cyber safe california

protecting our children, safeguarding our privacy, securing our future

Summary Report

2008 Cyber Safe California Summit

March 4 – 5, 2008
Burbank Airport Marriott Hotel & Convention Center

cyber safe california

protecting our children, safeguarding our privacy, securing our future

contents

Thank you to our sponsors

The summit would not have been possible without the support of our sponsors Thank you to Silver Sponsors the California Victim Compensation and Government Claims Board, Microsoft, and Debix; and to Bronze Sponsors AOL, the Children's Educational Network, ContentWatch, Deloitte & Touche LLP, SSH Communications Security, and the Los Angeles County Department of Consumer Affairs

cyber safe california

protecting our children, safeguarding our privacy, securing our future

overview

Cyber Safe California was the fifth privacy summit presented by the California Office of Privacy Protection, the Department of Consumer Affairs, and the State and Consumer Services Agency, and the first to bring together children's online safety and current consumer privacy issues Cyber Safe California was the product of a successful partnership of government, business, and community organizations The Summit Advisory Committee included leaders of California technology companies, privacy and child safety advocacy organizations, and experts in high-tech crime They worked together to create an event that provided advice and resources and a forum for policy discussions about future privacy challenges and how to meet them without stifling emerging technologies

More than 300 consumers, business people, parents, educators, law enforcement officers, government leaders, and community activists attended the two-day event in Burbank On the first day, expert panels discussed current public policy issues such as social networking Web sites, medical identity theft, and the privacy challenges posed by new technologies On the next day, 15 different workshops provided practical information and guidance on topics of interest to consumers, business people, law enforcement, government, and higher education Topics included protecting your home computer, Internet safety programs for schools, patient privacy rights, data security, and investigating Internet crimes against children

summit advisory committee

Parry Aftab
WiredSafety, TeenAngels

Kimberly Allman
Recording Industry Association of America

Bill Ashworth
Yahoo!

Cathy Coyne
California State Sheriffs' Association

Pam Dixon
World Privacy Forum

Kathy Door
Department of Motor Vehicles

Scott Frizzie
California Governor's Office of Emergency Services

Beth Givens
Privacy Rights Clearinghouse

Roxanne Gould
AeA

Robyn Hines
Microsoft

Laura Jeffries
Association of California School Administrators

Tiffany Jones
Symantec

Chris Kelly
Facebook

Marc Klaas
KlaasKids Foundation

K.J. Lavoie
California Alliance of Boys and Girls Clubs

Carrie Lopez
California Department of Consumer Affairs

Lieutenant Bob Lozito
Sacramento Valley Hi-Tech Crimes Task Force

Larry Magid
ConnectSafely org

Kevin McCartney
Boys and Girls Clubs of America

Joanne McNabb
California Office of Privacy Protection

Kathy Moffat
California State PTA

Robert Morgester
California Department of Justice

Hemanshu Nigam
MySpace (Fox Interactive Media)

Tom Oscherwitz
ID Analytics

Rebecca Randall
Common Sense Media

Afzal Rashid
California Victim Compensation & Government Claims Board

Luan B. Rivera
California School Boards Association

Teri Schroeder
i-SAFE, Inc

Lynda Swenson
California Department of Consumer Affairs, Division of Investigation

Judi Westberg Warren
Web Wise Kids

Dena Wilson
California Office of the Secretary of Education

general sessions

keynote speakers

Peter Cullen, Chief Privacy Strategist, Microsoft

"The New Privacy Landscape and Why it Matters"

Peter Cullen discussed the concept of building consumer trust as a multi-party effort "Consumers are concerned about the security and privacy of their personal data By working together, businesses, government, law enforcement, and consumers can better protect data and earn consumer trust," Cullen said "Business and government must be responsible for managing consumer information, law enforcement's role is to go after bad actors, and consumers need to be smart about protecting their information "

At Microsoft, Cullen has been a leading advocate for strong and innovative safeguards for personal information, privacy, and other data, as well as technologies, services, and processes that enhance trust He is on the board of the International Association of Privacy Professionals and the board of TRUSTe, a group dedicated to building trust on the Internet In 2003, Cullen was honored with the IAPP Vanguard Award for Privacy Innovation for his contributions to the privacy profession

Hemanshu Nigam, Chief Security Officer, MySpace

"Setting the Bar for Social Networking Safety"

As Chief Security Officer for News Corp's Fox Interactive Media, Hemanshu Nigam oversees all safety, security, education, privacy, and law enforcement programs for MySpace and other Fox Interactive properties He has also served as a federal and state prosecutor against Internet child exploitation and computer crime, as well as an advisor to Congress on online child safety, and advisor to the White House on cyber stalking

He announced that MySpace has joined with iKeepSafe to release a broadcast public service announcement aimed at encouraging parents to talk with teens about their Internet use and help them to make smart decisions to be safe online He explained that MySpace operates on the belief that parents are equipped with the know-how and ability to talk with their teens about appropriate and safe behavior, but need to extend the conversation to online activities

Jim Steyer, CEO, Common Sense Media

"Education and Raising Kids in the New Digital World"

Jim Steyer is the CEO and founder of Common Sense Media, the nation's leading nonpartisan organization dedicated to improving the media lives of kids and families

He has spent more than 20 years as one of the most respected experts and entrepreneurs on issues related to children's policy and media in the United States As CEO, he is responsible for the overall leadership of Common Sense Media, the nation's leading nonpartisan organization dedicated to improving the media lives of kids and families Prior to founding Common Sense, Steyer was Chairman and CEO of JP Kids, a respected family media company Before that, he served as president of Children Now, a leading national advocacy and media organization for children, which he founded in 1988 Steyer began his career as an elementary school teacher and then became a public interest lawyer He served as a law clerk for the California Supreme Court, as a deputy district attorney, and as a civil rights attorney with the NAACP Legal Defense Fund

panels

PANEL 1
Internet Safety: What Kids Know — and You Don't

The day opened with a dynamic panel in which kids and reporters compared their knowledge of safe online practices In a game show format, Randy Paige, Consumer Interest Reporter for KCBS–TV CBS, Los Angeles, and Phil Shuman, Investigative Reporter for KTTV Fox, Los Angeles posed questions to the young members of Tweenangels and the kids asked the reporters questions

With the artful moderating of Larry Magid, syndicated columnist and founder of SafeKids com, SafeTeens com, and co-director of ConnectSafely org, the two teams covered topics such as spyware and why it's a danger to your PC, and the secret lingo kids use in instant messaging It was a close contest, but the kids came out on top

Tweenangels is a group of 9- to 12-year-old volunteers who have been specially trained by law enforcement and leading safety experts in all aspects of online safety, privacy, and security After completing the required training, the Tweenangels run programs in schools to spread the word about responsible and safe Web surfing to other kids, parents, and teachers Tweenangels was founded by Parry Aftab, Executive Director of WiredSafety org

PANEL 2
Emerging Technology and Our New World

State Chief Information Security Officer Colleen Pedroza moderated a panel of experts who discussed how new technologies are affecting our everyday lives, our decisions, and our future How can policymakers ensure that the new world made possible by technology is safe without discouraging further technological advances?

Harry Valetk, Corporate Privacy Director for MetLife, discussed the impact of social networking sites like MySpace, Friendster, and Facebook, which have seen enormous growth over the past few years He pointed out some of the problems caused by the lack of boundaries between our social network "friends" and our offline relationships, our online postings and our workplace

Pam Dixon, Executive Director of the World Privacy Forum, introduced the emerging issue of medical identity theft, "the information crime that can kill you " Medical identity theft occurs when someone uses a person's name or other identifying information to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods Medical identity theft can result in fraudulent charges and can also leave a trail of falsified information in medical records that can plague victims' medical and financial lives for years Dixon recommended expanding the rights and recourses available to victims of identity theft, including allowing them the ability to remove false information from their files

Jane Horvath, Senior Privacy Counsel, Google, addressed protecting privacy on the Internet The definition of personally identifiable information is evolving, with IP addresses sometimes seen as personally identifying The challenge is to achieve a good balance between privacy and security and the panoply of information and services available online Transparency about data collection and use is a critical privacy element, allowing individuals to make informed choices Limiting the retention of personally identifiable information is another element, with anonymization of search logs one strategy for protecting privacy while enabling the improvement of search algorithms and allowing fraud detection

PANEL 3

The Reality of Our Children's Virtual World

Marc Klaas, president of the KlaasKids Foundation, moderated a panel of experts, who discussed the issues facing our children as they work and play in cyberspace

Denny Shaw, Chief Operations Officer of i-SAFE, presented information on the Internet use patterns of kids and teens, from the latest National Assessment Center annual report, At Risk Online, based on data provided by kids and teachers More than 50 million children in the United States have Internet access, with more than half having their own e-mail accounts by the sixth grade and the majority using the more popular instant messaging by the seventh grade Among the risky online behaviors noted are reckless sharing of personal information online with strangers and cyberbullying (threats or insults intended to embarrass, harass, intimidate, and terrify) The report also indicated that intellectual property theft is rampant among youths Parents overestimate what they know about their children's online activities, and as children grow older, they increasingly hide their online activities from parents Twenty percent of 5th–8th graders and 24 percent of 9th–12th graders say they are not comfortable going to their parents if they are "in trouble" online

James Harris, Special Agent, FBI, discussed recent investigations of crimes against children, including the story of a young girl who vanished for two weeks She had told others that her friends online were more real to her than her friends in real life He also discussed the difficulties in locating online predators, quoting the famous *New Yorker* cartoon, "On the Internet, no one knows you're a dog "

Hemanshu Nigam, Chief Security Officer, Fox Interactive Media and MySpace, stressed that teens live their lives online and while there are risks in the online world, the same is true in the offline world Internet safety requires bringing together a number of elements, and parents play a key role In addition to education for teens, parents, and others, advocacy organizations are important, as well as trained and effective law enforcement, sound public policy, and industry-wide leadership He described MySpace's safety efforts in the categories of contact, content, and collaboration He concluded by stating that Internet safety is a journey, not a destination

PANEL 4
Can You Find Me Now?

Kathleen Webb, Director of the Governor's Office of the Insurance Advisor, moderated a panel discussion of the privacy issues raised by the integration of wireless technology with GPS, which can enable mountain rescue to find a lost hiker, allow OnStar to unlock your car when you lose your keys, help you meet your best friend in the nearest Starbucks—or maybe expose you to a stalker

Brian Knapp, Vice President of Corporate Affairs for Loopt, Inc., outlined the "privacy by design" approach his company took in developing their new location application for mobile phones, including consulting with privacy and security organizations Loopt allows users to turn their cell phones into "a social compass " He explained that the service is permission-based, with users having the option to turn off location-sharing at any time on a friend-by-friend basis or for all friends at once The company also provides safety tips and resources for parents

Deepti Rohatgi, Policy Director, Yahoo! Inc., spoke about the importance of building customer trust in developing new products, particularly when location information is involved She cited the importance of providing notice, choice, and a positive user experience In the mobile space, achieving this can be challenging, given factors such as the small screen and emerging phone standards She emphasized the importance of starting privacy discussions early in the product development process and the need to re–evaluate policies as technological changes emerge

Chris Hoofnagle, Senior Staff Attorney at the Samuelson Law Technology & Public Policy Clinic, provided some background for the discussion of location privacy when he reported on a recent survey of Californians' attitudes towards the privacy of location data The survey found that most (65 percent) Californians understand that policy can track their location through wireless phones and that even more (83 percent) agreed that the police should be able to locate them through their cell phone in an emergency Respondents were concerned about the police having non–emergency access to such data, with more than 70 percent favoring both a subpoena standard and a stronger warrant standard before the police could obtain location information from a cell phone company

PANEL 5
Verifying Identity to Prevent Fraud

California Deputy Attorney General Robert Morgester moderated a panel of experts who discussed the challenge of fighting fraud in the online world Faced with identity theft losses of $40 billion a year, businesses are using new technologies and processes to detect and prevent fraudulent transactions

Mike Cook, Chief Operating Officer, ID Analytics, Inc., explained that businesses and consumers are facing an entirely new genre of risks in transactions, which are now both real-time and remote The reliance on consumer identity information to enable "customer not present" transactions has put the consumer's need to protect their identity at odds with a business's need to make instantaneous, yet sound, decisions The requires a new generation of identity intelligence solutions to help organizations meet the challenges of accurately assessing transaction risk in a real-time virtual world, while at the same time maintaining data security and privacy

Avivah Litan, Vice President and Distinguished Analyst, Gartner, Inc., talked about the different techniques used in new account fraud and existing account fraud, with weaknesses in identification and authentication enabling both forms She summarized best practices in combating new account fraud, which include using client device identification such as geo-location, PC fingerprinting, and keystroke biometrics, as well as stepped up applicant verification and document validation The challenge of authentication in the use of existing accounts is balancing convenience with security, which requires layering with transparent fraud detection An optimal scenario to prevent fraud escalation in the future would include credentialing by a trusted party, federated identify management, or a shared user/payer authentication and would require cooperation among government, merchants, financial services companies and Internet infrastructure players

Bill Rosenkrantz, Director of Product Management, Symantec Corp., discussed consumers' roles in protecting themselves from fraud Protection strategies include using only trusted sites when providing sensitive information, checking out new sites before providing any information, and not clicking on links in e-mails He also noted that using a zero-liability payment mechanism like a credit card is another way to reduce risk He recommended that organizations up the ante on authentication by being more diligent at customer enrollment, asking more out-of-pocket questions at the time of transactions, and using out-of-band methods such as cell phone confirmation to authenticate users

workshops

1. **Law Enforcement Workshop**
   Investigating and Prosecuting Internet Crimes Against Children
   (for law enforcement and prosecutors only—POST/MCLE)
   Deputy District Attorney Robin Sax, prosecuting attorney for the Child Sexual Assault Division of the L A County Sex Crimes Unit, conducted a two–hour training course on the investigation and prosecution of Internet crimes against children She provided law enforcement officers and prosecutors with information on new investigative techniques, as well as advice on how best to work with company experts to track down predators and other online criminals

2. **Internet Safety Program Demos** (for parents, educators)
   Denny Shaw of i-SAFE, Judi Westberg Warren of Web Wise Kids, and Laurie Nathan of NetSmartz, provided a review of their nationally recognized Internet safety programs Workshop participants learned about key program features to determine which ones would be appropriate for their children, students, or communities

3. **Privacy Practices for Preventing Medical Identity Theft**
   (for health care providers, plans, businesses)
   Recent studies have found that medical identity theft is a crime that can cause great harm to patients, practitioners, and insurers Two leading experts on the subject, Sharon Anolik of Blue Shield of California and Pam Dixon of the World Privacy Forum, presented workshop attendees with a picture of what is known about medical identity theft They also discussed practices that health care providers and plans are using to detect, prevent, and respond to this crime

4. **Protecting Card Data: PCI Data Security Standard** (for business and government)
   Large breaches of credit and debit card data at major retailers have focused the attention of the public on how retailers and other organizations secure—or don't secure—this data Kieran Norton, a Senior Manager with Deloitte & Touche's Enterprise Risk Services practice, outlined the "digital dozen" requirements that merchants, state agencies, and other organizations that collect payment card data must follow

5. **Safe Social Networking Practices** (for parents, educators)
   When your children run home from school and log on to the computer, chances are they're visiting one of the many social networking sites Sites such as MySpace, Facebook and Xanga have become the coolest places to hang out for this tech-savvy generation In this workshop, Simrin Mangat of MySpace and Nancy Willard of the Center for Safe and Responsible Internet Use provided parents and educators with an overview of how social networking sites work and how children can take part safely

6. **Your Patient Privacy Rights** (for consumers)
   Linda Ackerman, Staff Counsel for Privacy Activism, and Beth Givens, Director of the Privacy Rights Clearinghouse, described the privacy rights consumers have in relation to their medical information They offered tips for consumers on how to safeguard their medical information and provided information on new offerings such as online personal health records

7. **Law Enforcement Workshop–Recognizing Counterfeit California Driver's License**
(for law enforcement and prosecutors only—POST/MCLE)
The California driver's license contains numerous security features that law enforcement officers can use to detect counterfeits Theodora Claudio and Mary Bienko, Supervising Investigators for the California Department of Motor Vehicles with a combined 24 years of experience, demonstrated techniques for uncovering even the most sophisticated fakes

8. **Privacy Breach Response: A Table-Top Exercise** (for business and government)
Stolen laptops, lost backup tapes, and hacked databases make headlines that companies and government agencies would rather not see Ravi Inthiran, a Senior Manager with Deloitte & Touche's Security & Privacy Services practice, led an exercise that simulated a real breach incident The exercise created an experience which workshop participants could use to evaluate their own organization's breach response plans

9. **Protecting Your Computer from Viruses, Hackers, and Spies** (for consumers)
Brian Zwit of AOL advised consumers that protecting their privacy online begins at home He instructed workshop participants in how to use appropriate safety measures to protect their computers and personal information from viruses, spyware, and other evolving threats

10. **Protecting Privacy on Campus: Identity Theft Prevention for College Students**
(for consumers, higher education)
Surveys show that 18-to-24-year olds are the most likely to become victims of identity theft Yet college students may undervalue the risks they face and may not know how to manage their personal information wisely Debra Castanon, Privacy Manager with the California Office of Privacy Protection, and Jackie Reynolds, UCLA's Director of Campus Services, offered tips for college students and ideas for educators on how to build identity theft protection training into existing campus programs

11. **Top 10 Tips for Identity Theft Protection** (for consumers)
Attorney Mari Frank conducted one session of this important and timely consumer workshop, and Debra Castanon, Privacy Manager with the California Office of Privacy Protection, led another They provided tips on ways consumers can make themselves less susceptible to identity theft, a crime that victimizes more than eight million people a year Workshop participants were told how to protect their personal information in their home, in the mall, and in cyberspace

12. **What Do Kids Do Online? Music, Gaming, and More** (for parents, educators, PTA)
Have you wondered what your kids could be doing on the computer for so long? Jennifer O'Reilly of the Entertainment Software Association and Joel Flatow of the Recording Industry Association of America provided answers to that question Kids are doing everything from playing games to downloading music and watching movies These two experts provided parents and educators with tips on how they can help children enjoy what the Internet has to offer in a safe and legal manner

13. **Education for Internet Safety: Assembly in a Box** (educators, PTA)
Internet use has become an integral part of our education system and as such, schools must use new ways to promote online safety Eric Clare of the Children's Way Foundation and Denny Shaw of i-SAFE presented information on what schools are currently doing, what the future holds, and the latest methods for bringing Internet safety into the school

14. **Common Sense Practices for Protecting Children Online** (for parents)
Parents are not able to protect their children every minute of the day, and so they must give them the tools they need to make good decisions Rebecca Randall, Director of Outreach for Common Sense Media, provided parents with common sense practices for the whole family to use in the online world

15. **Recognizing Counterfeit California Driver's Licenses at the Point of Sale** (for retailers)
Identity theft and check fraud can victimize consumers and merchants alike Theodora Claudio and Mary Bienko, Supervising Investigators for the California Department of Motor Vehicles, teamed up to educate retailers on how to use the many security features built into the California driver's license to detect counterfeits and reduce fraud losses

16. **Law Enforcement Workshop: Investigating and Prosecuting Identity Theft: Advanced Topics**
(for law enforcement and prosecutors only—POST/MCLE)
Deputy District Attorney Jonathan Fairtlough from the High Tech Crime Unit of the L A County District Attorney's Office, and Joanne McNabb, Chief of the California Office of Privacy Protection, trained attendees on techniques for investigating and prosecuting identity theft, including bail issues and collecting and presenting online evidence Attendees received a number of resources, including *ID Theft Reference Manual for California Law Enforcement*, and *High Technology Crime: Email and Internet Chat Prosecutor/Investigator Resource*, both on CD-ROM

Presentations and Handouts

Panels

Emerging Technology and Our New World
Jane Horvath, Google
Harry Valetk, MetLife

The Reality of Our Children's Virtual World
Hemanshu Nigam, MySpace and Fox Interactive Media
Denny Shaw, i-SAFE

Can You Find Me Now?
Chris Hoofnagle, Samuelson Law Technology & Public Policy Clinic
Deepti Rohatgi, Yahoo!

Workshops

Internet Safety Program Demos
Denny Shaw, i-SAFE
Judi Westberg Warren, Web Wise Kids

Privacy Practices for Preventing Medical Identity Theft
Sharon Anolik, Blue Shield of California,
Pam Dixon, World Privacy Forum

Protecting Card Data: PCI Data Security Standard
Kieran Norton, Deloitte & Touche

Your Patient Privacy Rights
Linda Ackerman, PrivacyActivism and
Beth Givens, Privacy Rights Clearinghouse

Top 10 Tips for Identity Theft Protection
Debra Castanon, California Office of Privacy Protection

Education for Internet Safety: Assembly in a Box
Denny Shaw, i-SAFE

California Department of Consumer Affairs

www dca ca gov

California Office of Privacy Protection

www privacy ca gov

Office of Information Security & Privacy Protection

www oispp ca gov

State and Consumer Services Agency

www scsa ca gov

cyber safe california

protecting our children, safeguarding our privacy, securing our future