Privacy in an Online World – Fact or Fantasy?

Ellis Holman
IBM Corp.

Wednesday, August 10,2011
Session Number 9773

Disclaimer

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS AND/OR SOFTWARE.

Introduction

- This is ***not*** a political presentation, although the nature of the subject matter in today's global political climate does have political overtones.
- This ***is*** a technical presentation.
- There is no technology, no matter how benign in concept, that cannot be subverted for evil ends.

"Those who would give up essential liberty
to purchase a little temporary safety,
deserve neither liberty nor safety."
Benjamin Franklin

Privacy - Definition

- What is meant by privacy?
  - **Law's view of privacy**.
  - Privacy **From** (all sorts of agencies and individuals) …
  - Privacy **For** (all sorts of things) …
- Potential threats and protection against them:

  Universal unique identification.

  Paranoia and schizophrenia (are your friends).

  The threats of the new digital world.

  Self defense: the judo approach and beyond.

  Some references, both on-line and books.
- Privacy and security are mutually exclusive

A view of privacy and the Law

- The Internet is supra-national
- No single body of law governs the Internet
- Many governments feel threatened
  - U.A.E, Egypt, Libya revolts started through social networks
- Jurisdiction is an issue the Internet is international
- There is little (or no) law that you can depend on for proctecion
- Where you reside determines what laws can be wielded against you:
  - PATRIOT (US)
  - RIP (UK)

Privacy from “others”

- Friends, neighbors, family, and co-workers
- Marketers and retailers
- Credit agencies and other financial institutions
- Employers, actual and prospective
- Governmental agencies
- Snoops: professional, criminal and amateur
- All ‘round bad folks!

Privacy to guard

- Life history
- Medical records
- Financial records
- Legal records
- Education and employment records
- Activities, habits and personal tastes
- Purchase transaction histories
- THE public record

Identity uniqueness

- Everyone is unique, just like everyone else!
- Ultimate control is represented by instant,
  - automated identification of any individual
- Without unique identity, it is impossible to
  - definitively connect all the dots for any given
  - individual
- Safety and privacy lie in fragmentation
- Many powerful tools are emerging to link
  - fragmented sets of data together
    - Good analytics tools based on powerful search engine technology at its heart

Universal Identifiers

National I.D. Numbers

- Passports
- "Secure" boarding information
- Medical Record Identifiers
- Social Security (even if it isn't supposed to)
  - California and some states have implemented laws to drive out SSN as an identifier
- Insurance Numbers
- Tax and Voting Roll Identifiers
- Name, Address, and Telephone Numbers
- Driving Licenses
- "Agency" Identifiers, both official and not

Biometrics

- What is meant by biometrics?
- It means the measuring of some (ideally unique) physical characteristic/attribute of an individual:
  - Fingerprints, thumbprints, and footprints
  - Voiceprints
  - Iris (eye) scanning
  - Facial profiling
  - DNA profiling
  - RFID Implanting

- The goal is **unique** identification of individual;
  - Preferably in under 10 seconds on the wall clock
  - To a discrimination of better than 1 in 1e11 (100 billion);
  - Discrimination to 1e10 isn't going to be good for very long!

Chip implantation anyone?

- A tiny computer chip approved for implantation in a patient's arm can speed vital information about a patient's medical history to doctors and hospitals
- But critics warn that it could open new ways to imperil the confidentiality of medical records.
- The Food and Drug Administration said that Applied Digital Solutions of Delray Beach, Fla., could market the VeriChip, an implantable computer chip about the size of a grain of rice, for medical purposes
- With the pinch of a syringe, the microchip is inserted under the skin in a procedure that takes less than 20 minutes and leaves no stitches
- U.S. Army is considering the use of these chips

Paranoia and Schizophrenia

- Which one of my enemies told you I was paranoid?
  - Yes, *they* really are out to get you
  - Never ascribe to malice that which can adequately be explained by stupidity (or incompetence and ineptness)
  - The combination is spectacularly deadly
    - Lowe's unsecured WiFi network at a store in suburban Detroit
- Schizophrenia is your friend:
  - The more personae you can present, the less chance *they* have of connecting them all to you
  - The increased effectiveness of data analytics will make this more difficult over time

The Digital Threat

- **Data sets are immortal**
- Specific data sets may vanish below the threshold of visibility, but are seldom totally eliminated
- Only dependence on obsolete media prevents near instant recovery
    - Government seeking ways to recover obsolete data
- Important data is never deliberately lost, and seldom accidentally rendered unrecoverable
- Distributed processing proliferates copies

Moore's Law

- Computer hardware doubles in power and halves in price every two years

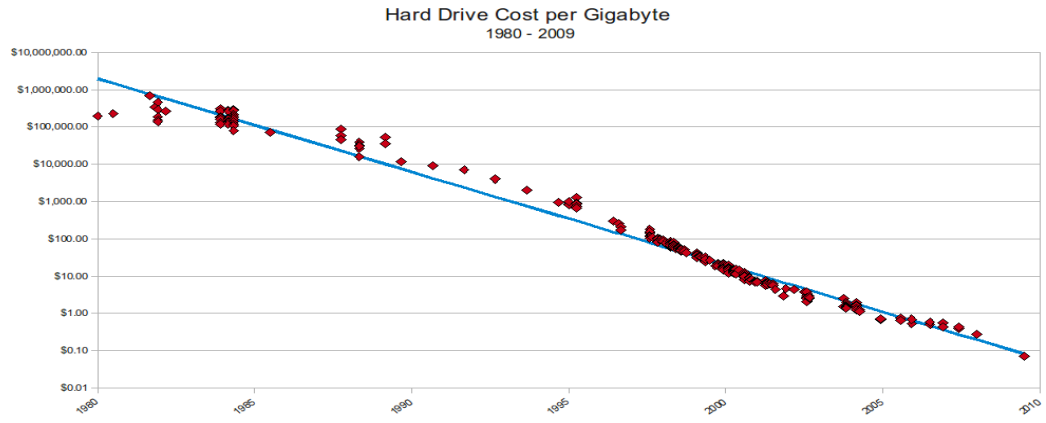
- Postulated in 1965 (for transistors on chips), by Gordon Moore, founder of Intel Corp

- We've remained ahead of the curve ever since:
  - Memory at $1M / megabyte in 1970 …
  - Disk at $1,000 / megabyte in 1970 …
  - 20 cps Teletype represented only universal data transmission infrastructure in 1970 ...
  - 256Gb flash drive

Data Density

20 megabytes represents:

- The entire bible (old and new testaments) as uncompressed text
- In 1970: one 1,600 bpi, 5,000 foot tape reel
- In 1970: two weeks of data transmission at 20 cps
- In 1975: 1/5th of a $100,000 IBM 3330-I disk — $1,000 / mb
- In 1980: 1/4 of a $10,000 80 megabyte SMD disk — $300 / mb
- In 1990: 6% of a $1,000 5 1/4 inch PC hard disk — ~ $10 / mb
- In 2000: 0.1% of a $400 20 gigabyte PC hard disk — ~ $0.50 / mb
- Today: 0.01% of a $200 240 gigabyte PC hard disk — <$0.50 / gb
- Today: of the order of 1 second of data transmission over a gigabit network



Division and Multiplication = Less (privacy)

- Replication of enormous data sets is a relatively easy task
- Systematic analysis of enormous data sets is routinely performed on desktop hardware
- Increasing trends among "*authorities*" to link databases, ideally via common unique IDs
  - *Data mining/warehousing* is the name of the game
- Web enablement everywhere: official, public, and private
  - Atom feeds and mashups common

Accidental/Intentional Exposure

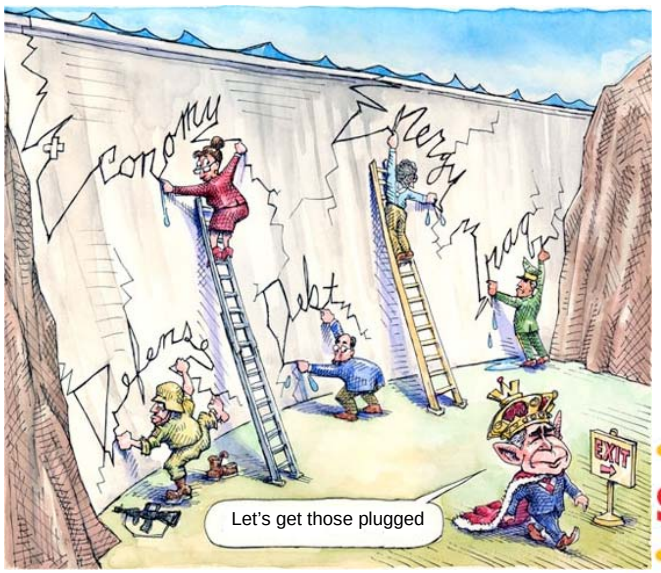
- Publishing data can have unexpected side-effects, and unforeseen consequences:
  - The Starr Report's deleted sections;
  - The British security report on Iraq's weapons threat

- Ease of access invariably exposes loopholes that enable unauthorized access
  - Patches issued weekly by Microsoft to 'fix' O/S and browser software

- Today's network infrastructures were designed around a trust model !

- None of today's popular publishing and storage technologies are intrinsically secure
  - Even less so, are the 'cloud' solutions

- WiKiLeaks
  - Disclosure of 250,000 US Embassy cables
  - Classified Guantanamo prisoner dossiers



Encryption Anyone?

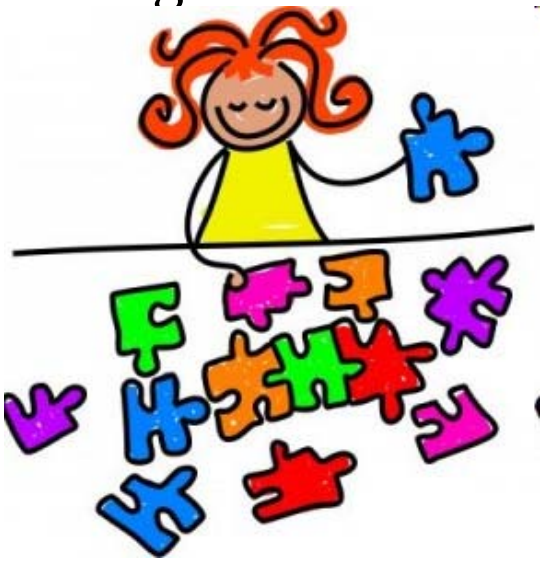
- Strong encryption is truly impenetrable:
  - The only viable attacks are via social engineering;
  - Alas, people are gullible, ignorant, and lazy.
- "*Authorities*" dislike not being able to know:
  - Key escrow in US (the Clipper chip);
  - RIP bill in the UK mandating key disclosure on demand
  - Anti-terrorist acts everywhere as excuse
- Weak encryption typically mandated or broken and continued use!
  - Resulting in cosmetic security
- Use of strong encryption often draws suspicion.
- When technology is strong, attack the people;
  - Social engineering plus direct and indirect surveillance
  - Key stroke trackers and password grabbers

The State of the Union

- Much replication of huge data sets
  - State/local use of federal databases
- Large proportion of stored data vulnerable to accidental exposure, especially when published on-line or transmitted over IP infrastructure
- Little legal recourse
  - Some countries have begun to enact privacy legislation
- "*Authorities*" are fundamentally opposed to strong protection that might delay or deny them access
- Everyone wants to construct (secret) profiles…
  - And stuff them chock full of details,
  - Which you can't see to validate, let alone veto, or even correct

The Judo Defense

- Employ leverage to use attacking agents' own momentum against them.
- Proportional response to scale of threat
- Learn to recognize when you can't win
- Avoidance is better than conflict



- Conflict leaves its own records, and they form their own patterns
- Avoiding creating patterns is the key

The Big Stick Wins

- You can never win against the three-letter agencies of the world
  - They have more resources (money, time, people)
- The trick is never to put yourself into their sights
  - The concept is the same as a stealth plane
- Creating and maintaining multiple public personae is a very costly partial defense
- It is extremely hard to avoid creating patterns of some kind, and patterns can be detected and analyzed
- Statistical methods and data analytics are astonishingly powerful in this regard

Fragmentation

- Record every individual release of a personal identifier, and the data associated with it
- Generate a viable variant on the identifier whenever possible, and track proliferation
    - Alter middle initial/name, etc.
    - Different SSN when demanded by say a physician
- Aggressively confront abusers and demand revocation or deletion from records
    - The law may help you, but this depends on the jurisdiction
    - Using the law creates patterns and draws attention
- Monitor all official records and insist on correction and amendment aggressively

Home Defense

- Hide behind a physical personal firewall with NAT translation for indirection
- Use of a proxy server is also good for adding layers to the defense
- Ideally add a second level of indirection
- Strongly encrypt everything all the time
  - Use secure access and control disciplines
  - Never allow software to “remember” a password, ever
- If paranoid, secure the physical environment
- Routinely scans for spyware (and malware)
- Ideally run a secure operating environment
- Absolutely do not run a Microsoft OS
  - PCs, Tablets and Smartphones
  - Turn off GPS services on Smartphones and tablets

Electronic Tracking

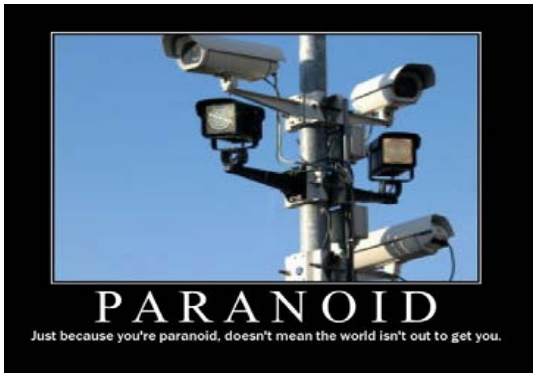
- GPS equipped cell phones/Smartphones;
  - Including those built into vehicles (e.g. GM's OnStar™)
  - Also tools like runners watches with built-in GPS
- Wireless emission trackers:
  - RFID is NOT our friend;
  - Bluetooth at ranges of up to a mile!
  - Voice over IP interception (the digital wire-tap on demand)
    - Note: Phil Zimmerman, creator of PGP, is now tackling this area.
- Surveillance:
  - Terrestrial (Closed Circuit video, card swipers, static sensors, credit card bluetooth);
  - Airborne - EMS imaging, UAVs;
  - Spaceborne - EMS imaging
    - Google Earth
- Desktop:
  - Web bugs, keyloggers and spyware

Anonymity and Free Speech

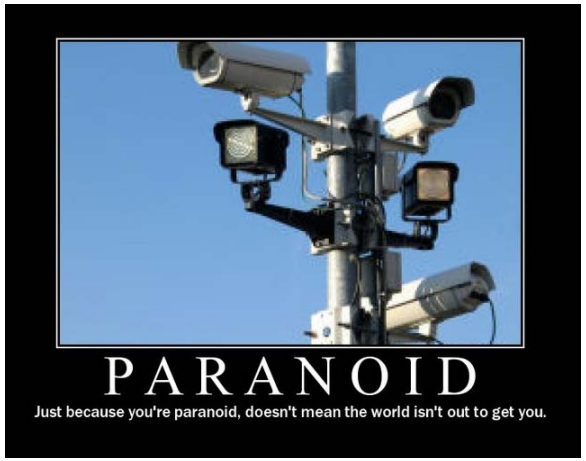
- Anonymity has been deliberately demonized:
  - Only those with something to hide …
  - True anonymity defeats control (which government HATES)
- Anti-terrorism and drug war have been seized as an excuse
- Maintaining anonymity *will* attract attention
- E-Mail: use an international version of PGP
- Usenet: use anonymous re-mailers
- WWW: use caching proxies and a non-standard browser such as Opera or OmniWeb
  - As a matter of course turn off cookies and cache

For the Seriously Paranoid

- Always use a lap-top, consider using public PCs like those at a library
- Always maintain critical data on an off-line storage device, and strongly encrypted
    - The “little” USB keychain memories (thumb disks) are great
    - You can also have an entire system on a 2 to 4 Gb USB thumb drive
- Always do your serious computing away from e-surveillance - a park bench, say
- Always connect to networks via public access points such as Internet cafés and hotel lobbies
    - War-chalking might be your friend
- Widely vary your use of such access points and do not use the same one with regularity



War Stories



- Google Groups:
  - regular changes of posting IDs render any matching of all my postings very difficult
- Evading urban surveillance:
  - http://www.appliedautonomy.com/isee/info2.html

  web-based application charting the locations of closed-circuit television (CCTV) surveillance cameras in urban environments
- Multiple different SSNs to use for medical care ID
  - Slight number variations, all unique, no two the same
  - California residents won't have this need

Final Thoughts

- Consider doing all your computing using an obscure natural language.
  - Did we all see the film “The Windtalkers”?
- Aggressive anonymity will draw attention:
  - Weigh the costs against the needs *very* carefully
- Aggressive defense of your records will draw both attention and active hostility:
  - Be prepared for legal battles and publicity
  - Demonization will be expected (The nail that sticks up will be hammered down)
- Martyrdom is currently on the cards:
  - Unheralded disappearance is also
  - Some steps already in place with laws already in effect

On-Line Reference Sites (1)

- The Electronic Privacy Information Center:
  - <**http://www.epic.org/**>
- People For Internet Responsibility:
  - <**http://www.pfir.org/**>
- Privacy International:
  - <**http://www.privacyinternational.org/**>
- The Privacy Forum:
  - <**http://www.vortex.com/privacy/**>
- The ACLU:
  - <**http://www.aclu.org/Privacy/PrivacyMain.cfm**>

On-Line Reference Sites (2)

- Bruce Schneier:
  - <**http://www.schneier.com/**>
- A list of advisories at the Privacy Foundation:
  - <**http://www.privacyfoundation.org/**>
- An excellent bibliography on anonymity:
  - <**http://www.freehaven.net/anonbib/**>
  - Well worth watching to see the current state of play.
- Privacy at the Open Directory Project (DMOZ):
  - <**http://dmoz.org/Society/Issues/Human_Rights_and_Liberties/Privacy/**>

Books for the Serious (1)

- The Digital Person: Technology And Privacy In The Information Age
  - Daniel J. Solove - New York University Press 2006
- How to Be Invisible
  - J.J. Luna - Thomas Dunne Books 2004

At **Amazon**, look at what other books customers of each of these books bought.

  - Daniel J. Solove, Marc Rotenberg - Aspen Publishers, Inc. 2003
- Beyond Fear: Thinking Sensibly about Security in an Uncertain World
  - Bruce Schneier - Copernicus Books 2003
- Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age
  - Steven Levy - Penguin Putnam 2002
- Database Nation: The Death of Privacy in the 21st Century
  - Simson Garfinkel, Deborah Russell - O'Reilly & Associates 2001

Books for the Serious (2)

- The End of Privacy: How Total Surveillance is Becoming a Reality
  - Reginald Whittaker - New Press 2000
- Privacy on the Line: The Politics of Wiretapping and Encryption
  - Whitfield Diffie and Susan Landau - MIT Press 1999
- Identity, Privacy, And Personal Freedom: Big Brother vs The New Resistance
  - Sheldon Charrett – Palidin Press 1999
- Technology and Privacy: The New Landscape
  - Philip E. Agre and Marc Rotenberg - MIT Press 1998
- Computer Privacy Handbook (currently cheap at Amazon)
  - Andre Bacard - Peachpit Press 1995