touche LLP

The day opened with a keynote address from internationally recognized privacy expert Rena Mears of Deloitte. She spoke about the identity theft firestorm, with the incidence of the crime and the amount stolen per victim rising dramatically from 2005 to 2006, while the amount of money victims recovered dropped. She cited several factors that are creating opportunity for identity thieves: the proliferation of data in the digital economy; data aggregation and data mining; the use of data for personalization of online transactions; and the resulting risk management challenges faced by organizations. Regulators have responded with security breach notice laws and laws protecting Social Security numbers. Businesses have responded with data security provisions in contracts between business partners and attempts to regain the confidence of consumers, particularly in relation to online commerce. She quoted a Wall Street Journal/Harris Interactive Survey, which found that 91 percent of consumers fear that their identities may be stolen and used to make unauthorized purchases, 30 percent limit their online purchases, and 24 percent have cut back on online banking. In conclusion, she urged consumers and enterprises to be proactive in protecting personal information and responding efficiently to incidents when they occur.

Panel 1: Nobody Knows You're a Dog: Identity in Cyberspace

The famous 1993 New Yorker cartoon of a dog surfing the Net illustrates the challenge of knowing who's who in the online world. The anonymity of the Internet allows us to seek out information and express ourselves freely and creatively. But predators, spammers, identity thieves, and other cyber criminals also use that same anonymity to deceive their victims and hide from prosecutors. State Chief Information Officer J. Clark Kelso moderated a panel of experts who discussed strategies for keeping the Web safe by verifying identity, while protecting individual privacy rights.

James Dempsey, Policy Director, Center for Democracy and Technology, described many of the scams that take advantage of the relative anonymity of cyberspace. He provided examples of phishing, keyloggers, and other kinds of spyware, and gave consumer tips for avoiding becoming a victim of them. His advice for policymakers included adopting baseline federal privacy legislation that would impose a custodial responsibility on organizations that collect personal information.

Christine M. Frye, Executive Vice President and Chief Privacy Officer, Countrywide Financial Corporation, reported that financial institutions are motivated to improve online security in order to reduce fraud losses, increase consumer confidence, and comply with new regulations. She described the new regulatory guidance requiring more than single-factor authentication for high-risk transactions. Extra authentication measures such as a shared secret, an automated phone call, or a token can provide a "mutual handshake" between a consumer and a financial institution. She cited a Gartner report that found that financial institutions that invest in additional controls beyond stronger authentication, such as fraud detection and transaction verification, will see fraud reduction that exceeds the cost of those controls by at least 25 percent. She counseled using complementary technologies, including fraud detection and stronger authentication and transaction verification to provide in-depth defenses.

Timothy Reiniger, Executive Director, National Notary Association, described how notaries are now able to provide identity verification services in a world of paperless documents. Documents ranging from mortgages to deeds to advance healthcare directives can be notarized electronically. Credential-based electronic notarization can facilitate faster and more efficient business processes, reduce costs and eliminate fraud. He explained that digital certificates are almost impossible to counterfeit and they comply with e-Notarization standards of the National Notary Association of Secretaries of State and the American Bar Association's digital signature guidelines.

Michelle Dennedy, Chief Privacy Officer, Sun Microsystems, Inc., explained federated identity management, an approach to managing and verifying identities online. Identity federation allows the user to link the personas he has created for different service providers into a single identity. This allows the user to log onto the Web site of one service provider and click through to an affiliated service provider with certain characteristics intact. Among the advantages of a federated

approach is user control (notice and consent), and a reduction in the movement of personal information from place to place. She cautioned that issues of consent, roles, and personas must be addressed holistically in an effort to find "the privacy sweet spot."

Panel 2: Public Records and Privacy

Public records have moved out of the relative obscurity of courthouses and county records offices into the 24/7 availability of the World Wide Web. This move has raised the vexing policy issue of balancing the public interest in open government with individual privacy rights. State Chief Technology Officer P.K. Agarwal moderated a panel of experts in privacy and First Amendment rights, who discussed their views on how we can continue to keep an eye on government without unduly spying on individuals.

Beth Givens, Executive Director of Privacy Rights Clearinghouse, spoke about the significant negative consequences to individuals, which she predicted will occur and are already occurring, when public records containing personally identifiable information are widely available on the Internet or via proprietary fee-based systems. She listed nine such consequences: less participation in public life; justice only for the rich (who will be able to take legal action to protect their personal information); identity theft; destruction of reputation; personal safety risks; secondary uses of personal information; growth of the dossier society; a loss of social forgiveness; and growing numbers of disenfranchised individuals.

Chris Hoofnagle, Senior Staff Attorney, Samuelson Law, Technology & Public Policy Clinic, pointed out that our nation's approach to access to public records evolved at a time when there were no computers or information brokers. Further, historically, public records had less personal information than they do today. Now, public records, tools for oversight of the government, are "recontextualized" to become tools to oversee individuals. We need to find a way to have ample access to public records, while reducing privacy problems. There are several options to obtaining this goal: first, the government should reduce, where possible, the amount of personal information collected in public records. Second, government should consider establishing use limitations to reduce commercialization of personal information in records. Third, the State should consider applying aspects of the Information Practices Act to county-level entities, where public records rich with personal information are stored. And finally, paper and electronic records should be treated the same, because while less accessible to the public, paper records are within the reach of data companies that transcribe personal information by hand.

Peter Scheer, Executive Director, California First Amendment Coalition, acknowledged that identity theft and similar crimes are a serious threat, both to personal privacy and the Internet generally. Unfortunately, there is no single, silver-bullet legislative solution or technological solution. The threat of identity theft, in its many aspects, will have to be addressed one aspect at a time—preferably with corrective measures that rely on market forces and competition for deterrence.

Some believe that State and federal freedom of information (FOI) laws are the root cause of unauthorized disclosures of private, identifying information. This is incorrect. There is nothing in the California FOI laws, or in federal FOIA, that would require or permit the release by government agencies of Social Security numbers and like information. If that information is flowing out of public agencies, it is happening illegally. Changes in public access laws will only further restrict the public's right to know about their government, while doing nothing to stem the illicit flow of information sought by identity thieves.

Courts—which are not subject to FOI laws—have been identified as a target-rich environment for information that can be used in identity theft. How to block access to Social Security numbers and like information? Not with legislation effectively ordering overworked court clerks to scrub legal documents of such information before placing records in open case files. That would cause huge delays in lawful access to important public information. Rather, the burden of redacting personal identifying information from court records should be placed on the lawyers who file records with the courts.

Susan Infantino, Product Counsel, Google, Inc., opened by stating Google's mission of making the world's information accessible and useful. She described the search engine's facilitation of bringing public record information to the public. She also mentioned the growth in social networking Web sites, where users voluntary disclose personal information. Acknowledging the need to balance public access and privacy, she described policies on removing confidential information from search results and hosted sites in response to requests.

Workshops

1. How to Protect Your Computer from Hackers, Viruses and Spies (for Consumers)

Ron Gabrielson, Deputy of Internal Affairs for the Geek Squad, told a large audience about the four basic steps for protecting their computers: turning on an Internet firewall; keeping the operating system up to date; installing and maintaining antivirus software; and installing and maintaining antispyware software. He also explained about practicing Internet behaviors that lower risk, such as deleting suspicious e-mail without opening it and using strong passwords, and the importance of paying attention to what kids do online.

2. Don't Get Hooked: Phishing, Pharming, and Other Online Scams (for Consumers)

Scott Shipman, eBay's Chief Privacy Counsel, and Michelle Jun, Staff Attorney for Consumers Union, teamed up to give consumers insight into the latest online scams and how to avoid them. Attendees were advised not to respond to e-mails requesting personal information, not to send money by wire transfer, and not to accept payment by cashier's checks. Some common scams were described in detail: Nigerian 419, Canadian lottery, and jury duty. Tips for safer online shopping included looking for "https" or the padlock icon on Web pages before keying in personal information.

3. Protect Your Kids Online (for Parents)

Syndicated columnist Larry Magid gave parents tips on how to alert kids to the hazards of cyberspace and how to protect them. He explained technological tools for protecting kids online, such as filters and rating systems, but cautioned that technology is not a substitute for parental involvement. His recommendations including setting family guidelines for computer use and posting them near the computer. He also provided information on how to report harassment and other cyber crimes to the National Center for Missing and Exploited Children's CyberTipline.

4. Law Enforcement Class—Part 1 & Part 2 (for Law Enforcement and Prosecutors only—POST/MCLE)

Assistant San Francisco District Attorney Laura Myers and Deputy Santa Clara District Attorney Bud Frank, both members of the REACT high-tech crimes task force, conducted a two-hour training course on identity theft investigation and prosecution. The course provided law enforcement officers and prosecutors with the basics, including the relevant statutory scheme addressing identity theft, how the crime is committed, and jurisdictional issues. They also provided information on gathering evidence, including computer forensic examination of digital evidence, and using search warrants. They discussed cases, including criminal identity theft cases, and explained the California procedure for getting a judicial finding of factual innocence and registering such victims in a special DOJ database. Participants were given a CD containing the new "Identity Theft Reference Manual for California Law Enforcement," developed by the California High Technology Crimes Task Force, the California District Attorneys Association, and the California Office of Privacy Protection.

5. Overview of California Privacy Laws (Business, Attorneys—MCLE)

Reece Hirsch of San Francisco law firm Sonnenschein, Nath & Rosenthal LLP, provided insight into many of the laws that have put California at the cutting edge of privacy regulation, often setting a de facto national standard. He discussed the landmark security breach notification law, as well as laws on the confidentiality of Social Security numbers, online privacy notices, reasonable security practices, and some industry-specific privacy laws.

6. Privacy Laws and Practices for Government Agencies (Government and Higher Education)

Two State government officials with responsibility for privacy and security gave attendees from government agencies and universities an overview of relevant laws and best practices. Debbie Castanon, Privacy Specialist with the California Office of Privacy Protection, described the privacy laws applying to State and local government, as well as legislation currently being considered by the State Legislature. She also identified resources providing more information for government agencies. Colleen Pedroza, the State Chief Information Security Officer, presented the major components of an information security program for a government agency, including best practice recommendations for executives, managers and supervisors, IT staff, and others inside and outside the organization.

7. Earning Customer Trust in the Online Marketplace (Business)

Two leading experts on consumer privacy shared the results of their 2007 survey on the most trusted companies for privacy. Larry Ponemon of the Ponemon Institute and Fran Meier of TRUSTe discussed what leads consumers to trust a company's respect for their privacy, which is of increasing concern as more business is done online. Among the interesting findings they reported were the factors most likely to increase privacy trust, which included overall company reputation and quality of products or services, as well as limits on data sharing and online security. The factors most likely to decrease privacy trust, on the other hand, were a data breach, irresponsible marketing, inaccurate data, and aggressive sharing of information.

8. Responding to Privacy Breaches (Business, Government and Higher Education)

Businesses, government agencies, and universities have all experienced breaches of personal information in recent years. Joanne McNabb, Chief of the California Office of Privacy Protection, and Lisa Sotto, who heads the Privacy and Information Management Practice of the New York office of Hunton & Williams LLP, provided practical advice on how to respond to a breach of personal information. Recommendations included involving appropriate stakeholders in preparing for a notification, notifying in all jurisdictions, and using plain language in the notice. Both stressed the need to have a response plan in place before an incident and the vital importance of top management focusing on data security. Among the lessons learned from breaches are the need to inventory an organization's personal information, with particular attention to mobile data (on laptops, thumb drives, and other portables).

9. Electronic Notarization (Notaries)

Kate Donovan of the National Notary Association provided practical training for notaries on eNotarization, the electronic equivalent of a notary's official physical seal or stamp. Whether a document is paper or electronic, by requiring personal appearance, verifying identity, and ascertaining the willingness and awareness of signers, the notary provides invaluable protection against fraud. She discussed the California laws applicable to eNotarization, and explained the requirements for the Electronic Notary Seal. She also described "papering-out," an interim stage on the road to entirely electronic real property transactions.

Links to Speaker Handouts

Workshops

1. How to Protect Your Computer from Hackers, Viruses and Spies

2. Don't Get Hooked: Phishing, Pharming, and Other Online Scams
   A. Michelle Jun
   B. Scott Shipman

3. Protect Your Kids Online

5. Overview of California Privacy Laws

6. Privacy Laws and Practices for Government Agencies

7. Earning Customer Trust in the Online Marketplace

8. Responding to Privacy Breaches
   A. Lisa Sotto
   B. Joanne McNabb

9. Electronic Notarization

Panels

1. Nobody Knows You're a Dog: Identity in Cyberspace
   A. James Dempsey
   B. Christine Frye
   C. Timothy Reiniger
   D. Michelle Dennedy

2. Public Records and Privacy

ID Theft Summit Advisory Committee

Scott Reid
Interim Director
California Department of Consumer Affairs

Alex Alanis
California Bankers Association

Cathy Coyne
California State Sheriffs' Association

Jim Dempsey
Center for Democracy and Technology

Michelle Dennedy
Sun Microsystems

Kathy Door
California Department of Motor Vehicles

Beth Givens
Privacy Rights Clearinghouse

Roxanne Gould
AeA

Chuck Halnan
Direct Marketing Association

Gail Hillebrand
Consumers Union

Robyn Hines
Microsoft

Tiffany Jones
Symantec

J. Clark Kelso
Chief Information Officer
State of California

David LaBahn
California District Attorneys Association

Bob Lozito
Sacramento Valley Hi-Tech Crimes Task Force

Fran Maier
TRUSTe

Joanne McNabb
California Office of Privacy Protection

Robert Morgester
Department of Justice

Karin Ogata
GTC

Afzal Rashid
Victim Compensation & Government Claims Board

Timothy Reiniger
National Notary Association

Scott Shipman
eBay Inc.

Nicole Wong
Google

Charlene Zettel
Former Director
California Department of Consumer Affairs

State and Consumer Services Agency
www.scsa.ca.gov

Department of Consumer Affairs
www.dca.ca.gov

California Office of Privacy Protection
www.privacy.ca.gov

STATE OF CALIFORNIA

dca

DEPARTMENT OF CONSUMER AFFAIRS