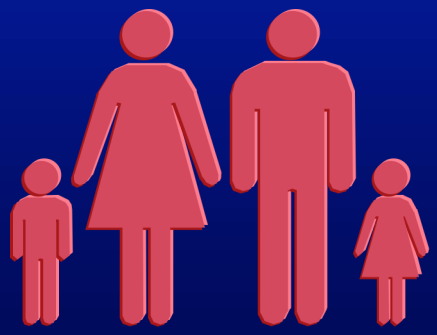
How Privacy Became a Top-Tier Socio-Political Issue -- and What's Next?

Alan F. Westin

Professor of Public Law & Government Emeritus, Columbia University and Principal, Privacy Consulting Group



at the Harvard Privacy Symposium, Cambridge, August 22, 2007

How Pervasive Privacy Has Become…

Hits from a Google Search -- August 13, 2007

Justice……. 207M		***Privacy…… 2.3B***	
Freedom…….. 203M		***Personal privacy….. 1.5B***	
Liberty…….. 88M		**Global privacy…..… 859M**	
Equality…… 49M		**Data security…….. 823M**	
Const. Rights…. 15M		**Data protection……. 314M**	
Civil liberties….. 4M			
		Consumer privacy.. 307M	
Free speech…. 122M		***Employee privacy… 89M***	
Democracy…….. 88M		***Citizen privacy…….. 58M***	

(Totals rounded)

Presentation Overview

- Between 1965-2004, privacy became a central value/issue/challenge of the deepening Information Age, first with computer and communication technologies, then the Internet
- Democracies developed current US/EU privacy frameworks, balancing privacy values with social interests in disclosure and protective surveillance
- But, since 2004, entering a new and transformative era of global information creation, communication, business and government applications, and surveillance
- Raises fundamental question: can we apply our existing privacy rules to this transforming environment or do we need to develop a new privacy system?

How the Privacy Issues Grew -- 1

- Over past 40 years, technological developments and their applications have revolutionized:
  - A. How organizations collect, combine, exchange, and use personal information about individuals
  - B. How individuals create and communicate personal information
  - C. How democratic societies use personal information to make decisions about consumer, employee, and citizen rights and opportunities
- Has produced the Information-Driven Society
- With "information privacy" a battleground for managing decision-making and power relationships between organizations and individuals

How the Privacy Issues Grew -- 2

- During First Computer Era (1965-1980) then the Second (1980-1993), information technology primarily an organizational resource and monopoly, with a few individual aids (e.g. PCs, cell phones, etc.)
- Internet 1.0 (1994-2004) empowered individuals -- to email, shop, chat, find information, etc. -- but still in an essentially organization-dominated Web
- The deepening global identity Theft plague raised the privacy and security ante
- And the terrorist attacks of 9/11 upset the pre-2001 balance between government surveillance and privacy/due process
- But, as of 2003-2004, there was a generally stable framework of privacy and data protection law and practice being applied to consumer, citizen, and employee information arenas

About 2004, the Information World Began to Change -- in Ten Dimensions

1. The all-pervasive Internet 2.0
2. “Identity crisis” and data breaches
3. Social networking and video posting
4. The Blogosphere
5. Behavioral target marketing
6. The mobile revolution
7. Anti-Terrorist surveillance
8. Monitoring and photographing public spaces
9. Electronic patient health records
10. In the U.S., a growing culture rejecting privacy constraints

1. The All-Pervasive Internet 2.0

- **Virtually all businesses now have Net operations**
- **Most personal information now flows online**
- **Employers use Net to communicate with employees**
- **Government agencies increasingly rely on Net**
- **Military management and combat ops are on Net**
- **65-85% of adult populations in advanced industrial nations go online and use Net; 93% of 12-17 year olds**
- **Mobile devices now connecting to the Net**

The Internet is now the central nervous system of a global society, the way masses now communicate and how everything is interconnected (VeriSign CSO)

2. “Identity Crisis” and Data Breaches

- Continued large-scale identity thefts from online personal information capture, organized in global rings, hard to identify and prosecute
- Also phishing, false web sites and other scams
- Widespread availability of individual’s personal information on Net and through data brokers
- Widespread data breaches at government, business, and educational organizations, from hard-copy losses and stolen laptops to thefts of data tapes and insider corruption -- “an insecure world”
- Plus larger ID challenges -- protecting children online; immigration control; access to data systems; protecting intellectual property; etc.

3. Social Networking

- **Explosion of self-revelatory postings by many individuals of personal profiles, photos, and videos -- worldwide. As of August 2007:**
  - MySpace: 100M open accounts; 43M active
  - Facebook: 39M active users
  - YouTube: 100M views a day
  - 55% of US teens post personal profiles; 61% go online daily
- **Supports creation of like-minded virtual communities -- local, regional, national and global -- very satisfying to people**
- **Privacy options for limiting access offered but often ignored by users**
- **Businesses now marketing on social networks (see panel 5)**
- **Employers, law enforcement, licensors scanning personal posts and using results to make business or government decisions**

4. The Blogosphere

- Blogging technology makes millions of persons into publishers, at small-scale level and also global, sometimes anonymous but often identified
- Political and news bloggers part of shift from print/broadcast media monopoly and professional experts to online "amateur" news and opinion
- Symbiotic relationship now between news/opinion blogs and traditional media presentations -- cable is now the blogger's echo chamber

- Privacy effect: adds to flows of personal info on Net; news and opinion blogs feed expose´ and voyeuristic cultural trends (See panel 10)

5. Behavioral Target Marketing

- **Shift in newspaper/magazine readership and TV watching to online and mobile fans trend for business marketers to seek personalized marketing, based on consumer transactions and profiles online**
- **Driving "behavioral targeting" -- linking online search behavior and activity trails to consumer preferences (e.g. Google plus Doubleclick) in order to post ads and offers**
- **Surveys show some consumers like this and others do not**
- **But not now a consensual process or covered by privacy laws, regulatory enforcement or private litigation**

6. The Mobile Revolution

- Cellphones and PDAs now widespread personal communication devices -- called the “third window” of information technology (TV and computer screens the others) -- 2B cell phones worldwide
- Mobile access to Net and transaction uses growing rapidly (already high in Japan, Scandinavia etc.)
- Marketers moving to offer services via mobile devices, based on user location or profile

- Mobiles provide personal location of users, through GPS technology, as well as message data, raising privacy issues for government access and target marketing

7. Anti-Terrorist Surveillance

- Wide range of government investigative and surveillance operations to meet terrorist threats, from telephone tapping and email monitoring to airport security procedures
- Need draws high public support, but how being done and what safeguards in place also draw high public concern -- tension with privacy/data protection norms
- Also, government calls for business cooperation (e.g. telcos, ISPs, air carriers, etc.) raise questions of scope and safeguards
- High government secrecy, while rational, fuels debates over threats to basic civil liberties

8. Monitoring/Photographing Public Spaces

- Explosion of closed-circuit cameras by police on streets and security locations and by private parties (stores, elevators, sports events, etc.); overall public approval but many privacy issues
- Use of camera phones by individuals producing new citizen photo capture of public events; also voyeuristic uses (have drawn legal controls)
- Google Earth and other mapping technologies producing photos of streets and movements
- Together, these developments threaten expectations (and prior realities) of anonymity in public places
- Now, when you go out, you may be "on camera"

9. Electronic Patient Health Records

- Medical/health records rated the most sensitive information by consumers
- Primarily local manual records until now, with limited computerization and networking
- National EHR program under way in US (and many other nations) since 2005 -- to automate and network health records, with government, vendors, medical leaders driving; also Net options for personal health records
- Privacy and data security issues recognized and being explored. But no legal framework beyond HIPAA in US

  and no empirical studies of how EHR programs handling patient consents, privacy rules

(My ppt in Track 1 Wednesday afternoon will examine…)

10. A Self-Revelatory and Expose´ Culture

- **Though public majorities always say want/need privacy, powerful current cultural trends reject privacy values**
  - **Many individuals are circulating intimate personal profiles/videos on social networking sites - exhibitionism**
  - **Reality TV and confessional television ventilate personal affairs -- a voyeuristic ethos**
  - **Avid media cover of "private lives" of celebrities -- a paparazzi age**
  - **"Public's right to know" generally trumps privacy of public figures today**
- **All these weaken the privacy constraints on investigation and publishing of private life, by media, political bloggers, employers, and for government social programs**
- **And Net 2.0 disseminates and amplifies the juicy details**

Summing Up…

- Between 2004 and present, combination of technology developments and applications, socio-cultural trends, and terrorism threats transforming information practices in democracies
- Many positive benefits, for consumers, employees, patients, citizens, with overall individual empowerment and providing needed response to terrorism challenges
- And no one can put these geniis back in the bottle
- But how should we approach creating sound privacy balances to meet current trends and risks?
  - Develop new privacy definitions and enforcement systems?
  - Apply and expand existing privacy systems and frameworks?

Is There a New Privacy Framework to Apply?

- Could we install an individual "ownership of personal information" framework?
- Could we require a "personal privacy responsibility" duty?
- Should U.S. create a federal Secretary of Privacy or a Federal Privacy Commission?
- Can the courts adopt a "thumb on the scale" approach in privacy cases?
- Could we develop a Global Privacy System rather than the national systems now in force?
- Are there major technology fixes for the Net 2.0 world?

My answers: no, no, no, no, no and no…

So How Do We Apply Existing Privacy Systems?

- Basic concepts of OECD Guidelines, Fair Information Practices, and EU Data Protection still provide sound foundation, though national implementation uneven
- The challenge is how to apply these concepts to the transforming developments described here
- No single silver bullet. Varying new information uses and flows will require mixture of:
  - -- new technology tools
  - -- market-driven policies
  - -- updated legal privacy definitions and rules
  - -- strong regulatory enforcement, and -- in the US:
  - -- incentives for private litigation
  - -- education in privacy values, to counter no-privacy cultural trends

Example: How Deal With Identity Crisis

- How US could deal with the Identity Crisis on and off Net:
  1. Comprehensive identity management programs for organizations
  2. Review and fix risky business marketing practices
  3. New identity protection tools (e.g. ID software, privacy-respecting biometrics, authentication models)
  4. Vigorous data security standards set by law and regulatory enforcement
  5. Data breach notification laws and liability standards
  6. Bring data brokers and public records under privacy rules
  7. Organize public demands for good data security, to spur competitive environment among businesses
  8. Stronger enforcement campaigns against ID thieves
  9. Consider adoption of a tailored national ID system

Contact Information

- My telephone: 201-836-9152
- My fax: 201-836-6813
- My email alanrp@aol.com
- Postal mail:

  1100 Trafalgar Street

  Teaneck, NJ 07666

And my thanks to my colleague, Vivian Van Gelder, for assistance in preparing this presentation