Getting Your Arms Around the Landscape of Data Privacy Law

Steven Emmert, Senior Director, Government Affairs

June 3, 2016

What is privacy?

“the right to be let alone” - Samuel Warren & Louis Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890)

“the state of being apart from other people or concealed from their view” - Dictionary.com

“the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively” - Wikipedia

What is data privacy?

“the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them” – Wikipedia

“the aspect of information technology that deals with the ability an organization or individual has to determine what data in a computer system can be shared with third parties” – Whatis.com

What is “personally identifiable information” or PII?

Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

What is “sensitive personal information” or SPI?

Information that if lost, compromised, or disclosed could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Do I own data about me?

You Don’t Own Your Data - “you may have privacy laws protecting you from being spied on and copyright laws protecting ownership of content you create, but data doesn't belong to you just because it's about you.” http://lifehacker.com/you-dont-own-your-data-1556088120

Fair Information Practice Principles

Notice – organizations should provide notice of their privacy/data collection policies, including the purpose for which data is collected, used, retained, and disclosed.

Choice/Consent – organizations should provide individuals with choice regarding data collection where appropriate, which can be implicit or explicit.

- Opt-out – data is collected unless the individual says “no”
- Opt-in – data is not collected unless the individual says “yes”

Access – organizations should provide access when possible to the individuals who are the subject of the data collected.

Accuracy – organizations should maintain data that is accurate and complete relative to the purposes for which the data is collected.

Security – organizations should employ reasonable administrative, technical and physical security to protect data from unauthorized access, use, disclosure, modification or destruction.

U.S. privacy protection framework:

As contrasted with the E.U. and some other countries, U.S. law does not contain a single uniform standard or baseline of privacy protection. Rather, U.S. law is more nuanced, segmented by industry and governmental sectors and data types. US laws are also subject to rigorous enforcement, both through private actions and by federal, state and local governments and agencies.

Sources of Law (or consumer protection):

- Common law (Tort)
- U.S. Constitution
- U.S. Code
- Code of Federal Regulations
- Treaties/trade agreements (U.S./E.U. Safe Harbour and Privacy Shield agreements)
- State Constitutions
- State Codes
- State Administrative Codes
- Industry self-regulatory principles (DMA Privacy Promise, BBBOnline, Data Transparency Coalition, Digital Advertising Alliance, etc.)
- Voluntary privacy policies/statements (website privacy policy statement, GLBA notice, etc.)

Prosser and the Restatement of Torts - 1960

1. **Intrusion upon seclusion**:

   "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS § 652B

   Would include "stalking"

2. **Public disclosure of private facts**:

   "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." RESTATEMENT (SECOND) OF TORTS § 652D

   This has been narrowly interpreted by the Court, particularly in recent years. The clear conflict with the protections afforded speakers under the First Amendment makes it difficult to restrict speech of lawfully obtained factual information. E.G. Publication in the newspaper of the name of a juvenile offender or of a rape victim.

Prosser and the Restatement of Torts, cont'd.

3. **False light of "publicity"**

   "One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed." RESTATEMENT (SECOND) OF TORTS § 652E

   Libel. Slander. Defamation.

4. **Appropriation**

   "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy." RESTATEMENT (SECOND) OF TORTS § 652C

   "Misappropriation"

   "New" Right of publicity

The U.S. Constitution

U.S. Constitution (signed September 17, 1787, ratified June 21, 1788)

The word “privacy” does not appear in the U.S. Constitution.

The U.S. Supreme Court has “found” limited protection for some privacy interests in the U.S. Constitution.

- First Amendment (ratified December 15, 1791)
  - Freedom of speech (including anonymously)
  - Freedom of association
- Third Amendment
  - Sanctity of the home
- Fourth Amendment
  - Protection against unreasonable searches and seizures
- Fifth Amendment
  - Privilege against self-incrimination
  - Due process protections

U.S. Code

Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681 et seq. – Regulates the use of personal information by consumer reporting agencies used to determine a consumers' eligibility for credit, insurance, employment, government licenses or government benefits.

Bank Secrecy Act of 1970, amended various sections of titles 12 and 15 U.S.C. – Requires banks to maintain records of consumer financial transactions; allows use in criminal investigations.

Privacy Act of 1974, 5 U.S.C. § 552a - Provides individuals with certain rights regarding personal information collected by federal records systems, including a right of access and a right to correct.

Family Educational Rights and Privacy Act of 1974, 20 U.S.C. §§ 1221, 1232g – Protects the privacy of school records.

Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 – Protects consumer financial records; imposes requirements for subpoenas and warrants for access.

Foreign Intelligence Surveillance Act of 1978, 15 U.S.C. §§ 1801-1811 – Regulates foreign intelligence collection activity.

U.S. Code, cont'd.

Privacy Protection Act of 1980, 42 U.S.C. § 2000aa et seq. - Protects journalists from being required to turn over to law enforcement any work product and documentary materials, including sources, before it is disseminated to the public.

Cable Communications Policy Act of 1984, 47 U.S.C. § 551 – Creates privacy protections for records maintained by cable companies.

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522 - Updated the Federal Wiretap Act of 1968, which addressed interception of conversations using "hard" telephone lines, to apply to the interception of computer and other digital and electronic communications, including the addition of limited privacy protections.

Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a - Provides procedural requirements for federal agencies when engaging in computer-matching activities; provide matching subjects with opportunities to receive notice and a right to refute adverse information; require agencies engaged in matching activities establish Data Protection Boards.

Employee Polygraph Protection Act of 1988, 29 U.S.C. §§ 2001-2009 – Governs use of polygraphs by employers

U.S. Code, cont'd.

Video Privacy Protection Act of 1988, 18 U.S.C. § 2710-2711 – Protects the privacy of videotape rental information.

Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 – Provides consumers with protections from repeated telemarketing calls.

Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 et. seq. – Restricts access to and use of records maintained by state departments of motor vehicles.

Health Insurance Portability and Accountability Act of 1996, 110 Stat. 1936 – Gives Health and Human Services authority to promulgate regulations governing the privacy of medical records.

Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 – Restricts the collection of personal information by websites from children under the age of 13.

Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. §§ 6801-6809 - Requires companies to give consumers privacy notices that explain the institutions' information-sharing practices. Consumers have the right to limit some sharing of personal information.

U.S. Code, even more…

USA Patriot Act of 2001, 115 Stat. 272 (2001) - Congress modified existing legal principles that were previously available to fight organized crime and retrofitted them to apply to efforts to fight global terrorism.

CAN-SPAM Act of 2003, 15 U.S.C. §§103, et. seq. - Established the United States' first national standards for the sending of commercial e-mail and requires the Federal Trade Commission (FTC) to enforce its provisions.

Others not listed here, including…

- **Freedom of Information Act of 1966**
- **REAL ID Act of 2005**
- **Junk FAX Protection Act of 2005**
- **Genetic Information Nondiscrimination Act of 2008**

Federal Trade Commission

Federal Trade Commission Act of 1914, 15 U.S.C. §§ 41-58 - The Commission is empowered, among other things, to (a) prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce; (b) seek monetary redress and other relief for conduct injurious to consumers; (c) prescribe trade regulation rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices; (d) conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and (e) make reports and legislative recommendations to Congress.

15 U.S. Code § 45 (Section 5 of the FTC Act) - Unfair methods of competition unlawful; prevention by Commission

(a) Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign trade

- Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.

Other sources of applicable law:

Code of Federal Regulations – contain implementing regulations for many of the identified federal statutes:

- Do Not Call

State laws

- Constitutional right to privacy in: AK, AZ, CA, FL, HI, IL, LA, MT, SC, WA
- Mini FCRA
- DPPA state laws
- GLBA state laws
- Student privacy laws
- Data breach laws
- Sunshine laws
- Freedom of Information Act laws
- Many others

Relevant International Laws and Agreements

OECD Privacy Guidelines - 1980

APEC Privacy Principles

EU Data Protection Directive – repealed (?) effective May 2018

US/EU Safe Harbour Agreement (voided October 2015)

US/EU Privacy Shield Agreement (effective July 2016???)

EU General Data Protection Regulation – effective May 2018

What's happening TODAY?

EU General Data Protection Regulation – effective May, 2018

- Many new laws will be adopted over the next 2 years to facilitate implementation

US/EU Privacy Shield Agreement – European Commission approval pending

- EU Parliament – Does not go far enough…
- Article 29 Working Party – Would be better if…
- EU Data Protection Supervisor Giovanni Buttarelli – not robust enough to withstand future legal scrutiny before the Courts and calls for significant improvements.
- The large majority of EU Member States in the Article 31 Committee support PS.
- None of this is binding on the European Commission, which has the final say.
- Expect a final decision before the end of June.

Data Localization Issues:

- Russia – Must maintain the database within Russia
- EU – adequacy of privacy protections?
- Brazil - considering

TODAY con't.

FCC Notice of Proposed Rulemaking on Protecting the Privacy of Customers of Broadband and Other Telecommunications Services – Written comments to the FCC due TODAY! June 3, 2016.

- Draft reads as if written by the consumer protection community – as a consequence there is concern among members of the business community about the lack of balance.
- May exceed FCC authority – Section 222 authority was written for telephony services
- Would expand the definition of PII to include data that is not individually identifiable such as application usage data, device identifiers, and Internet browsing history.
- Consent standard is very restrictive – most use limited to opt-in.
- No "record" of consumer harm to support promulgation of these rules.
- Concern that this standard will be extended to "edge" providers that do not clearly fall under the supervision of the FCC.

NTIS Final Rule on Access and Redistribution of the Social Security Administration Death Master Index

- Requires statutorily enumerated use
- Requires significant data security safeguards
- Requires audit by an "accredited conformity assessment body" every 3 years.

Today… con't.

NTIA Multistakeholder Privacy Best Practice Recommendations For Commercial Facial Recognition Use

- New discussion draft.
- Based on FIPP's
- Intended to provide a flexible and evolving approach to the use of facial recognition technology, designed to keep pace with the dynamic marketplace surrounding these technologies.
- Expect these to be finalized soon.

NTIA Multistakeholder on Unmanned Aircraft Systems (UAS or drones)

- Concluded May 18, 2016
- Produced a consensus set of best practices
- Focus is on data collected via a UAS, including both commercial and non-commercial UAS
- Strong first amendment exception for news media companies

In the courts – Is Harm a Necessary Element?:

Spokeo, Inc. v. Robins, 2016 U.S. LEXIS 3046 – A plaintiff asserting a statutory claim must make a showing of particularized and concrete harm sufficient to establish Article III standing, even if the underlying statute provides for statutory damages without a separate showing of injury.

In the matter of LabMD Inc., FTC Docket No. 9357 – FTC ALJ dismissed the complaint holding that consumer harm that is merely possible due to data security weaknesses, without any evidence to support that such harm is in fact likely, is insufficient to prove unfairness under Section 5 of the FTC Act. FTC staff has appealed to the full FTC.

FTC v. Wyndham Worldwide Corp., 2015 U.S. App. LEXIS 14839 - Federal Trade Commission had authority to regulate cybersecurity under the unfairness prong of 15 U.S.C.S. § 45(a) and the company had fair notice its specific cybersecurity practices could fall short of that provision. This case included a showing of actual consumer harm in the form of an actual data breach and resulting direct losses.

Questions?

Steven M. Emmert, Esq.
Senior Director, Government & Industry Affairs

RELX Inc.
1150 18th Street NW, Suite 600
Washington, DC 20036
steven.emmert@relx.com
202-262-5944