

**Workshop  
on the  
Relationship between Privacy and Security**

**May 29-30, 2002**

**Robert Thibadeau, Ph.D.  
Director of the CMU Security Research Workshop Series  
Institute for Software Research International  
School of Computer Science  
Carnegie Mellon University  
And  
Director of Security Architectures  
Seagate Technology, Inc.  
rht@cs.cmu.edu**

**Workshop Sponsored By  
AMS ([www.ams.com](http://www.ams.com))  
Wave Systems, Inc. ([www.wave.com](http://www.wave.com))**

## Summary

This workshop provided a deep exploration of how personal information privacy interplays with modern cybersecurity. The explicit management of personal information privacy has costs for the person, the enterprise, and the socio-political culture. These costs bring benefits. For people, the benefit is explicit identity management. For the enterprise, the benefit is conforming with the legal obligations and good business practices. For the culture there are express benefits to the economy.

An essential foundation for managing privacy is security. Indeed, technically strong security reinforced with well-designed policy and law, appear to reduce the costs of strong privacy while also having obvious security benefits for individuals, enterprises, and the culture. Privacy management involves using this security infrastructure to achieve the control of personal information in such a way as to support functionality. The functionality includes the control of the use of information and the anonymization without a loss of authority.

The talks explored these issues in great depth with many examples. The slides and video of the workshop are presented at the workshop web site: [www.security.scs.cmu.edu](http://www.security.scs.cmu.edu).

## Talks

### **Privacy and Security in the eMarketplace**

**Moselle W. Thompson, Commissioner, Federal Trade Commission**

The main theme of Moselle's talk was that good privacy and security are an essential part of good customer relationship management. With the economy increasingly dependent on information services as opposed to hard goods, people need to feel confident in the information infrastructure. It is simply good business to practice strong privacy and security practices. As one example, he recalled the failure of an entire industry through a loss of trust. The 900 number industry was nine billion dollars four years ago but it was only 300 million dollars last year. People associated 900 numbers with pornography and other unscrupulous uses and have abandoned the economic mechanism. Moselle pointed out that the U.S. policy involves legal rules for privacy on a case-by-case basis, and that he believed there should also be some broad rights to privacy established. The U.S. is one of the most ardent countries in protecting the privacy of the citizen with over 400 internet-related cases prosecuted by the FTC. The second greatest number of prosecutions internationally is 5 by Australia.

### **Privacy and Security**

**Robert Thibadeau, CMU/Seagate Technology**

Bob pointed out that the means and ends of information privacy and information security are essentially similar. Both depend critically on technologies for authentication, authorization, hiding, integrity checking, auditing, and availability. Both have to recognize the role of both technology and law/policy: once a secret is disclosed to exactly one other person, you have to assume the secret is out and there has to be law/policy that shapes future behavior around the exposed information.

However, the goals of privacy and security can be in conflict: one attempts to protect information about the individual and the other may require disclosure of information about the individual in order to secure information about other things. Bob used the metaphor to 'half-cooked chicken' to point out that just as incomplete security solutions lead to no security at all, incomplete privacy solutions lead to no privacy at all.

Bob outlined a number of hard problems in privacy. For one, 'privacy negotiation in a millisecond', he shows a single-token solution that could make it practical to have two way negotiations between user agents and data consumers that can occur in just a handful of data exchanges.

## **Privacy and Security – A Win-Win Situation** **David Chaum, President, Chaum LLC.**

David pointed out that legal mechanisms can't do it all. Technology is an essential participant in privacy assurance just as it is essential in security assurance. He pointed out that there are important privacy technologies that are "directly effective." This means that the technology itself insures with high confidence, direct privacy preservation. Among these technologies are anonymizing technologies that preserve authority.

David founded DigiCash which promoted a family of technologies where digital cash is possible (anonymous guarantees of payment). More generally, there needs to be a notion of 'infomediary' in order to provide directly effective privacy assurances. Finally, he pointed out that the technologies for this are all well understood and well deployed in many places. Public key methods are at the root of these technologies.

## **P3P and Privacy Bird**

**Lorrie Cranor, AT&T Labs Research, Chair of the P3P Working Group of the World Wide Web Consortium.**

Lorrie provided a comprehensive overview of the W3.org/P3P standard that was adopted April 2002. This standard enables the individual to have some control over how his personal information is used within the extensive semantics developed by P3P. She also described the "compact P3P policy" that is supported by Microsoft browsers.

The compact policy is basically a privacy policy on a cookie that permits a browser to alert users about possible violations of personal cookie privacy policies by the data consumer. Despite its recent acceptance by the W3, P3P is now supported by about a third of all major web sites and the number is growing by the day.

Finally, Lorrie demonstrated her Privacybird.com browser plugin that supports full P3P policies, not just compact policies. This is a free download that is gaining reputation as a great educational tool for consumers.

## **User-Managed Privacy Technology**

**Lark Allen, Senior Vice President, Wave Systems, Inc.**

Like Lorrie, Lark focused on privacy at the edge. However, in keeping with the need for a strong grounding in security, he focused on the need to develop user-managed privacy from strong sources of trust. Just as strong authentication is needed for good security, it is imperative in order to assure privacy from such problems as identity theft.

He mentioned that there is a tendency in privacy to veer sharply between “nuclear power” and “sticks” and that the ultimate solution seems to be in the direction of providing an ID layer for web services.

He demonstrated a Wave enhanced keyboard as a perimeter device that can provide for strong authentication while maintaining directly effective privacy.

### **The Convergence, “Submergence” and Impact of Privacy and Security Practices**

**Chris Israel, Deputy Assistant Secretary, U.S. Department of Commerce**

Chris mentioned that there are now estimated to be about 500 million people online and there are about 1.2 billion email addresses that are active. Despite this usage, the distrust people have in privacy controls has a dramatic depressing effect. Online retailers estimate a loss of about \$3.4 billion in 2001 due to privacy concerns. As one instance, about 27% of consumers report having abandoned a purchase because of privacy concerns on a web site after having made the decision to go ahead and make purchase.

Security is the biggest concern of the fortune 100 in doing business online. Sixty five percent of adults in the U.S. are extremely concerned about the government’s ability to protect personal information privacy. All this points to the need to provide the technologies and laws necessary to insure control and management of privacy and security.

### **Analysis of Corporate Privacy and Data Protection Practices**

**Larry Ponemon, CEO, Privacy Council, Inc.**

Larry talked about both individual and enterprise privacy issues and pointed out that privacy practices in corporate America are pretty dismal.

Less than 24% of corporations are in fact in compliance with their own stated privacy policies. There are also egregious violations. He mentioned a retirement community that provides free computers and free internet service to people in the community. The cost is that all the communications are monitored. This may not on the surface seem bad since these people are relatively uninteresting from the point of view of marketers, but they are using the computers to communicate with their children. So the real privacy violation is occurring indirectly.

In a survey of 181 Fortune 1000 companies, it was found that 72% had privacy policies of less than 10 pages, 19% met all well-accepted fair information practices, 21% contained a letter from executive management, 9% contain examples and illustrations, 8% were easy to read, 5% were in multiple

languages, 24% contained privacy policies toward employees, 12% explained the privacy practices.

Larry finally covered the fact that after 9-11, authentication has taken a paramount focus over privacy. However, strong authentication also provides the basis for strong anonymity with authorization. All this points to the need to bring the privacy management processes to greater levels of maturity.

**European Research in Cybersecurity and Protection of the Citizen**  
**Marc Wilikens, European Directorate – General Joint Research**  
**Center, Milan Italy**

Marc described European Commission research in security and privacy. The goals are to improve prevention, cybercrime operations, forensics, information sharing, detection, and early warning.

Privacy is viewed as a human right to informational self-determination. It follows the accepted principles of data management of fairness, consent, transparency, purpose specification, data retention, security, and access.

He pointed out that law is not self-acting and that technology must be present to support the law. He described two types of privacy technology: PET (privacy enhancing technologies) and PIT (privacy intruding technology). There are legitimate roles for both. Privacy intrusion technologies may become important in forensics and public health.

Marc showed the system started at CMU and moved to Java as the European privacy demonstrator and available at p3p.jrc.it. This is the first complete implementation of P3P and the client rule system in a proxy architecture which enables privacy proxies and enterprise privacy management.

Identity management is seen as a central problem in both security and privacy. This must be at both the edge and the enterprise and will serve the needs of security, privacy, and combating cybercrime.

**Dynamix Illustration of Anonymization**  
**Phil Hayes, Consultant, and Ganesh Mani, Chairman**

Dynamix illustrated how data mining applications could be developed that would preserve privacy despite the fact that the data mining could also be employed to invade privacy. They illustrated a data mining console that permitted analysis to proceed to more fine granularity with more risk of personal identification.

## **Dinner Talk: Talking to Strangers** **Scott Blackmer, Attorney**

Scott provided a tour-de-force of the personal and personally identifiable information that people give up to other parties on a routine daily basis.

He provided a pivotal example in the form of a story about a nude sunbathing area for monks. When some visitors accidentally came upon two monks, one monk covered his private parts and the other covered his face. When the first monk asked why the second covered his face, the second said "I don't know about you, but I am recognized by my face."

The information that may become pertinent to privacy is not always the most obvious information. Scott emphasized that this represents a real problem both for writing law and developing technology.

## **Operational Risk Management** **Jonathan Rosenour, Point Tiburon Group**

Jonathan discussed the roles of security and privacy in operational risk management. In one example of identity theft a kid in hospital in Florida saw a pile of HIV results and picked up phone and called all the people and told them they were HIV positive. Privacy practices are indeed important to risk management.

Another example of the kinds of risk management problems was the case of the Bank of Chicago. In 1996, a single ATM software error inflated over 800 customer balances by 763.9 billion dollars. JP Morgan reported 2/27/02 that insurers were denying claim for 965 million dollars on surety bonds arising from Enron failure on grounds the bonds were procured through fraud.

Arthur Anderson, a company with between 10 and 20 billion in revenues, was brought down by one memo on a retention policy by one lawyer.

In today's world where assets are intellectual, the idea is that privacy violations could cost a lot. Reputation problems can cost billions of dollars in very short time frames.

Risk management in today's world requires multi-dimensional approaches to implement and demonstrate appropriate risk management systems and processes. There must be tools for root cause analysis and alerting and these tools must be flexible, suiting any control objective, and must monitor in real time. He then reviewed the state of the art in this area. He showed that the NIST Common Criteria provides a basic framework, and overviewed a number of products that are available today that begin to give us a vision of what risk management systems will look like in the future.

## **XNS: Unifying Identity, Security, and Privacy**

**Drummond Reid, CTO of Oname, Inc., and Chairman of XNS . org**

Drummond presented a system that is nearing public release for providing identity management services on the Internet. Privacy is defined as a relationship between data controllers (agents that wish to hide or control the use of data). Security is a mechanism to hide the data. Privacy is a mechanism to control the use of the data and therefore is in the relationship between data controllers: preferences and policies between controllers generate permissions.

XNS organizes Identity trees: a person has a directory of identities: For example, down one tree from the root to a leaf would be: identity->travel->preferences->airlines->(carriers | seating). Such trees define Identity documents. XNS provides a DOM (document object model) for identity. These identity documents are indexed in a scheme similar to DNS on the Internet.

From this XNS also provides people with the capability to disclose identity information only as needed and against a contract with the data consumer who then becomes a data controller for other data consumers.

XNS is an advanced system in use by a number of large corporations and nearing the point where it will be proposed for standards work in Internet wide identity management. It well demonstrates how Identity, Security, and Privacy can be unified in an approach that also unifies both enterprise privacy management and individual privacy.

## **Making Digital Privacy Operational**

**Latanya Sweeney, Assistant Professor Computer Science and Public Policy, Carnegie Mellon University**

Latanya Sweeney focused on the problem of handling data depositories that already contain non-anonymous data and for which there is no a priori anonymization methodology. How do you anonymize this data? Instances include medical repositories, government repositories and commercial repositories.

Latanya demonstrated a number of cases where limited data extraction from a repository did not actually anonymize the data. For example, she showed a case where just the date of birth and five digit zip code, could be demonstrated to still uniquely identify a large number of individuals nationally. She illustrated how more care given to the anonymization could lead to meeting a particular anonymization requirement using just automated tools.

In the case of security, she showed pandemic situations where a first alert to a pandemic can be with a high degree of anonymity but as the certainty increases

of a real pandemic, the data gradually becomes less anonymized in keeping with the need to identify the actual parameters of the pandemic.

**International Security Trust and Privacy Alliance ([www.istpa.org](http://www.istpa.org)).**

**ISTPA Privacy Framework**

**John Sabo (Computer Associates), Chairman**

**Michael Willett (Wave Systems), Chair of the Framework Committee**

The International Security Trust and Privacy Alliance is a trade organization that is developing policy-neutral privacy architectures and studies in service to corporate and organizational needs to obey their own privacy policies, whatever these may be. The ISTPA Framework document, version 1.0, was first publicly introduced. This document is available from the ISTPA web site at [www.istpa.org](http://www.istpa.org). It contains detail on the 10 services and capabilities that any Chief Information Officer or Chief Privacy Officer should consider in auditing his own technical capabilities deliver Personal Information privacy assurances. The 10 services and capabilities are

1. Interaction
2. Negotiation
3. Control
4. Access
5. Usage
6. Validation
7. Certification
8. Audit
9. Enforcement
10. Agent

### **Hard Problems**

The conference included a number of vibrant discussions on hard problems. Perhaps the hardest problem to manifest itself was the wide range of strong views with regard to the use of language in talking about privacy. It was clear, for example, from the heated discussions following the ISTPA presentation that the use of terminology could cause immediate accusations of one sort of another. The tendency of the debate in privacy and security to be reduced to one of mistrust among the interested parties was manifested on a number of occasions. This certainly exposed the need for many open venues to develop understanding, and for strong and complete technical solutions that can show the way for privacy and security technology benefiting individuals and organizations. The understanding of privacy and security in today's age is only just beginning.

## Appendix I: Agenda

Wednesday, May 29, 2002  
Carnegie Mellon University  
GSIA Room 152 – The Bach Auditorium

- 8:45**            ***Keynote – Privacy and Security in the eMarketplace***  
Mozelle W. Thompson, Commissioner, Federal Trade Commission
- 9:30**            ***Industry Issues in Privacy and Security***  
Robert Thibadeau, Principal Research Scientist, School of  
Computer Science,  
Carnegie Mellon University
- 10:15**           ***Privacy and Security – A Win/Win Situation***  
David Chaum, Technology Innovator
- 11:15**           ***P3P and Privacy Bird***  
Lorrie Cranor (AT&T Labs Research, Chair, World Wide Web  
Consortium, P3P)
- 12:00 pm**      ***User Managed Privacy Technology Presentation***  
Wave Systems
- 1:30**            ***The Convergence, “Submergence” and Impact of Privacy and  
Security Practices***  
Chris Israel, Deputy Assistant Secretary, U.S. Department of  
Commerce
- 2:15**            ***Analysis of Corporate Privacy and Data Protection Practices***  
Larry Ponemon, CEO, Privacy Council, Inc.
- 3:15**            ***European Perspective***  
Marc Wilikens, European Directorate - General Joint Research  
Centre
- 4:00 – 4:30**   ***Database Technology Presentation***  
Dynamix, Inc.
- Dinner Presentation: “Talking to Strangers”***  
Scott Blackmer, Attorney

**Thursday, May 30, 2002**

- 8:30**            ***Operational Risk, Privacy and Security***  
Jonathan Rosenoer, President, Point Tiburon Group
- 9:15            *XNS: Unifying Identity, Security and Privacy*  
Drummond Reed, CTO, OneName Corporation and Founder,  
XNSORG
- 10:15**           ***Making Digital Privacy Operational***  
Latanya Sweeney, Asst. Professor/Computer Science & of Public  
Policy,  
Carnegie Mellon University
- 11:00**           ***ISTPA Privacy Framework***  
John Sabo, Chairman, ISTPA *and*  
Michael Willett, Ph.D., Security Architect, Wave Systems
- 11:45**           ***Hard Problems***  
Robert Thibadeau, Principal Research Scientist, School of  
Computer Science,  
Carnegie Mellon University

## Appendix II: Attendees

Mr. John Adamczak Manager - Information Security Federated Investors  
Mr. Lark M. Allen Executive Vice President Wave Systems Corp.  
Mr. Rex Althoff CIO Federated Investors  
Mr. Scott Blackmer Attorney  
Mr. Nigel Brown Senior Consultant IBM  
David Chaum Privacy Consultant Chaum, LLC  
Dr. Lorrie Cranor Principal Technical Staff Member AT&T Labs-Research  
Mr. Dwight Dietrich Vice-Chairman Dynamix Technologies  
Mr. John V. Foley President VigilantMinds Inc.  
John Harrison Associate Computer Scientist RAND  
Dr. Phil Hayes Sr VP Technology Dynamix Technologies  
Mr. William L. Hunt Research Associate West Virginia University  
Mr. Chris S. Israel Deputy Assistant Secretary U.S. Department of Commerce  
Ms. Anne F. Jackson Information Designer  
Dr. Srinivas Kankanahalli Research Associate Professor West Virginia University  
Mr. Wick Keating VP & Director of AMSCAT American Management Systems  
Mr. Andrew P. Keddie Manager, Data Security West Penn Allegheny Health System  
Mr. Jim Kezman Network Engineer Respironics Inc.  
Mr. David L. Klugman VP VigilantMinds  
Ms. Jeongwoo Ko Research Programmer Carnegie Mellon University  
Mr. Donald L. Kociela Web Development Lead UPMC Health System  
Dr. Chris Long Postdoctoral Research Fellow Carnegie Mellon University  
Mr. Christopher E. Maher President Fosforus  
Mr. Charles Mance Director of Information Technology Respironics Inc.  
Dr. Ganesh Mani Chairman Dynamix Technologies  
Mr. Julie E. Mehan Director EWA IIT  
Ms. Enid Miller Vice-President & Corporate Privacy Officer Mellon Financial  
Mr. Jonathan A. Moore Attorney  
Dr. Lisa S. Nelson Assistant Professor Graduate School of Public and International Affairs  
Mr. John R. Nestor Persistent Data Systems, Inc.  
Miss Donna M. Olszewski Web Manager UPMC Health System  
Mr. Kevin O'Neil Executive Director International Security, Trust & Privacy Alliance  
Dr. Jon M. Peha Associate Director, Center for Wireless and Broadband Networks  
Carnegie Mellon University  
Ms. Stephanie Perrin Chief Privacy Officer Zero-Knowledge Systems Inc.  
Mr. Timothy J. Pittman Web Systems Engineer Respironics, Inc.  
Dr. Larry A. Ponemon Chief Executive Officer Privacy Council, Inc.  
Mr. Drummond Reed CTO OneName Corp.  
Mr. Gary S. Roboff Senior Consultant BITS - The Financial Services Roundtable  
Mr. Jonathan Rosenoer President Point Tiburon Group  
Mr. John T. Sabo Manager, Security, Privacy, Trust Initiatives Computer Associates  
Ms. Antonia L. Scarlata Carnegie Mellon Data Privacy Lab

Dr. Michael I. Shamos Co-Director, Security Workshop Series Carnegie Mellon University  
Mr. Peter M. Shane Director, Institute for the Study of Info. Tech. and Society Heinz School of Public Policy and Management  
Dr. Stuart Shapiro Senior Information Security Scientist MITRE Corporation  
Dr. Latanya A. Sweeney Asst. Professor/Computer Science & of Public Policy Carnegie Mellon University  
Mr. Ashoke S. Talukdar Manager, Information Security & Compliance The MetroHealth System  
Dr. Robert Thibadeau Principal Research Scientist, School of Computer Science Carnegie Mellon University  
Mr. Mozelle W. Thompson Commissioner Federal Trade Commission (FTC)  
Mr. Adriaan W. Veldhuisen NCR Corporation  
Dr. Marc Wilikens Joint Research Centre  
Dr. Michael Willett Consultant Wave Systems Corp.  
Mr. John A. Winegarden Web Developer UPMC Health System  
Mr. Edward T. Yablonski VP Business Development Dynamix Technologies