WHAT IS PRIVACY?

Context Matters
WHAT IS PRIVACY?

• Definition of PRIVACY from Merriam Webster Dictionary
  o plural privacies
  – 1a: the quality or state of being apart from company or observation: SECLUSION
  – b: freedom from unauthorized intrusion one's right to privacy
  – 2archaic: a place of seclusion

• https://www.merriam-webster.com/dictionary/privacy
WHAT IS PRIVACY?

- Wikipedia - Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively. **The boundaries and content of what is considered private differ among cultures and individuals, but share common themes.** When something is private to a *person*, it usually means that something is inherently special or sensitive to them. **The domain of privacy partially overlaps security (confidentiality), which can include the concepts of appropriate use, as well as protection of information.** Privacy may also take the form of bodily integrity.
- https://en.wikipedia.org/wiki/Privacy
WHAT IS PRIVACY?

• Information Collection
  – Surveillance

• Information Processing
  – Aggregation
  – Identification
  – Insecurity
  – Secondary Use
  – Exclusion

• Information Dissemination
  – Disclosure*
  – Breach of Confidentiality
  – Exposure
  – Increased Accessibility
  – Blackmail
  – Appropriation
  – Distortion

• Invasion
  – Intrusion
  – Decisional Interference

Understanding Privacy
Daniel J. Solove

BRACEWELL
WHAT IS PRIVACY?

• Privacy laws are those laws which govern the collection and use of the personal information of individuals
WHAT IS PRIVACY LAW

Speak the Language
DEFINITIONS

Personally Identifiable Information (PII), Personal Data

• Information that can alone identify an individual

Sensitive Information

• Information that is significantly related to the notion of a reasonable expectation of privacy

Data Collector

Data Subject

Non-PII

Personal Data

Personally Identifiable Information (PII)
ELEMENTS COMMON TO PRIVACY LAWS

• Notice: What data is being collected?
• Choice: Why is it being collected?
• Access: Can the data subject opt-out? How?
• Security: How long will it be used?
• Enforcement: Can the data subject correct/amend?

What is done to maintain personal data?
What if a company violates the law?
**NOTICE**

- Provides the transparency to the data subject
CHOICE

- Opt-in
- Opt-out
- Informed Consent
CHOICE - OPT-OUT

- Consumer Credit Reporting Companies
  - Prescreened offers of credit and insurance
- Telemarketing
- Mail and Email

www.optoutprescreen.com

www.donotcall.gov or call 1-888-382-1222

www.DMAchoice.org

https://www.consumer.ftc.gov/articles/0262-stopping-unsolicited-mail-phone-calls-and-email
ACCESS

• The right to view, amend, delete your data
• Limited right in some circumstances
• Right to be Forgotten
• Right to Know
Privacy ≠ Security
LAWS, WHAT LAWS?

A brief survey of the US and world
US LAWS

No generally applicable US privacy law
Tend to be industry specific or actor specific
Include federal, agency, and state regulations

- Gramm-Leach-Bliley
- Health Insurance Portability Accounting Act/HITECH Act
- Fair Credit Reporting Act (FCRA)
- Telemarketing – The Do Not Call List
- Telephone Consumer Protection Act (TCPA)
- E-Mail Marketing
- Children’s Online Privacy Protection Act (COPPA)
- Privacy Act of 1974
GRAMM-LEACH-BLILEY

• Requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data

• SOFI privacy notice

• Applies to:
  – Banks, brokerages, insurance companies, credit companies, mortgage companies, tax preparers, debt collectors
HIPAA

- Establishes national standards to protect individuals' medical records and other personal health information

- Applies to:
  - Health plans (health insurers), health care providers, health care clearinghouses, health care employee benefit plans, business associates and subcontractors (service providers, including law firms and consultants)

- Does not apply to
  - Insurance entities for life, auto
  - Fitness trackers, mobile applications
  - Wellness programs
COPPA

• Imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age
• Can generally be characterized as an omnibus “code of fair information practices” that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies
EU LAWS

Overarching EU privacy protections
Countries can pass individual legislation
EEA countries pass legislation similar to EU

Directive 95/46/EC (the “Directive”) – Old Law
General Data Protection Regulation (GDPR) – New Law (Enforcement May 2018)
GDPR

- Designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.
- Applies to controllers and processors
NOTABLE DIFFERENCES BETWEEN THE DIRECTIVE AND THE GDPR

• Applicability: Applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company’s location

• Penalties: Enhanced penalties – the greater of 4% of annual global turnover or €20 million

• Consent: Must be intelligible, using clear and plain language; withdrawal must be as easy as giving consent

• Breach Notification: mandatory notification where breach is likely to “result in a risk for the rights and freedoms of individuals”
  o Controllers notify authorities within 72 hours of becoming aware
  o Processors notify controllers “without undue delay”
NOTABLE DIFFERENCES BETWEEN THE DIRECTIVE AND THE GDPR

• Right to Access: Right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose.

• Right to be Forgotten: Lots of attention in the news - entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.

• Data Portability: Right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.
NOTABLE DIFFERENCES BETWEEN THE DIRECTIVE AND THE GDPR

• Privacy by Design: ‘The controller shall..implement appropriate technical and organisational measures..in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects’. Calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.
TRANSFER OF DATA FROM EU TO THIRD COUNTRY

• Under both the Directive and the GDPR, personal data can only be transferred to countries outside the EU when an adequate level of protection is guaranteed
  – Countries deemed to have an adequate level of protection
  – Binding Corporate Rules
  – Model Clauses
  – EU-US Privacy Shield
COUNTRIES RECOGNIZED AS HAVING ADEQUATE PROTECTION

• Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay
BINDING CORPORATE RULES

• Internal rules adopted by group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection
  – European subsidiary transferring to US
  – Officially recognized under GDPR
  – Provides a global compliance solution
  – Flexibility to draft situation dependent rules
  – Available for both controllers and processors

• Process can take 18 months
MODEL CLAUSES

• Standard contractual clauses that provide adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights

• Standard contractual clauses for transfers from EU data controllers to data controllers outside the EU

• Standard contractual clauses for transfers from EU data controllers to processors outside the EU
  – Requires new contract with any new data transfer
  – Not considered commercially friendly (drafted by the Commission)
EU-US PRIVACY SHIELD

• Participating organizations are deemed to provide “adequate” privacy protection when transferring personal data from the European Union to the United States in support of transatlantic commerce.
  – Replaces Safe Harbor
  – Privacy Shield Framework lays out compliance requirements
  – Administered by the Department of Commerce
REST OF THE WORLD

- Argentina
- Australia
- Canada
- Colombia
- Israel
- Malaysia
- Philippines
- Singapore
- South Korea
TALKING POINTS

What is keeping you awake at night?
US PRIVACY REGULATIONS

• Current administration
  – FTC?
  – FCC?
• No overarching privacy regulation
• Big Data concerns
• Employee Privacy
  – Sensitive Information
  – Expectation of Privacy?
  – Disclosures
• State Breach Notification Laws
EU PRIVACY REGULATIONS

• Privacy Shield future is uncertain
• Regulations are complex
• Compliance can take months to a year to implement
• New role: Data Protection Officer
LAST THOUGHTS

• Publicly Available Information
  – Family Tree Now (www.familytreenow.com)
  – Spokeo (www.spokeo.com)

• LinkedIn
  – Me ➔ Settings & Privacy ➔ Privacy Tab (at top) ➔ Profile Privacy ➔ Profile viewing Options, 3 options
  – www.linkedin.com
REMOVING PUBLICLY AVAILABLE INFORMATION

• Family Tree Now
  – Go to http://www.familytreenow.com/optout
  – Read the directions and follow the steps.

• Spokeo
  – Search for yourself (see field at top of webpage)
  – Select your profile (based on name and age).
  – Visit the optout page https://www.spokeo.com/optout
  – Follow the directions
Questions?
LUCY TYSON

Associate

T: +1.713.221.3328
E: Lucy.Tyson@bracewell.com
www.bracewell.com
This presentation is provided for informational purposes only and should not be considered specific legal advice on any subject matter. You should contact your attorney to obtain advice with respect to any particular issue or problem. The content of this presentation contains general information and may not reflect current legal developments, verdicts or settlements. Use of and access to this presentation does not create an attorney-client relationship between you and Bracewell.