Managing Identity: Bringing Administrative, Legal, and Technology Controls Together

Privacy Symposium
August 20, 2008

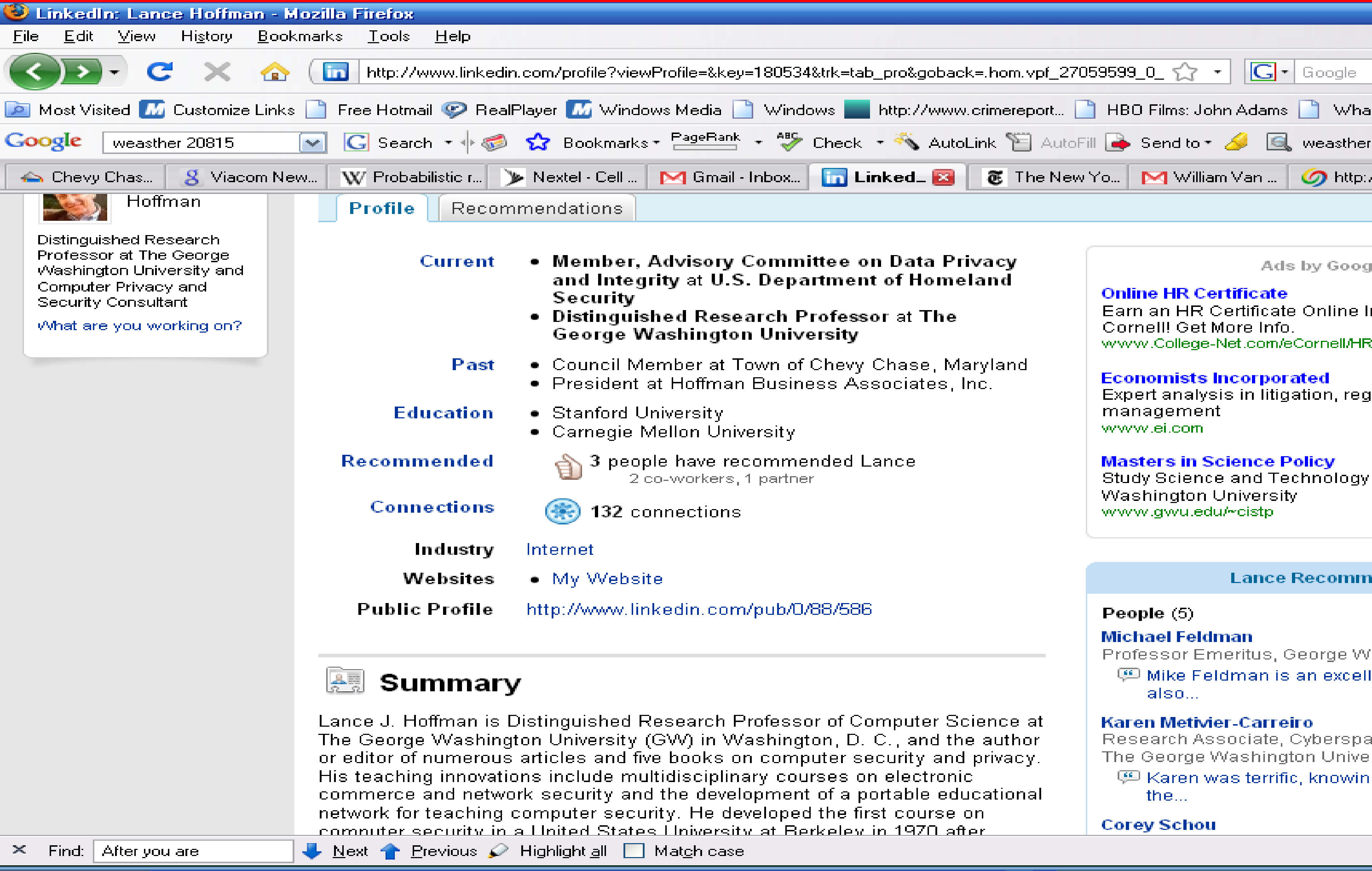
Lance J. Hoffman[1]
Cheryl Enokawa[2]

The George Washington University
Washington, DC

[1]Distinguished Research Professor, Computer Science Department, lanceh@gwu.edu
[2]CyberCorps Scholar, Computer Science Department, enokawac@gwu.edu

Managing Identity in the Future

Much more professional networking



Hoffman

Distinguished Research Professor at The George Washington University and Computer Privacy and Security Consultant

What are you working on?

Current
- **Member, Advisory Committee on Data Privacy and Integrity at U.S. Department of Homeland Security**
- **Distinguished Research Professor at The George Washington University**

Past
- Council Member at Town of Chevy Chase, Maryland
- President at Hoffman Business Associates, Inc.

Education
- Stanford University
- Carnegie Mellon University

Recommended
3 people have recommended Lance
2 co-workers, 1 partner

Connections
132 connections

Industry Internet

Websites
- My Website

Public Profile http://www.linkedin.com/pub/0/88/586

Summary

Lance J. Hoffman is Distinguished Research Professor of Computer Science at The George Washington University (GW) in Washington, D. C., and the author or editor of numerous articles and five books on computer security and privacy. His teaching innovations include multidisciplinary courses on electronic commerce and network security and the development of a portable educational network for teaching computer security. He developed the first course on computer security in a United States University at Berkeley in 1970 after

Lance Recomm

People (5)

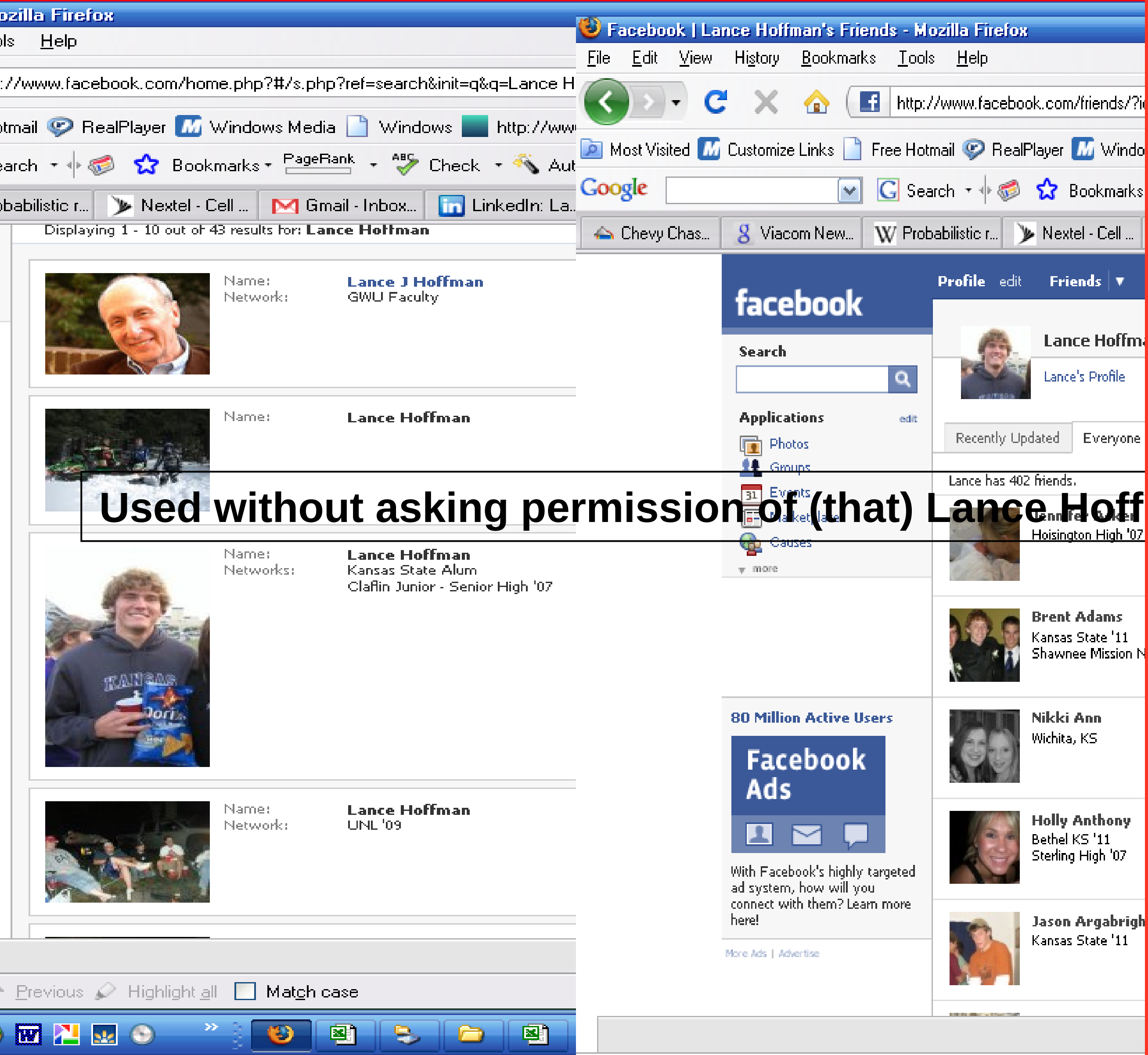
Michael Feldman
Professor Emeritus, George W
Mike Feldman is an excell also...

Karen Metivier-Carreiro
Research Associate, Cyberspa
The George Washington Unive
Karen was terrific, knowin the...

Corey Schou

Managing Identity in the Future

Much more social networking (too much?)


ozilla Firefox
ols Help
://www.facebook.com/home.php?#/s.php?ref=search&init=q&q=Lance H
otmail RealPlayer Windows Media Windows http://www
earch Bookmarks PageRank Check Aut
obabilistic r... Nextel - Cell ... Gmail - Inbox... LinkedIn: La...
Previous Highlight all Match case
Facebook | Lance Hoffman's Friends - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.facebook.com/friends/?i
Most Visited Customize Links Free Hotmail RealPlayer Windo
Google Search Bookmarks
Chevy Chas... Viacom New... Probabilistic r... Nextel - Cell ...
facebook
Profile edit Friends
Search
Applications edit
Photos
Groups
Events
Marketplace
Causes
more
Recently Updated Everyone
80 Million Active Users
Facebook Ads
More Ads | Advertise

Displaying 1 - 10 out of 43 results for: Lance Hoffman

Name:	Lance J Hoffman
Network:	GWU Faculty
Name:	Lance Hoffman
Name:	Lance Hoffman
Networks:	Kansas State Alum Claflin Junior - Senior High '07
Name:	Lance Hoffman
Network:	UNL '09

Lance Hoffm
Lance's Profile

Lance has 402 friends.

Jennifer Acker
Hoisington High '07

Brent Adams
Kansas State '11
Shawnee Mission N

Nikki Ann
Wichita, KS

Holly Anthony
Bethel KS '11
Sterling High '07

Jason Argabrigh
Kansas State '11

With Facebook's highly targeted ad system, how will you connect with them? Learn more here!

Used without asking permission of (that) Lance Hoff

Hackers' Latest Target: Social Networking Sites

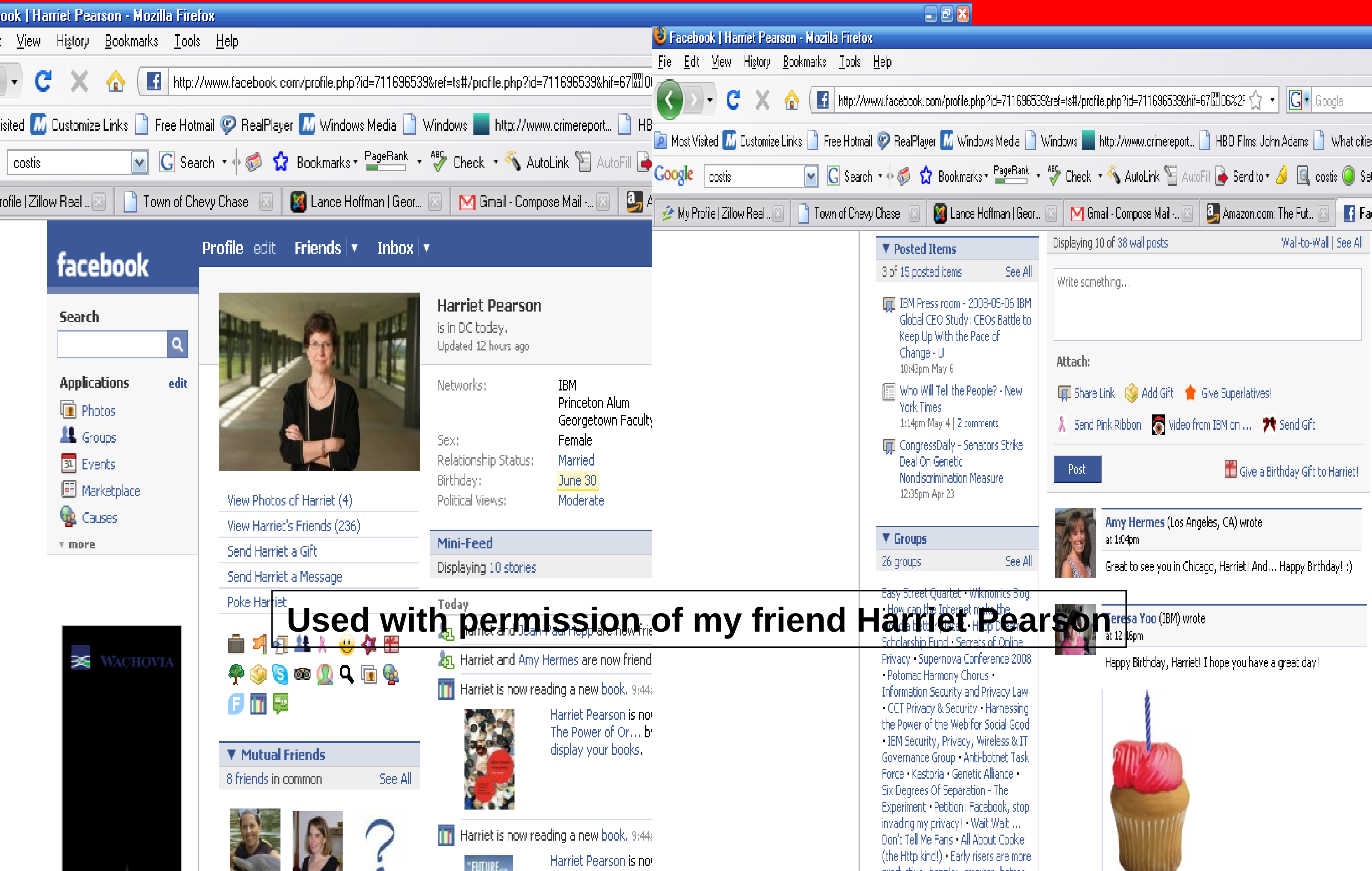
By Brian Krebs
Washingtonpost.com Staff Writer
Saturday, August 9, 2008; D01

LAS VEGAS -- Social networking sites such as Facebook, MySpace and LinkedIn are fast emerging as some of the most fertile grounds for malicious software, identity thieves and online mischief-makers. And while some of the talks given here at Black Hat, one of the larger hacker conferences in the country, would probably make most people want to avoid the sites altogether, it turns out that staying off these networks may not be the safest option, either.

…

Paradoxically, there may be a danger in remaining a social networking site Luddite. After all, if you don't claim a space on these networks, someone else may do it for you as a way of scamming or attacking your friends and business contacts. **With the permission and good humor of security pioneer Marcus Ranum, Hamiel and Moyer created a LinkedIn profile on Ranum's behalf, including a photo of him and bits from his résumé to make the profile look legit. In less than 24 hours, more than 50 people had joined his LinkedIn network. Among those taken in by the stunt was Ranum's sister.**

Is this social or professional networking or both, and does it matter, and if so, why?


Facebook | Harriet Pearson - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.facebook.com/profile.php?id=711696539&ref=ts#/profile.php?id=711696539&hif=67
Most Visited · Customize Links · Free Hotmail · RealPlayer · Windows Media · Windows · http://www.crimereport... · HBO Films: John Adams · What cities
Google · costis · Search · Bookmarks · PageRank · Check · AutoLink · AutoFill · Send to
My Profile | Zillow Real ... · Town of Chevy Chase · Lance Hoffman | Geor... · Gmail - Compose Mail ... · Amazon.com: The Fut...
facebook
Profile edit · Friends · Inbox
Search
Applications edit
Photos
Groups
Events
Marketplace
Causes
more
WACHOVIA

Harriet Pearson
is in DC today.
Updated 12 hours ago

Networks:	IBM Princeton Alum Georgetown Faculty
Sex:	Female
Relationship Status:	Married
Birthday:	June 30
Political Views:	Moderate

View Photos of Harriet (4)
View Harriet's Friends (236)
Send Harriet a Gift
Send Harriet a Message
Poke Harriet

Mini-Feed
Displaying 10 stories
Today
Harriet and Jean Paul Hepp are now frie
Harriet and Amy Hermes are now friend
Harriet is now reading a new book. 9:44
Harriet Pearson is no The Power of Or... b display your books.
Harriet is now reading a new book. 9:44
Harriet Pearson is no

Mutual Friends
8 friends in common See All

Posted Items
3 of 15 posted items See All

IBM Press room - 2008-05-06 IBM Global CEO Study: CEOs Battle to Keep Up With the Pace of Change - U
10:43pm May 6

Who Will Tell the People? - New York Times
1:14pm May 4 | 2 comments

CongressDaily - Senators Strike Deal On Genetic Nondiscrimination Measure
12:35pm Apr 23

Groups
26 groups See All

Easy Street Quartet • Wikinomics Blog • How can the Internet make the ... Scholarship Fund • Secrets of Online Privacy • Supernova Conference 2008 • Potomac Harmony Chorus • Information Security and Privacy Law • CCT Privacy & Security • Harnessing the Power of the Web for Social Good • IBM Security, Privacy, Wireless & IT Governance Group • Anti-botnet Task Force • Kastoria • Genetic Alliance • Six Degrees Of Separation - The Experiment • Petition: Facebook, stop invading my privacy! • Wait Wait ... Don't Tell Me Fans • All About Cookie (the Http kind!) • Early risers are more

Displaying 10 of 38 wall posts Wall-to-Wall | See All

Write something...

Attach: Share Link · Add Gift · Give Superlatives! · Send Pink Ribbon · Video from IBM on ... · Send Gift

Post · Give a Birthday Gift to Harriet!

Amy Hermes (Los Angeles, CA) wrote
at 1:04pm
Great to see you in Chicago, Harriet! And... Happy Birthday! :)

Teresa Yoo (IBM) wrote
at 12:16pm
Happy Birthday, Harriet! I hope you have a great day!

Used with permission of my friend Harriet Pearson

Facebook’s Privacy Policy

… when printed out is nine pages (3,753 words) long

Will someone please tell me what its third-party privacy policy (1,212 words below) means?

Sharing Your Information with Third Parties

Facebook is about sharing information with others — friends and people in your networks — while providing you with privacy settings that restrict other users from accessing your information. We allow you to choose the information you provide to friends and networks through Facebook. Our network architecture and your privacy settings allow you to make informed choices about who has access to your information. We do not provide contact information to third party marketers without your permission. We share your information with third parties only in limited circumstances where we believe such sharing is 1) reasonably necessary to offer the service, 2) legally required or, 3) permitted by you. For example:

Your News Feed and Mini-Feed may aggregate the information you provide and make it available to your friends and network members according to your privacy settings. You may set your preferences for your News Feed and Mini-Feed on your Privacy page.

Unlike most sites on the Web, Facebook limits access to site information by third party search engine "crawlers" (e.g. Google, Yahoo, MSN, Ask). Facebook takes action to block access by these engines to personal information beyond your name, profile picture, and limited aggregated data about your profile (e.g. number of wall postings).

We may provide information to service providers to help us bring you the services we offer. Specifically, we may use third parties to facilitate our business, such as to host the service at a co-location facility for servers, to send out email updates about Facebook, to remove repetitive information from our user lists, to process payments for products or services, to offer an online job application process, or to provide search results or links (including sponsored links). In connection with these offerings and business operations, our service providers may have access to your personal information for use for a limited time in connection with these business activities. Where we utilize third parties for the processing of any personal information, we implement reasonable contractual and technical protections limiting the use of that information to the Facebook-specified purposes.

If you, your friends, or members of your network use any third-party applications developed using the Facebook Platform ("Platform Applications"), those Platform Applications may access and share certain information about you with others in accordance with your privacy settings. You may opt-out of any sharing of certain or all information through Platform Applications on the Privacy Settings page. In addition, third party developers who have created and operate Platform Applications ("Platform Developers"), may also have access to your personal information (excluding your contact information) if you permit Platform Applications to access your data. Before allowing any Platform Developer to make any Platform Application available to you, **Facebook requires the Platform Developer to enter into an agreement which, among other things, requires them to respect your privacy settings** and strictly limits their collection, use, and storage of your information. However, while we have undertaken contractual and technical steps to restrict possible misuse of such information by such Platform Developers, we of course cannot and do not guarantee that all Platform Developers will abide by such agreements. **Please note that Facebook does not screen or approve Platform Developers and cannot control how such Platform Developers use any personal information that they may obtain in connection with Platform Applications. In addition, Platform Developers may require you to sign up to their own terms of service, privacy policies or other policies, which may give them additional rights or impose additional obligations on you**, so please make sure to review these terms and policies carefully before using any Platform Application. You can report any suspected misuse of information through the Facebook Platform and we will investigate any such claim and take appropriate action against the Platform Developer up to and including terminating their participation in the Facebook Platform and/or other formal legal action.

We occasionally provide demonstration accounts that allow non-users a glimpse into the Facebook world. Such accounts have only limited capabilities (e.g., messaging is disabled) and passwords are changed regularly to limit possible misuse.

We may be required to disclose user information pursuant to lawful requests, such as subpoenas or court orders, or in compliance with applicable laws. We do not reveal information until we have a good faith belief that an information request by law enforcement or private litigants meets applicable legal standards. Additionally, we may share account or other information when we believe it is necessary to comply with law, to protect our interests or property, to prevent fraud or other illegal activity perpetrated through the Facebook service or using the Facebook name, or to prevent imminent bodily harm. This may include sharing information with other companies, lawyers, agents or government agencies.

We let you choose to share information with marketers or electronic commerce providers through sponsored groups or other on-site offers.

We may offer stores or provide services jointly with other companies on Facebook. You can tell when another company is involved in any store or service provided on Facebook, and we may share customer information with that company in connection with your use of that store or service.

Facebook Beacon is a means of sharing actions you have taken on third party sites, such as when you make a purchase or post a review, with your friends on Facebook. In order to provide you as a Facebook user with clear disclosure of the activity information being collected on third party sites and potentially shared with your friends on Facebook, we collect certain information from that site and present it to you after you have completed an action on that site. You have the choice to have Facebook discard that information, or to share it with your friends.

To learn more about the operation of the service, we encourage you to read the tutorial here. To opt out of the service altogether, click here.

Like many other websites that interact with third party sites, we may receive some information even if you are logged out from Facebook, or that pertains to non-Facebook users, from those sites in conjunction with the technical operation of the system. In cases where Facebook receives information on users that are not logged in, or on non-Facebook users, we do not attempt to associate it with individual Facebook accounts and will discard it.

If the ownership of all or substantially all of the Facebook business, or individual business units owned by Facebook, Inc., were to change, your user information may be transferred to the new owner so the service can continue operations. In any such transfer of information, your user information would remain subject to the promises made in any pre-existing Privacy Policy.

When you use Facebook, certain information you post or share with third parties (e.g., a friend or someone in your network), such as personal information, comments, messages, photos, videos, Marketplace listings or other information, may be shared with other users in accordance with the privacy settings you select. All such sharing of information is done at your own risk. **Please keep in mind that if you disclose personal information in your profile or when posting comments, messages, photos, videos, Marketplace listings or other items , this information may become publicly available.**

Managing Identity in the Future

What about privacy in third party applications*?

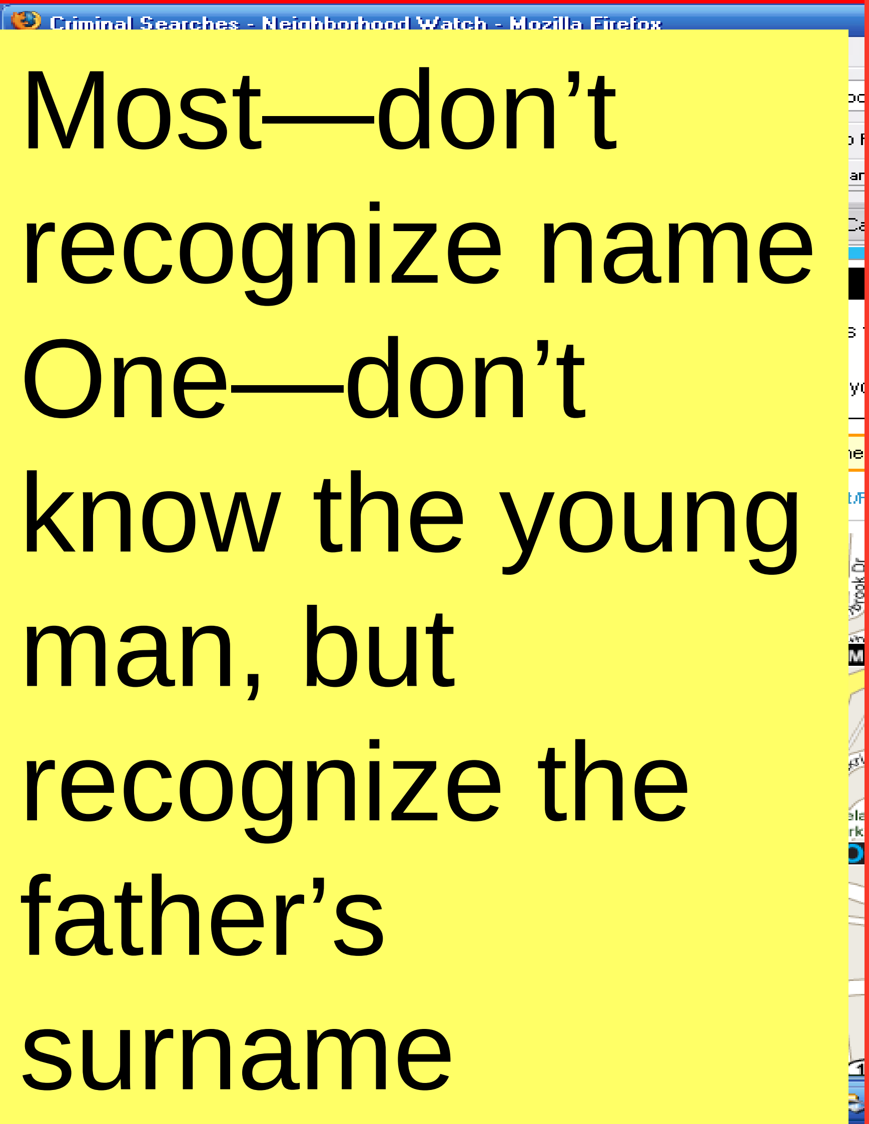
- Defaults are typically set to encourage a lot of sharing
- There are app-checkers for privacy written by unknown suppliers, since third party application defaults may allow (and even coerce) even more sharing

- But even these app-checkers may have permissive defaults

- And, of course, it’s easy to share these, with their permissive defaults, with your “friends”

“Third party applications” often involve “generative systems” (Jonathan Zittrain, *The Future of the Internet and How to Stop It*, Yale University Press, 2008)

Lurching towards the panopticon?



Most—don’t recognize name

One—don’t know the young man, but recognize the father’s surname

Prof. Lawrence Lessig of Stanford Law School says that the average Internet user is living increasingly in a "panopticon-like" environment, where Web users can be observed without being able to tell whether they are being watched. Internet protocol addresses are extraordinarily efficient fingerprints, he says. "So anybody who thinks you're going to get on the Web and be anonymous is just ignorant about the way the Web functions."

Components of Decentralized (“Federated”) Identity Management Systems

Dhamija, Rachna and Lisa Dusseault. *“The Seven Flaws of Identity Management”* IEEE: Security and Privacy 6.2 (March/April 2008): 24-29

- Identity Provider (IdP): Issues identities or credentials to users (they log in to it and may store attributes of common interest to share with various service providers (SPs)
- Relying Party (RP): Depends on the IdP to check the user credentials before it allows users to access services on a website.
  - An RP is a web application such as a expense-reporting application that offloads authentication to a third party or an Identity Provider.
  - Any service provider (SP) can be an RP
- User: Individual who assumes a digital identity to use the services online.
- User Agent: a browser or other software application that runs on any computer or PDA.

Challenges and Solutions in Identity Management

Dhamija, Rachna and Lisa Dusseault. *“The Seven Flaws of Identity Management”* IEEE: Security and Privacy 6.2 (March/April 2008): 24-29

- Identity management is not a goal in itself (give users what they want)
- Users follow the path of least resistance (make it the secure path)
- Reduce cognitive burden -- Think of how your system will be used in the larger context of other systems. Don’t replace one burden with another.
- Reduce the number of trust decisions users have to make, since repeated user consent could lead to maximum information disclosure
- Use mutual authentication (not just user authentication). Assume that your systems and users will be attacked and design your systems with that in mind.
- Relying Parties (RPs) (like service and application providers) want to control the customer experience, so offer them some control over the customer relationship, security of their accounts, and user experience
- Trust must be earned, so be trustworthy

Data Breach Management

Justice Breyer Is Among Victims in Data Breach Caused by File Sharing

WashingtonPost.com, July 9, 2008; A01

Jones, Michael E. *"Data Breaches: Recent Developments in the Public and Private Sectors"*
I/S: A Journal of Law and Policy for the Information Society Vol 3, Issue 3 (Winter 2007-2008): 555-580

- **Federal Government Breaches**
  - **Majority due to physical theft of electronic storage devices and accidental publication of personal information over the internet.**
  - Biggest source is the 1,100 laptops stolen, missing, lost since 2001
- **Federal government created "ID Theft Task Force" with new guidelines from OMB – Agencies must**
  - **Safeguard information under existing law and reduce the use of SSN.**
  - **Report data breaches to US-CERT within 1 hour of identifying breach**
  - **Develop external notification procedures**
    - When to notify, timeliness, notification source, contents, means of providing the notification, who receives it
    - Must consider nature of elements breached, number of individuals affected, likelihood the breach may lead to harm. likelihood the information is accessible and useable, ability of the agency to mitigate the risk of harm
- As of June 20, 2008, at least **44 states, the District of Columbia and Puerto Rico have enacted legislation requiring notification of security breaches involving personal information.**

  http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm
- **Federal legislation introduced**

Some Definitions

- Identification
  - Mapping a known quantity (name like John Smith or identifier like Unix) to an unknown quantity (user, system, etc.) so as to make it known
- Authentication
  - verifying a person's (or system's) identity
- Authorization
  - verifying that a known person (or agent or program) has the authority to perform a certain operation

(Often problems arise when identification is confused with authentication.)

Technical Controls for Security and Privacy – Authentication

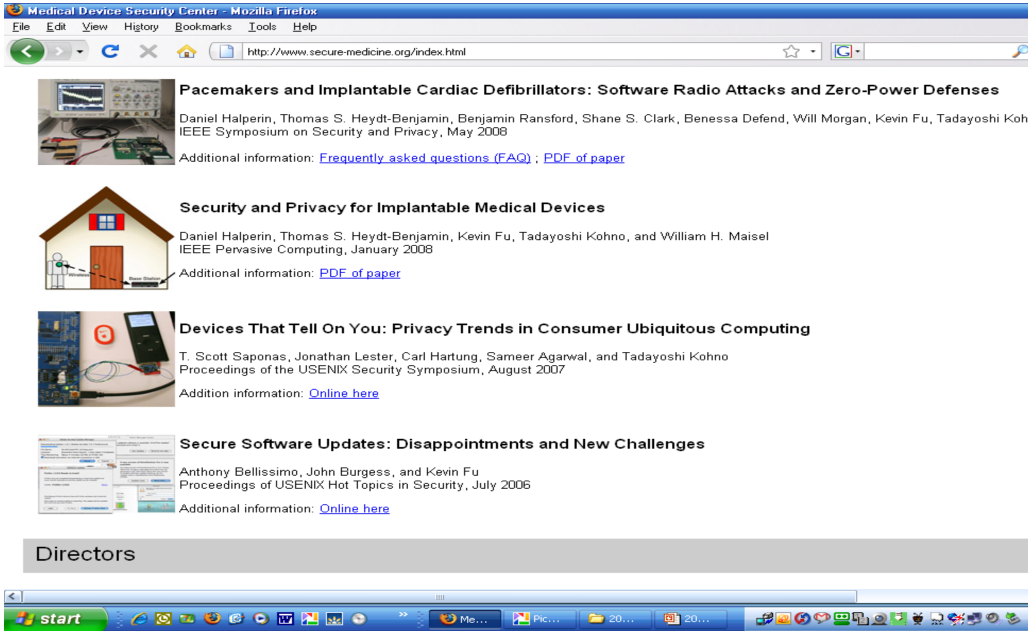
Authentication: Verifying a person's (or system's) identity

- Something you know
  - Passwords – traditional
  - Passwords – federated
  - Passphrases, images, challenge responses
- Something you have
  - Physical (machine-readable) token

May include RFID tags in cards, driver licenses, passports, clothing, etc. (these are often unencrypted and may also contain personally identifiable information that can be read by unauthorized and unauthenticated RFID readers)

IEEE Security & Privacy Best Paper Award

http://www.secure-medicine.org/index.html


Medical Device Security Center - Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
http://www.secure-medicine.org/index.html
Wireless
Base Station
start
Me...
Pic...
20...
20...

Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Koh
IEEE Symposium on Security and Privacy, May 2008

Additional information: Frequently asked questions (FAQ) ; PDF of paper

Security and Privacy for Implantable Medical Devices

Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H. Maisel
IEEE Pervasive Computing, January 2008

Additional information: PDF of paper

Devices That Tell On You: Privacy Trends in Consumer Ubiquitous Computing

T. Scott Saponas, Jonathan Lester, Carl Hartung, Sameer Agarwal, and Tadayoshi Kohno
Proceedings of the USENIX Security Symposium, August 2007

Addition information: Online here

Secure Software Updates: Disappointments and New Challenges

Anthony Bellissimo, John Burgess, and Kevin Fu
Proceedings of USENIX Hot Topics in Security, July 2006

Additional information: Online here

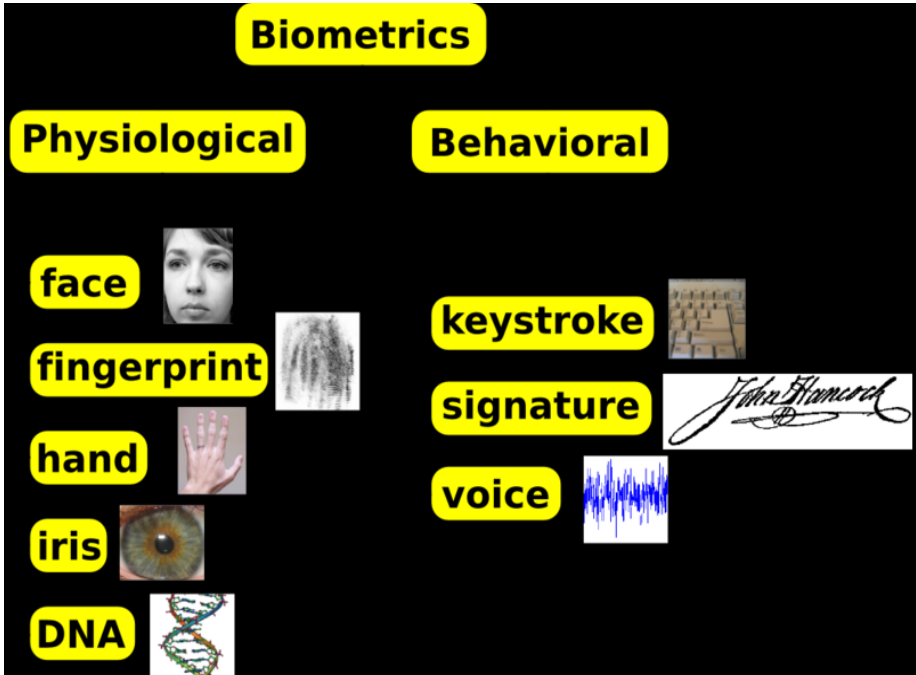
Directors

Technical Controls for Security and Privacy -- Authentication

- Something you know
  - Passwords – traditional
  - Passwords – federated
  - Passphrases, images, challenge responses
- Something you have
  - Physical (machine-readable) token
- Something you are

At Walt Disney World biometric measurements are taken from the fingers of guests to ensure that the person's ticket is used by the same person from day to day

Source: Wikipedia

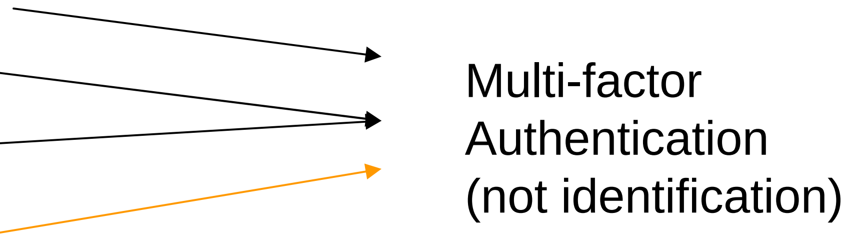


Technical Controls for Security and Privacy Authentication -- Biometrics

Wayman, James L. *“Biometrics in Identity Management Systems”* IEEE: Security and Privacy 6.2 (March/April 2008): 30-37.

- Biometrics reduce need for other identifiers
- Still have to safeguard the data representing the biometrics
- Helpful when used in conjunction with other items

  (“multi-factor authentication”)
- Example
  - Something you know
  - Something you have
  - Your location
  - Something you are

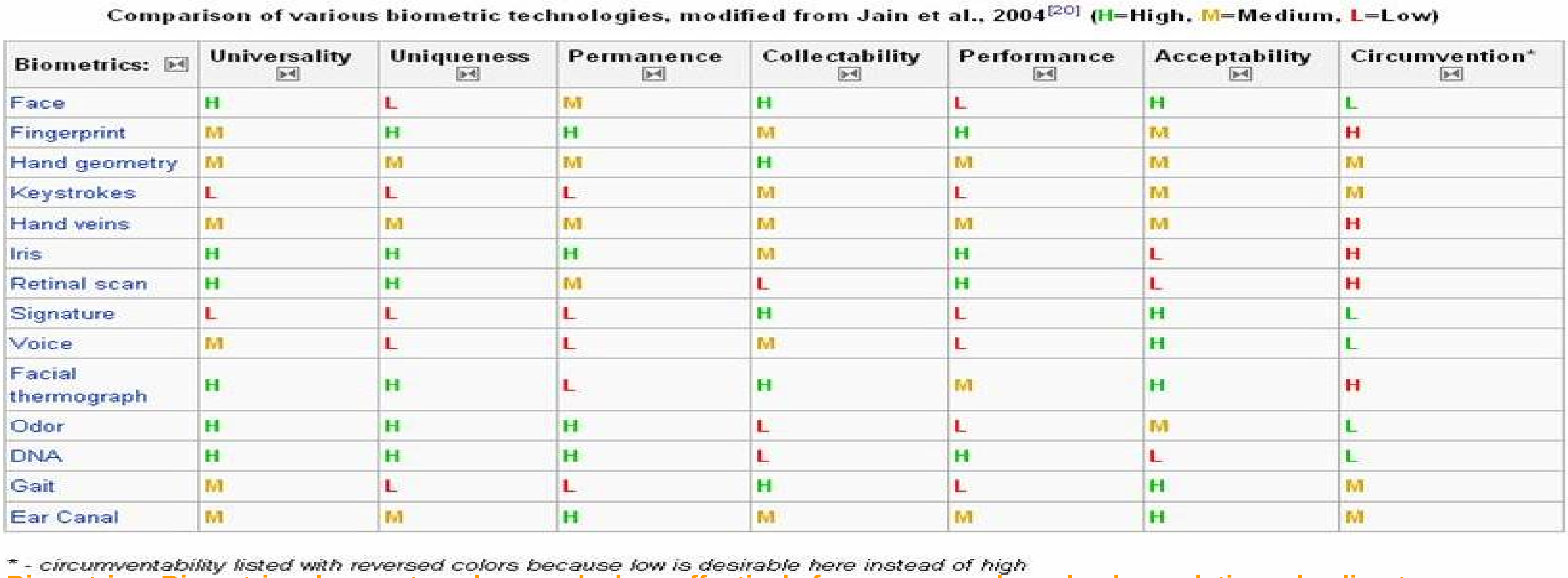


Multi-factor Authentication (not identification)

Comparison of Biometrics

Jain, A. K.; Ross, Arun & Prabhakar, Salil (January 2004),
"An introduction to biometric recognition",
IEEE Transactions on Circuits and Systems for Video Technology 14th (1): 4 - 20

Universality: each person should have the characteristic; **Uniqueness:** is how well the biometric separates individually from another; **Permanence:** measures how well a biometric resists aging; **Collectability:** ease of acquisition for measurement; **Performance:** accuracy, speed, and robustness of technology used; **Acceptability:** degree of approval of a technology; **Circumvention** : ease of use of a substitute.



Comparison of various biometric technologies, modified from Jain et al., 2004[20] (H=High, M=Medium, L=Low)

Biometrics:	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention*
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand geometry	M	M	M	H	M	M	M
Keystrokes	L	L	L	M	L	M	M
Hand veins	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retinal scan	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial thermograph	H	H	L	H	M	H	H
Odor	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear Canal	M	M	H	M	M	H	M

** - circumventability listed with reversed colors because low is desirable here instead of high*

Biometrics: Biometrics does not work or works less effectively for some people and subpopulations, leading to many false positives and negatives. Biometrics can become shared secrets. Biometrics used at the periphery by millions of readers don't solve many problems of accuracy and fraud in core databases --

Peter Swire and Cassandra Butts, "The ID Divide: Addressing the Challenges of Identification and Authentication in American Society", Center for American Progress, https://americanprogress.org

Building a System that Manages Identity

Landau, Susan and Deirdre Mulligan. *"I'm Pc01002/SpreingPeeper/ED288l.6; Who are you?"*
<u>IEEE: Security and Privacy</u> 6.2 (March/April 2008): 13-15
Hansen, Marit, Ari Schwartz, and Alissa Cooper. "*Privacy and Identity Management",*
<u>IEEE: Security and Privacy</u> 6.2 (March/April 2008): 38-45

- Determine whether identity is necessary
  - What is the application?
  - What are its uses?
  - What is the larger context?
- If identity is necessary,
  - consider identity risks
    - What can go wrong with the system, or what are the initiators or initiating events (undesirable starting events) that lead to adverse consequences)?
    - What and how severe are the potential problems or the adverse consequences?
    - How likely to occur are these undesirable consequences, or what are their probabilities or frequencies?
  - Discourage unnecessary linkages -- Ex: separate medical PII from other PII and from non-PII
- Implement privacy and security during design ("build in, don't bolt on")
  - Resist using a single credential for multiple purposes (see federated identity management systems)
- Adopt trust-enhancing measures …

Building a System that Manages Identity

Adopt Trust-Enhancing Measures

- **Be a Trustworthy Gatekeeper so users will choose you over competition**
- **Take advantage of previous work (don't reinvent the wheel)**

Ex: Microsoft Privacy Guidelines for Developing Software Products and Services

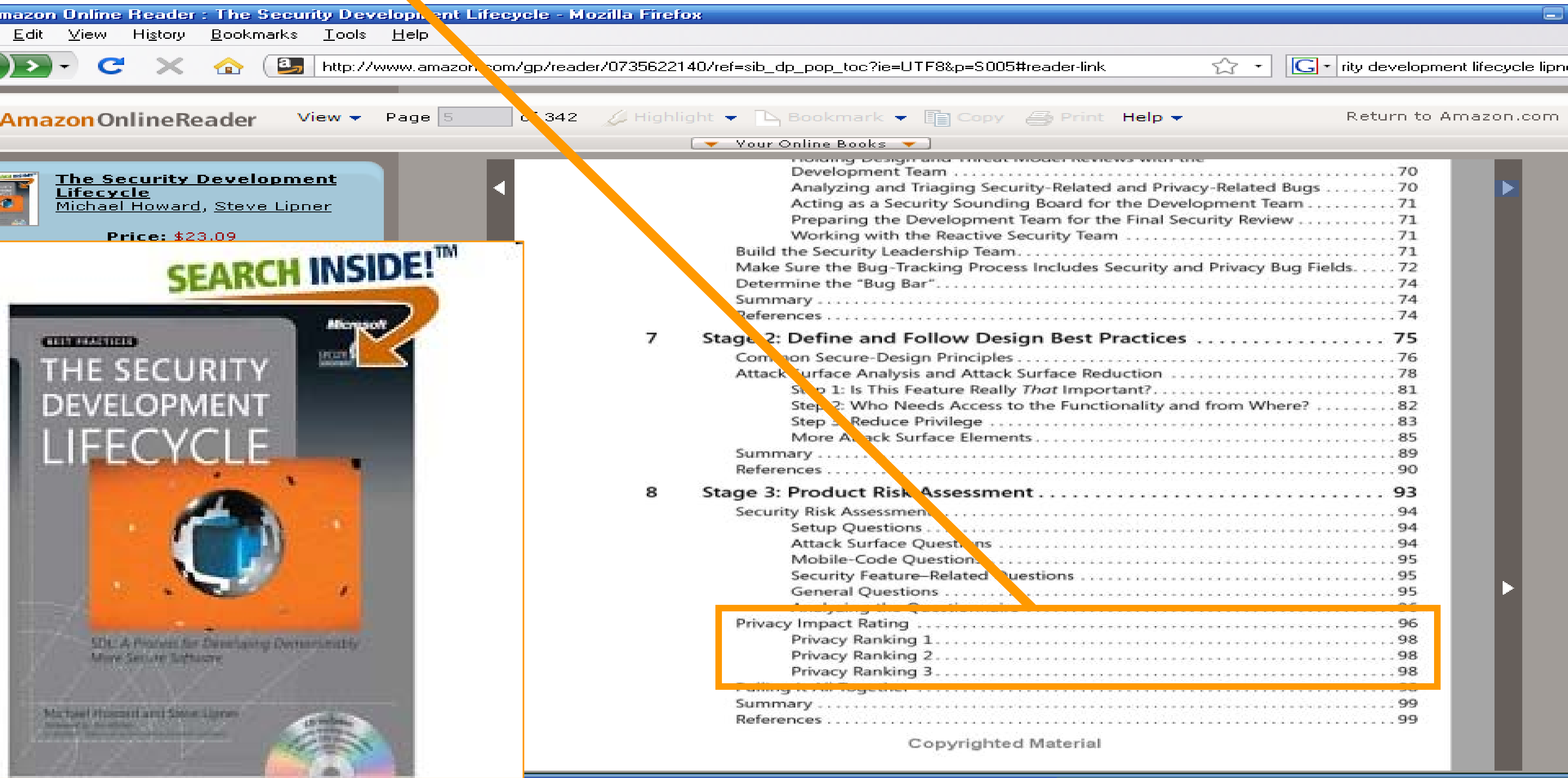
http://www.microsoft.com/downloads/details.aspx?FamilyId=C48CF80F-6E87-48F5-83EC-A18D1AD2FC1F&displaylang=en

Scenario 1: Transferring PII to and from the Customer's System
Scenario 2: Storing PII on the Customer's System
Scenario 3: Transferring Anonymous Data from the Customer's System
Scenario 4: Installing Software on a Customer's System
Scenario 5: Deploying a Website
Scenario 6: Storing and Processing User Data at the Company
Scenario 7: Transferring User Data Outside the Company
Scenario 8: Interacting with Children
Scenario 9: Server Deployment

Building a System that Manages Identity

Adopt Trust-Enhancing Measures

Privacy is in the Security Development Lifecycle for Computer Software So get to know and work with your security people; suggest using something like the following to build security and privacy together.


mazon Online Reader : The Security Development Lifecycle - Mozilla Firefox
Edit
View
History
Bookmarks
Tools
Help
http://www.amazon.com/gp/reader/0735622140/ref=sib_dp_pop_toc?ie=UTF8&p=S005#reader-link
rity development lifecycle lipn
AmazonOnlineReader
View
Page 5 of 342
Highlight
Bookmark
Copy
Print
Help
Return to Amazon.com
Your Online Books
The Security Development Lifecycle
Michael Howard, Steve Lipner
Price: $23.09
SEARCH INSIDE!™
Microsoft
THE SECURITY DEVELOPMENT LIFECYCLE
SDL: A Process for Developing Demonstrably More Secure Software
Michael Howard and Steve Lipner

Privacy Management Insights

Ryan West, “The Psychology of Security”, Communications of the ACM 51:4 (April 2008), pp. 34-40

Work with, not against, human psychology

Users routinely multitask and if bad things have not happened to them in the past tend to not read relevant text (e.g., privacy statements)

Possible solutions:

- Increase user awareness (outreach program)
- Create alerts and messages that are distinguishable from other messages and have a higher level of importance when seen,
- These alerts should not get in the way of users’ primary goals (users are often in the middle of a task when the system asks them to make a security and privacy decision that may require diverting their attention to it)
- Increase awareness that web traffic is being monitored

Identity in the Future

Research in progress to address privacy and security issues

Strengthening authentication while increasing usability (example: financial institutions)

Assessing linkability of online data to individuals (statistical inference issues)

Establishing trust using reputation rather than traditional identification and authentication. (eBay, PGP)

Creating a set of standardized agreements by which sites can offer and users can select the terms under which they agree to share their information.

- Needed especially for incipient social and professional networking sites
- Some steps towards this already taken in the technology
  - P3P (one of first general metadata description languages)
  - Google's "Protocol Buffers," an open source data description language that the company developed for internal use (a "simpler, smaller, and faster XML" (Extensible Markup Language))
  - PRIME - Privacy and Identity Management for Europe (EU-funded)
  - Policy Aware Web, funded by NSF, a collaboration between MINDSWAP and DIG to work toward creating discretionary, rules-based access for the World Wide Web.
  - The Transparent Accountable Datamining Initiative (TAMI) Project, funded by NSF, is creating technical, legal, and policy foundations for transparency and accountability in large-scale aggregation and inferencing across heterogeneous information systems.
  - OASIS XACML (Organization for the Advancement of Structured Information Standards eXtensible Access Control Markup Language)