

Defining e-Topia:
*Emerging Internet Privacy Issues
and the Challenge Posed to
Protecting Genetic Information*

Dr. Bitá Amani,
Queen's University, Faculty of Law
Kingston, ON, CANADA

Privacy...

“Like the fabled elephant fondled by a dozen blind sages, is described uniquely by each beholder. Even legal scholars cannot agree what the word means.”

David Brin, The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom? (United States, Perseus, 1998) at 15.

Defining Privacy: Historical Challenges

- Definitional problems, bundle of rights depending on context for substance and protection, principle based on reasonable expectation of privacy, as property/commodity, legislated right, constitutional right etc
- CL as response to new media technology invading “private sphere” (photo, newspaper, mass media technology and publication)
- Freedom of Information v. protection of privacy
- Public v. Private realm (spatial and geographic)

Privacy Defined:

- Profs. Warren and Brandeis, “The Right To Privacy”(1890) 4 Harvard L. Rev. 193:

right of the individual to be let alone

A “person who reasonably and seriously interferes with another’s interest in not having his affairs known to others or his likeness exhibited to the public is liable to the other” Restatement of Torts → relational privacy extended to protect individuals from state intrusion by 1940s; essential for autonomy, liberty, and dignity against intrusion by emerging surveillance technology-focus still on expectations based on “private” space.

Defining Privacy: A Theoretical Framework

1960: Dean Prosser: review > 300 tort cases:

1. Intrusion: physical/other violation of one's solitude in an offensive manner
2. Public disclosure of private facts: publication of offensive private information not of legitimate public interest
3. False light in the public eye: reputation integrity against distortion
4. Appropriation: exploitation of attributes of the plaintiff's identity by the taking of their name, likeness, goodwill, or other identity data for unauthorized use.

Privacy as Human Dignity

- Single theory premised on spiritual interest; right is integral aspect of the pursuit of happiness and “preservation of human dignity and individuality” with “psychological, social and political dimensions...” Prof. Bloustein. A natural HR.
- Quasi-constitutional protection
- Nature of the right may rely on different values (liberty, autonomy etc.); protection from intrusion by whom? State? Individuals? Corporations? Insurers? Employers?

The Growing Use of Telecom

- Telecom transforms communication and information exchange, storage, access
- Electronic/digital surveillance
- 1/3 of Canadian households use internet; 54% for health information; > 20% to buy goods and services online
- Uses (shopping, communication, entertainment, banking) and search tools create data footprints and digital profiles → focused mostly on e-commerce regulation to secure transactions, minimize unsolicited ads (SPAM)

Privacy in Genetic Information

- Is Genetic Information “Personal”?
- Most personal type of biographical health information (genetic determinism)
- But also the most universal of data-shared with family, community, etc.
- Genetic information adds a layer to the formation of “data” identities and risk relates to the “DNA oracle”

Regulating Genetics as *Special* Health Information

- Rx as health information means it is private & personal information; duty of confidentiality attaches
- Shares predictive quality, can be used to discriminate and stigmatize BUT
- Provides more detailed risk information than other tests, more amenable to reductionisms in relation to self and family, raises more complicated challenges regarding the duty to inform 3rd parties (family) of health risks
- Higher volume, automated computational search/match
- Info can be extracted from sample over time, kept indefinitely and with unique consent/care/control issues.

Google's interest in your genes and your health records

- Mapping → Geneticization, public health genomics, genomics approach to medicine coupled with growing use of information and communication technologies in delivery of health care services (telehealth/telemedicine, WHO)
- 23andMe- “Google’s Genetic Start-UP”- “help you make sense of your genetic information”, Sept. 2007
- “Dr. Google” Plus: EHR help you track your health, universally, remotely, digitally accessible- pilot testing EHR w/ 10K volunteer patients at the Cleveland Clinic
- Efficiency arguments in helping pts map health history meets ethical challenges: privacy, access, language

Other Developments

- Microsoft also launched similar EHR product (Health Vault) in 2007
- Canada Health Infoway, national body pushing for public EHR but delivery date set at 2015.
- In Canada, 2000 health transactions every minute and 322 million office based visits/yr, 94% on paper- lots of \$ to be saved in a public health system by going electronic

Identity Profiles and Data-Self Determination

- Informational interconnectivity create a data “self”; EHR promote in some way patient self-management: can see record, correct it, discuss it, access it etc but who is right about content of medical records? Dr v. pts control
- New DNA businesses focus on self “empowerment”: DNAPrint, DNA Heritage and GeneTree, companies provide ancestral research using individual DNA w/direct to consumer marketing (\$100/test)
- Increase genetic divide, promote determinism “buy in”
- Genographic Projects, subsidizes National Geographic Society & IBM Corps program to build an ancestral DNA database analyzing 100,000 blood samples from indig.

The *Synergistic Threat* To Privacy

- Proliferation of genetic mapping technology and telecommunications portend a genomics approach to medicine with increased risk of exposing the data self to privacy intrusions and dangerous diagnostics.
- Speed/ease personal info collected, organized, aggregated, and analyzed make privacy paramount for public debate- data mining & matching, electronic/camera surveillance, debit/credit card trails, cell phone locator technology, gait/face/voice recognition software, employer/state email surveillance, ID theft

The “Synergistic Threat”

“In that the threat of the profile is greater than the sum of the privacy threats associated with each individual bit of information considered in isolation”

- Genetic reductionism based on aggregated data of propensity linked with behavioural patterns
- Unauthorized uses of “identity” data and unsolicited marketing/advertising

Special Privacy Challenges

- Rules on 3rd party access N.B: Individual maps compared to golden standard and used to deny employment, insurance, or other benefits
- Outsourcing and privacy intrusions
- Security v. privacy; public interest and private rights; Data banks v. DNA banks
- Foreign jurisdiction and control- US Patriot Act

Canadian Regulatory Responses: IN TELECOM

- FCC- where service is primarily data processing, shouldn't be regulated but if communication, should- impossible distinction led to new telecom regulation
- *Telecommunications Act*- distinguishes content v. carriage, carrier not control content unless provided for by the Canadian Radio-TV and Telecom Commission
- S. 7(h) and (i) policy objective to “respond to the economic and social requirements of users of telecom services; and to contribute to the protection of privacy of persons- but focus more on access to telecom than privacy protection in the collection or use of information.

With Privacy Legislation

- Federal *Privacy Act*
- *Ontario Freedom of Information and Protection of Privacy Act (FIPPA)*
- *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*
- *FIPPA and MFIPPA* protect recorded personal information (list of examples) and strive to balance the public's right to know with an individual's right to privacy but may not be effective with net privacy or re: private sector
- 2004, *Ontario Personal Health Information Act (PHIPA)* specifically ensures personal health information of patients is kept private, confidential and secure.

Privacy Legislation for e-challenges

- New legislation governing privacy and e-commerce of only federally regulated businesses (banks, airlines, telecom providers) in first three years will now likely apply to ISPs- provision forcing them to store data would threaten users' privacy and would create a pool of data that could be put to unauthorized uses.

Legislation Cont...

- Federal *Personal Information Protection and Electronic Documents Act (PIPEDA)*- private sector undertakings adopts model code for the Protection of Personal Information based on OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980)- affects personal data in both private and public sectors- took 3 yrs to come into force within each province after which are incorporated by reference.

Privacy & PIPEDA

- 4 areas of governance w/ PIPEDA:
- Collection of Data; 2. use of data/internal access; 3. disclosure (external access); 4. retention (duration of data storage and disposal)
- applies to every “organization” re personal info it CUDs *in the course of commercial activities (extending to employment) S.2 definition: “includes an association, a partnership, a person and a trade union” and exception for limited circs regarding use, collection, or disclosure without knowledge or consent of subject.*
- CIO and privacy policy required.

PIPEDA'S Limitations

- Excludes: government institutions to which Privacy Act applies; personal information CUD for non-commercial purposes (“personal or domestic purpose...or any other purpose”); or the CUD is for journalistic, artistic, or literary purposes → focus on commercial use of data NOT privacy protection per se.
- Only protects *private* personal information. Personal info publicly available, like address, phone number, employer, salary would not be captured
- Is there expectation of privacy over unsecured networks? Wireless? Email? Is info transmitted “public”?
- Unless are entitled to privacy, consent irrelevant

Office of the Information and Privacy Commissioner

- Canadian Privacy Commissioner: Privacy as the defining issue of the next decade
- Uncovered vast DB created by HR Development Canada w/> 2000 pieces of personal information on more than 33 million Canadians: privacy issues on collection and uses of this information.
- Role of Commissioner to educate, investigate complaints, ensure compliance with laws
- National and provincial

Other considerations

- “Monopolies of knowledge”- differential access: Canada beats US, Italy, Japan, Germany, UK, and France on number of personal computers:inhabitants ratio
- Internet culture depends on infrastructure, local phone rates (monopolies or competition), acceptability and use of credit cards, language of the net and data banks.
- Debate about government v. technological control of net; public v. private control:
- Property/licencing models for protecting privacy

Recommendations for further Law and Policy Development in Canada

- Develop specific legislation for regulation of genetic information in real and cyberspace
- Expand definition of personal and/or private information under existing law to include genetic information and overcome apparent gaps
- Create some regulatory oversight for internet governance in relation to non-commercial activities and ensure proper notice, consent, enforcement mechanisms available
- “Smart Cards”, to exclude genetics if adopted

Lessons for Iran

- Policy: scope of protection; regulatory instruments
- Clear legal articulations of protections, definitions to include genetics as health information and as “personal data” similar to the EDD with broad inclusive definition
- Public education programs- hospitals etc.
- Information dissemination booklets on rights and duties
- Regulatory oversight- ombudsman/Commissioner for investigations and complaints
- Fair information practices, FTC: notice, choice, access, security, and enforcement allowing “self” to ensure data security and integrity.

Lessons for Iran (cont...)

- Information management systems: at individual, organizational, and even societal level to avoid net inefficiency, ensure fair/equitable access balanced against protection of privacy
- Recognition of special nature of genetic information, “from cradle to grave” → unique ELSI
- parties have “incentives to learn about the DNA of others, while regulatory regimes will lag technological advances” Hsien Lei

To Conclude: The Utopia of E-Topia

“Privacy is a human right with a grand tradition, both nationally and internationally...[P]rivacy in today’s high – tech world has taken on a multitude of dimensions...It is the right to enjoy private space, to conduct private communications , to be free from surveillance and to respect the sanctity of one’s body;...the right to control one’s personal information...Privacy is a core human value that goes to the very heart of preserving dignity and autonomy. It is a precious resource because once lost, whether intentionally or inadvertently, it can never be recaptured.”

Report of the House of Commons Standing Committee on Human rights and the Status of Persons with Disabilities, 1997