DISCLOSURE AND PRIVACY ISSUES IN A DIGITAL AGE

Randall G. Rueth
Marshall, Gerstein & Borun LLP
233 South Wacker Drive
6300 Willis Tower
Chicago, IL 60606-6357
Direct: (312) 474-6602
Firm: (312) 474-6300
Facsimile: (312) 474-0448
RRueth@marshallip.com
www.marshallip.com

J. Michael Slocum
Slocum & Boddie, P.C.
Suite 300
5400 Shawnee Road
Alexandria, VA 22312
Telephone: 703-451-9001
Facsimile: 703-451-8557
jmichaelslocum@slocumboddie.com
www.slocumboddie.com

DIFFERENT APPROACHES TO PROTECTION OF PRIVACY

- The United States and its respect for the discipline of the "marketplace"
- Privacy regulation in Europe
- Canada's approach to privacy
- Privacy law in Asia

U.S. LEGISLATIVE MEASURES AFFECTING PRIVACY

- The Privacy Act of 1974
- The Electronic Communications Privacy Act of 1986 (ECPA)
- The Privacy Protection Act of 1980
- The Family Educational Rights and Privacy Act (FERPA)
- The Driver's Privacy Protection Act
- The Right to Financial Privacy Act
- Legislation protecting privacy in the private sector
- The Fair Credit Reporting Act (FCRA)
- The Financial Modernization Act
- The Identify Theft and Assumption Deterrence Act
- The Cable Communications Policy Act
- The Videotape Privacy Protection Act
- The Telephone Consumer Protection Act
- The Telecommunications Act of 1996
- The Health Insurance Portability and
- Accountability Act of 1996 (HIPAA)
- The Children's On-line Privacy Protection Act of 1998 (COPPA)
- U.S. Constitutional concerns and privacy
- The PATRIOT Act

EUROPEAN PRIVACY

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)
  http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
- European Union Directive on Data Protection (1995/1998)
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML
- CSA Model Code for Protection of Personal Information (1996)
  http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code/article/principles-in-summary
- United States Safe Harbor Agreement (2000) and EU reaction
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML
- Global Privacy Standard (2006)
  www.ipc.on.ca/images/Resources/up-gps.pdf
- IPC's Privacy By Design Principles
  http://privacybydesign.ca/about/principles

DATA PROTECTION IN THE WORLD TODAY

- Europe: EU member states (and most other states) have implemented data protection acts based on the Directive
  - (In certain European states, based on the right of informational self-determination; level of protection varies considerably)
- U.S.: patchwork regulation, industry self-regulation schemes (U.S. privacy regulation system is not "adequate" according to EU standards)
  - Safe Harbour Agreement, PNR data
- EU-style data protection regimes appear in Asia, Canada and South America

CSA PRIVACY CODE PRINCIPLES

1. Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. Consent

The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.

(continued)

CSA PRIVACY CODE PRINCIPLES (2)

4. Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure and Retention

Personal information shall not be used or disclosed for purposes other than those for which it is collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of the stated purposes.

6. Accuracy

Personal information shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is used.

7. Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

(continued)

CSA PRIVACY CODE PRINCIPLES (3)

8. Openness

An organization shall make specific information about its policies and practices relating to the management of personal information readily available to individuals.

9. Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information, and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

http://www.csa.ca/standards/privacy/code/Default.asp?articleID=5286&language=english

APEC INFORMATION PRIVACY PRINCIPLES

- Preventing harm
- Notice
- Collection limitations
- Uses of personal information
- Choice
- Integrity of personal information
- Security safeguards
- Access and correction
- Accountability

APEC CROSS-BORDER PRIVACY ENFORCEMENT ARRANGEMENT (CPEA)

- Facilitate information sharing among Privacy Enforcement Authorities (PE Authorities) that enforce Privacy Laws)
- Provide mechanisms to promote effective cross-border cooperation between authorities in the enforcement of Privacy Law
- Encourage information sharing and cooperation on privacy investigation and enforcement with PE Authorities outside APEC

PRIVACY AND PUBLIC RECORDS

- The Privacy Act of 1974
  - Mandates how U.S. government agencies shall collect, maintain, use and disseminate personally identifiable information (PII) about individuals that is maintained in systems of records

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

- Privacy Rule
  - Establishes national standards to protect individuals' medical records and other PHI
- HIPAA Security Rule
  - Establishes national standards to protect individuals' electronic personal health information (ePHI) that is created, received, used or maintained by a covered entity

FREEDOM OF INFORMATION ACT (FOIA)

- Inform the public of information while appropriately protecting government interests
- Applicability: Executive branch government agencies
- Provides individuals with access to many types of records that are exempt from access under the Privacy Act
- Unlike those of the Privacy Act, FOIA procedures are available to non-resident foreign nationals

E-GOVERNMENT ACT OF 2002 PUBLIC LAW 107-347

- Improve internet-based technology to make it easier for citizens and businesses to interact with the government
- Applicability: All executive branch departments and Federal agencies
- Protects personal information that agencies collect, use, maintain or disseminate within information technology systems

E-GOVERNMENT ACT - FISMA

- Information Security Management Act (FISMA) provides a framework to ensure effectiveness of information security controls for Federal systems

PAPERWORK REDUCTION ACT PUBLIC LAW 104-13

- Reduce the total amount of paperwork handled by the Federal government and general public
- Maximize utility of information
- Agencies must ensure disclosure policies will honor any claims of confidentiality on forms

RECORDS MANAGEMENT
36 CFR CHAPTER 12

- Supports the creation, maintenance and use, and disposition of records in order to document Federal policies, operations, and transactions appropriately and economically
- What it protects: All information, related to an agency's business transaction, that is created, used, maintained, disseminated, or disposed of.

EUROPEAN AND OTHER LAWS

- Countries around the world have some form of freedom of information laws
- Other countries are working towards introducing such laws
  - See: http://www.unesco.org/new/en/communication-and-information/freedom-of-expression/freedom-of-information/
- In the East Asia Pacific (EAP) region progress in adopting and implementing FOI legislation has been limited (compared to other regions such as Latin America and South Asia)

GEOGRAPHIC AND OTHER PERSONAL INFORMATION

- "… a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them is communicated to others"
  - Duckham, M. and L. Kulik, *Location Privacy and Location-aware Computing*, in *Dynamic & Mobile GIS: Investigating Change in Space and Time*, J. Drummond, et al., Editors. 2006, CRC Press: Boca Raton, FL USA. p. 34-51

GEOGRAPHIC INFORMATION ISSUES

- Privacy
- Data ownership
- Use by
- Government (zoning, land use, etc.)
- Medical intervention (disease tracking, etc.)
- Law enforcement
- Work and education (worker and student tracking, etc.)

FUTURE ISSUES

- Privacy will become a critical issue for GIS as use expands to legal applications
- Data ownership will remain critical to GIS, with a delicate balance between public and private GIS data
- Legal areas particularly important for GIS:
  - Liability
  - Intellectual Property Rights
  - Information access laws
  - Privacy

PERSONAL E-HEALTH RECORDS

- Europe
  - SUSTAINS (Sweden)
  - NHS Direct
  - NHS Health Space
- USA
  - Large Group Practices
  - U.S. Veterans Administration
  - DOD
  - Insurers/payers and corporations for employees

ISSUES WITH PERSONAL HEALTH RECORDS

- Security & privacy
- Operations
  - Passwords & support
  - Service level expectations
- Patient entered data
- Liability

WHAT IS E-HEALTH?

- Internet-enabled Healthcare Applications
  - Consumer health information
  - Personal health records
  - Internet-based services (e-Pharmacy, e-Care (including email and e-communication, etc.)
- Electronic Health Record (EHR) Systems
- Administrative and Financial Health Systems

IMPORTANCE OF HEALTHCARE SECURITY

- Confidentiality/data security
- What if something goes wrong?
  - System failure (crash or virus causes loss of data)
  - Outside force damage (hacker, other)
  - Disaster
- Design issues (signature, authentication, others)
- Compliance issues

E-HEALTH SECURITY ISSUES

- Security for (patient) confidentiality
- Security that enables electronic health records
  - Authentication
  - Data integrity
- Systems security
  - Secure transmission
  - Secure processing
  - Secure storage
  - Etc.

ELECTRONIC MEDICAL RECORD SYSTEMS

- Personal data protection
- Health information standards frameworks
- Conflicting requirements
- Privacy and security
- Systems developed ahead of regulatory frameworks
- Open source and open standards

CLOUD COMPUTING

- Cloud Computing changing the whole IT, service industry and global economy. Clearly, cloud computing demands ubiquity, efficiency, security, and trustworthiness.
- Cloud computing has become a common practice in business, government, education, and entertainment leveraging 50 million of servers globally installed at thousands of datacenters today.

(continued)

CLOUD COMPUTING (2)

- Private clouds will become widespread in addition to using a few public clouds, that are under heavy competition among Google, MS, Amazon, Intel, EMC, IBM, SGI, VMWare, Saleforce.com, etc.
- Effective trust management, guaranteed security, user privacy, data integrity, mobility support, and copyright protection are crucial to the universal acceptance of cloud as a ubiquitous service.

PRIVACY AND CLOUD COMPUTING

- Individual user control
- Anonymity for individual users
- Use of Cloud to "export' data
- Identity information and authentication
- Ability of Cloud operators (and state through them) to break anonymity
- Encryption of data pros and cons

(continued)

PRIVACY AND CLOUD COMPUTING (2)

- Compartmentalizing data processing and storage
- Coordinating privacy and security requirements between cloud service providers
- EULA's and notice about privacy
- Privacy enhancing and privacy destroying technologies
- Privacy enforcement and compliance across jurisdictions

EXPORTING DATA ACROSS BORDERS

- An actual shipment or transmission of items (commodity, technical data, or software) across national borders
- Releasing (including oral or visual disclosure) "technical data" or software "source code" to a "foreign person," even inside a single country ("deemed export")

(continued)

EXPORTING DATA ACROSS BORDERS (2)

- Performing technical assistance, training or other "defense services" for, or on behalf of, a "foreign person," (including foreign corporations) whether in a single country ("deemed export") or across borders
- Re-exporting from foreign countries country - of -origin goods or technical data, goods incorporating components or goods manufactured from country-of-origin technology or re-exporting "technical data" or software

NON-U.S. LAWS

- Export control rules for encryption technologies fall under the Wassenaar Arrangement
- The Wassenaar Arrangement was established to contribute to regional and international security and stability
  - It promotes transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations
- Many nations have more restrictive policies than those agreed upon as part of the Wassenaar Arrangement

EU 58:PRIVACY, SECURITY AND DATA

- European Directive 2002/58/EC introduced new rules on the subject addressing:
  - General security
  - Confidentialiy
  - Cookies
  - Traffic data
  - Location data
  - Directories
  - Unsolicited mail
  - Data retention

INTERNATIONAL ISSUES

- What privacy provision law will apply to terrestrial/satellite networks?
- Or to a ship in international waters providing services?
- EU has directives but no coherent model of sanctions and law enforcement is different in each country

CRIMINAL LAWS RELATED TO ABUSE OF DATA AND PRIVACY

- Convention on Cybercrime
  - The product of four years of work by the Council of Europe, United States, Canada, Japan and other countries
  - The convention is similar to a draft treaty

(continued)

CRIMINAL LAWS RELATED TO ABUSE OF DATA AND PRIVACY (2)

- Convention on Cybercrime (continued)
  - Pursues a common criminal policy aimed at protecting the society against cybercrime by adopting legislation and promoting international cooperation
  - The convention deals with infringements of copyright, computer-related fraud, child pornography and violations of network security

UNITED STATES LAWS

- The Patriot Act REDUCED the individual privacy in U.S.
  - It extends the tap and trace provisions of wiretap statutes to the Internet
  - It mandates technological modifications at ISPs to facilitate electronic wiretaps on the Internet
  - It permits the Justice Department to roll out of the Carnivore program – an eavesdropping program for the Internet
  - It permits Federal law enforcement personnel to investigate computer trespass and enacts civil penalties for trespassers

CONCLUSION

- Questions?

Looking for a PowerPoint presentation? The majority of concurrent session materials will be available at www.sra2012.org/presentations. Use your smartphone and link to the site by this QR code!