ACC Association of Corporate Counsel
GREATER PHILADELPHIA

PRIVACY REGULATION IN A DIGITAL AGE

Thomas Kennedy, General Counsel and Chief Compliance Officer
Versa Capital Management LLC

Jonathan D. Klein, Esq., Attorney
Clark Hill PLC

Scott B. Galla, Esq., Attorney
Clark Hill PLC

2017 IT/Privacy/eCommerce Institute

Making Data Privacy and Security a Priority

Why should you care about this?

- More federal and state laws, increasing penalties
- Theft of consumer information is on the rise, resulting in government investigations, private consumer litigation, and extreme damage/harm to your brand (*e.g.*, Sony).
- Attacks on systems increasing:
  - State-sponsored attacks becoming more commonplace
  - NYSE has suffered several recent incursions

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

What is Privacy?

- Definition of PRIVACY

  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

  www.merriam-webster.com/dictionary/privacy

- Definition of PRIVACY

  [A]bility 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. . . .

  https://en.wikipedia.org/wiki/Privacy

- Information Collected • Information Processing • Information Dissemination • Invasion

- Privacy laws govern the collection and use of the personal information of individuals

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

What is Personal Information?

- Not so easy to figure out without more information!
- One key step in managing privacy risks is to determine what constitutes “personal information” that requires protection.
- Unfortunately, there is no universal “one size fits all” definition of “personal information” otherwise referred to as “PII” under laws in the U.S. or a single applicable legal rule that applies in all circumstances.
- Instead, as will be discussed below, this definition depends upon the particular law that applies, the context in which it is used, and each organization’s privacy policies and procedures.

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

What is Privacy Law?

- **Federal Law**
  - "Sectoral" approach to data privacy regulation.
  - No single, federal regulatory authority dedicated to data protection.
  - Regulatory authority varies by law or regulation in question.
    - For Example: financial + medical data, electronic communications, children's privacy, consumer reports, background investigations
  - Not all regulations mirror each other, creating inconsistencies.

- **State Law**
  - Ten state constitutions reference right to privacy.
  - Hundreds of data/security laws among 50 states and territories.
  - 48 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands all have enacted laws requiring notification of security breaches involving personal information. Alabama and South Dakota are the only states with no security breach notification law.

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

U.S. Laws Impacting Data Privacy and Security

- Administrative Procedure Act. (5 U.S.C. § § 551, 554-558)
- Cable Communications Policy Act (47 U.S.C. § 551)
- Cable TV Privacy Act of 1984 (47 U.S.C. § 551)
- Census Confidentiality Statute (13 U.S.C. § 9)
- Children's Online Privacy Protection Act of 1998 (15 U.S.C. § 6501, et seq., 16 C.F.R. § 312)
- Communications Assistance for Law Enforcement Act of 1994 (47 U.S.C. § 1001)
- Computer Fraud and Abuse Act, as amended by the USA PATRIOT Act (18 U.S.C. § 1030)
- Computer Security Act (40 U.S.C. § 1441)
- Consumer Financial Protection Act of 2010 (Pub. L. No. 111-203, 124 Stat. 1376)
- Criminal Justice Information Systems (42 U.S.C. § 3789g)
- Counterfeit Access Device and Computer Fraud Abuse Act of 1984 (18 U.S.C. § 1030)
- Customer Proprietary Network Information (47 U.S.C. § 222)
- Driver's Privacy Protection Ac (18 U.S.C. § 2721)
- Drug and Alcoholism Abuse Confidentiality Statutes (21 U.S.C. § 1175; 42 U.S.C. § 290dd-3)
- Electronic Communications Privacy Act (18 U.S.C. § 2701, et seq.), Stored Communications Act
- Electronic Funds Transfer Act (15 U.S.C. § 1693, 1693m)
- Employee Polygraph Protection Act (29 U.S.C. § 2001, et seq.)
- Employee Retirement Income Security Act (29 U.S.C. § 1025)
- Equal Credit Opportunity Act (15 U.S.C. § 1691, et. seq.)
- Equal Employment Opportunity Act (42 U.S.C. § 2000e, et seq.)
- Fair Credit Billing Act (15 U.S.C. § 1666)

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

U.S. Laws Impacting Data Privacy and Security

- Fair and Accurate Credit Transactions Act of 2003
- Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.)
- Fair Debt Collection Practices Act (15 U.S.C. § 1692, et seq.)
- Fair Housing Statute (42 U.S.C. § § 3604, 3605)
- Family Educational Rights and Privacy Act (20 U.S.C. § 1232g)
- Freedom of Information Act (5 U.S.C. § 552) (FOIA)
- Genetic Information Nondiscrimination Act (P.L. 110-233, 122 Stat. 881)
- Gramm-Leach-Bliley Act (15 U.S.C. § § 6801, et seq.)
- Health Insurance Portability and Accountability Act (Pub. Law No. 104-191 262,264: 45 C.F.R. 160-164))
- Health Research Data Statute (42 U.S.C. § 242m)
- HITECH Act
- Mail Privacy Statute (39 U.S.C. § 3623)
- Paperwork Reduction Act of 1980 (44 U.S.C. § 3501, et seq.)
- Privacy Act of 1974 (5 U.S.C. § 552a)
- Privacy Protection Act (42 U.S.C. § 2000aa)
- Right to Financial Privacy Act (12 U.S.C. § 3401, et seq.)
- Tax Reform Act (26 U.S.C. § § 6103, 6108, 7609)
- Telecommunications Act of 1996 (47 U.S.C. § 222)
- Telephone Consumer Protection Act of 1991 (47 U.S.C. § 227)
- U.S.A. Patriot Act (Pub. L. 107-56) (bill extending three anti-terrorism authorities signed 02/25/11)
- Video Privacy Protection Act of 1998 (18 U.S.C. § 2710)
- Wiretap Statutes (18 U.S.C. § 2510, et seq.; 47 U.S.C. § 605)

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

ACC Association of Corporate Counsel

GREATER PHILADELPHIA

Elements Common to Privacy Laws

What data is being collected?

Why is it being collected?

Can the data subject opt-out? How?

How long will it be used?

Can the data subject correct/amend?

What is done to maintain personal data?

What if a company violates the law?

Notice • Choice • Access • Security • Enforcement

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

Financial Protection

Gramm-Leach-Bliley Financial Services Modernization Act ("GLB")

- Regulates collection, use, and disclosure of financial information.

- A consumer is someone who has obtained a financial product or service but does not have an ongoing relationship with the financial institution.

- Applies broadly to financial institutions (banks, securities firms, insurance companies) and other business that provides financial information.

- Limits disclosure of non-public, personal information collected by financial institution, and in some cases requires financial institutions to provide notice of their privacy practices and an opportunity for data subjects to opt out of having their information shared.

- Several privacy rules promulgated by national banking agencies and the FTC that relate to protection and disposal of financial information.

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

Health Protection

Health Insurance Portability and Accountability Act of 1996 ("HIPPA")

- Establishes national standards to protect individuals' medical records and to other personal health information.
- Applies to:
  - health plans (health insurers)
  - health providers
  - health care clearinghouses
  - health care employee benefit plans
  - business associates
  - subcontractors (service providers, including law firms and consultants)
- Does **NOT** apply to:
  - insurance entities for life and auto insurance;
  - fitness trackers, mobile applications; or
  - wellness programs

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

General Consumer Protection

Federal Trade Commission

- FTCA (1914) § 5 – Prohibition against unfair or deceptive practices

- Authority
    - CAN-SPAM Act
    - Children's Online Privacy Protection Act
    - Fair Credit Reporting Act

- Consumer Privacy and Data Security
    - Enforcement actions
    - Civil monetary penalties
    - Educational efforts

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

Privacy Policy Primer

- ✓ Provides details about your company's views and procedures on the information collected from visitors.
- ✓ Technically a legal document, but should be written in a way that a lay person can understand its contents.
- ✓ Not something that can be thrown together in a day – requires consultation between company/lawyers.
- ✓ Must contain certain information to comply with various state laws regarding information collection.
- ✓ Should be published conspicuously on any company website once finalized.

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

Terms & Conditions Primer

Can Safeguard Your Company

- ✓ Legally binding?
- ✓ Allocates rights, risks, and responsibilities
- ✓ Allows company to own website content
- ✓ Customizable
- ✓ Limits liability
- ✓ Sets governing law in disputes
- ✓ Outlines prohibited activities on a company website

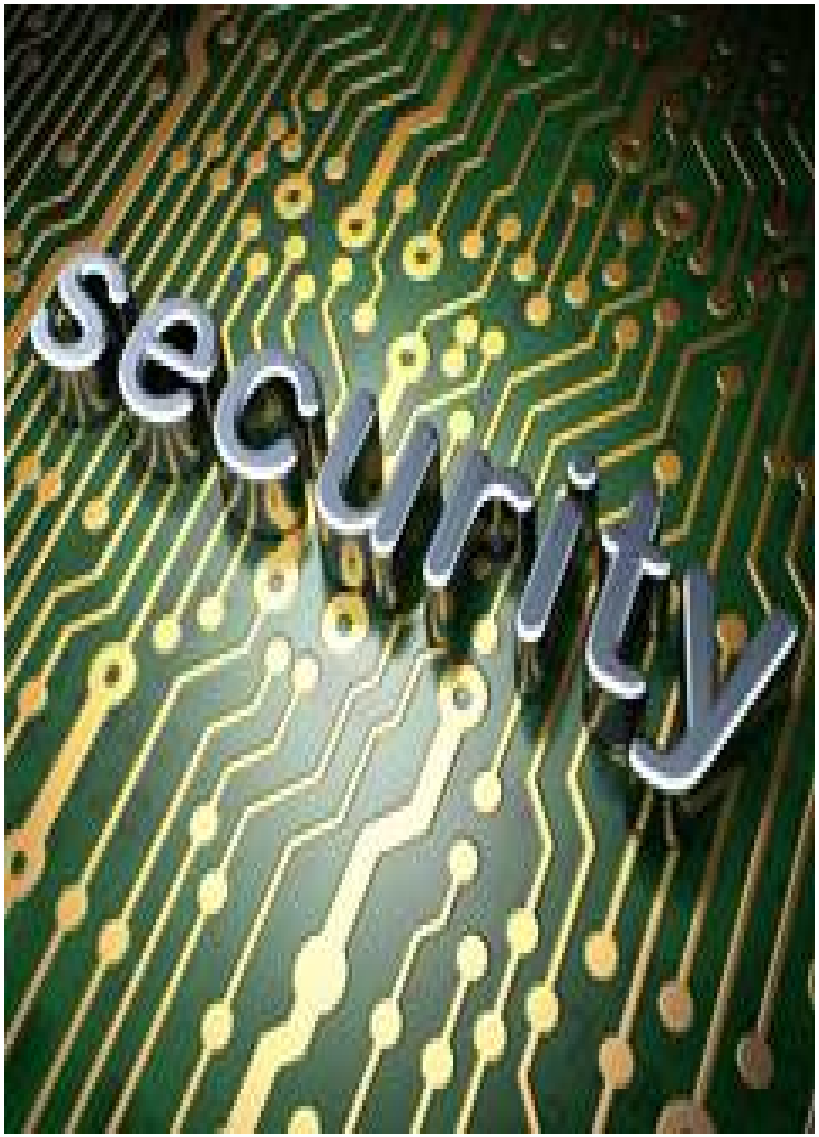
ACC Association of Corporate Counsel
GREATER PHILADELPHIA

Murky Areas in Data Use

- Laws do not expressly address all use
- Disclosures with changing media
- Legal review of novel uses of consumer data
- Context Dependent

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

State of Data Security



- States are becoming more active in enacting data security and privacy policy.
- Why is that?
- As a result, political motivations have become more pronounced.
- Privacy laws are often a convergence of progressive and conservative ideologies.
- In 2017 lawmakers have been explicit about being politically motivated.

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

How to Protect Your Business (1)

- Risk Assessment:
  - What is it, who should conduct it and how should it be conducted?
  - Perform a risk assessment/gap analysis

- Policy Development: Adopt a comprehensive Personal Information Security Policy, addressing policies are needed and the role of in-house and outside counsel in their development.

- Education and Training:
  - Form an Information Security Committee to help implement the new policy
  - Determine who should train corporate personnel and what role in-house counsel plays in that process

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

How to Protect Your Business (2)

- Current data privacy and security laws generally do not contemplate an off-the-shelf policy.

- Any business must first assess the risks relating to the sensitive and personal information it possesses by asking questions about how that information is accessed, used, maintained, processed, disclosed, retained, modified and destroyed.

- Once a risk assessment conducted, businesses need to examine the information they have collected against the safeguards they currently employ to protect it in order to identify vulnerabilities or gaps in those protections.

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

Key Security Questions to Consider

- Have you performed a risk assessment of your business?
- Do you have an actionable incident response plan?
- Have you trained your employees lately on cybersecurity?
- Have you updated your privacy policy?
- Do you have a recent terms & conditions on your site?
- Would you consider your business security aware?

If you answered “NO” to any of these, why is that?

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

Risk Assessment

- Step 1: Identity Information Assets
- Step 2: Classify Information Assets
- Step 3: Identify Security Requirements
- Step 4: Identify Risks

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

Breach Detection and Response

- What is in-house counsel's role in responding to a breach?
  - ✓ Notice:
    - To federal/state agencies;
    - To those impacted by the breach as both a matter of state law and risk management
  - ✓ Mitigation
- The role of notice and credit monitoring
- In post-breach public statements, what key points should be included to minimize litigation risk?
- To what extent can a company be liable for lost data?
- How much can a typical breach cost a company both in time, brand equity and internal distraction?
- What kind of insurance, if any, can a company use to offset costs?
  - Does it really help cover the costs?
- The role of outside counsel

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

Preparing for a Breach

- Incident investigation and response:
  - Preparing for **WHEN** a business will be breached, not **IF** the business may be breached.
- Breach notification and resolution
- Anticipate government investigations and possible litigation, as well as consumer litigation
- Press/public relations strategy

Words to Live by:

Identify & Protect + **Detect, Respond & Recover**

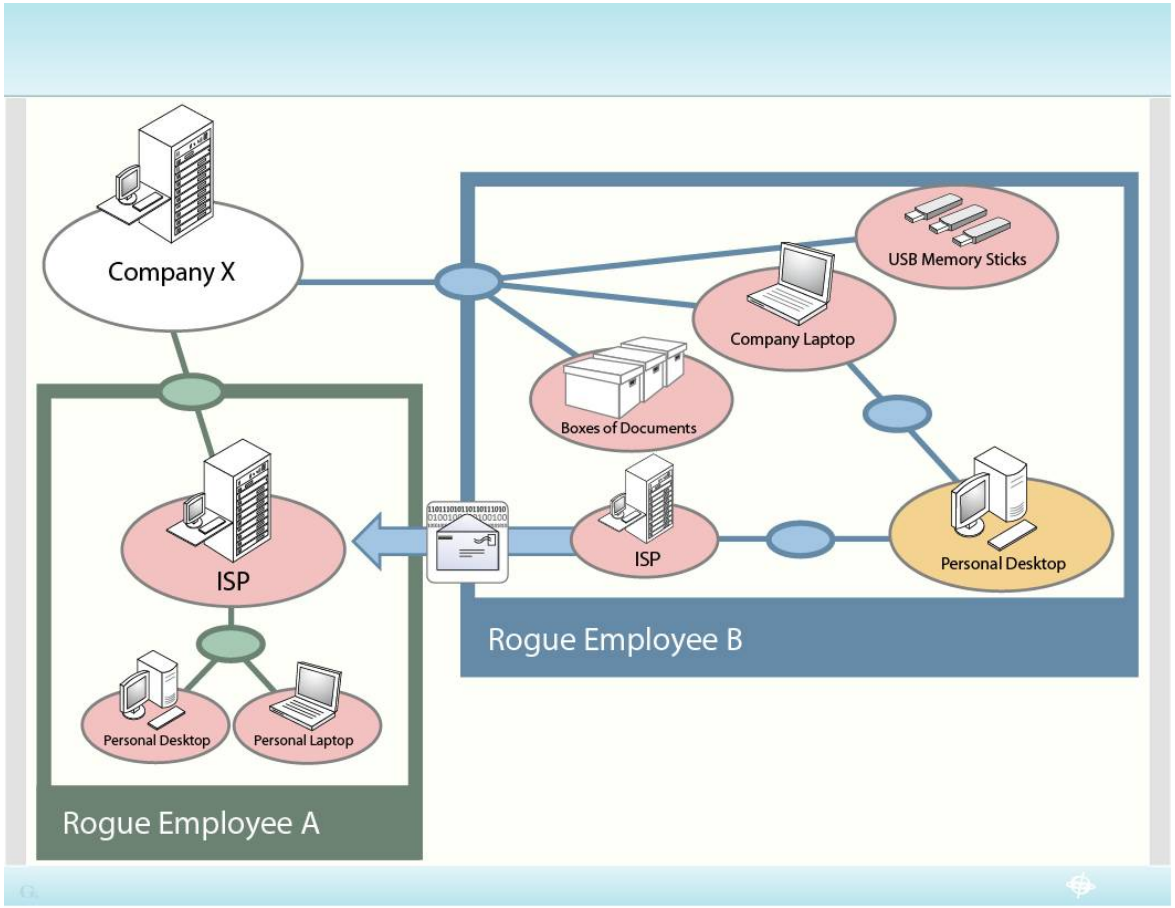
ACC Association of Corporate Counsel
GREATER PHILADELPHIA

Threat Actors

- Cybercriminals
- Hackers
- Hactivists
- Government surveillance
- State sponsored / condoned espionage
- Competitive espionage
- Insiders (disgruntled / dishonest / bored / untrained)

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

Anatomy of a Data Breach



ACC Association of Corporate Counsel
GREATER PHILADELPHIA

Cybersecurity Insurance

- Even with an incident response plan and cybersecurity tools in place, you should still consider cybersecurity insurance as a fail safe to protect your business from cyber risks.

✓ Standalone coverage usually;

✓ Helps companies recover faster from data loss owing to a security breach or other cyber event;

✓ Transfers some of financial risk of security breach;

✓ Investigate current coverage before you apply; and

✓ Know the limitations of your coverage (likely will not cover theft of intellectual property).

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

Types of Insurance

- Data breach/ privacy crisis management
- Multimedia/ Media liability coverage
- Extortion liability coverage
- Network security liability

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

Questions?

Thomas Kennedy
215.609.3400

Jonathan D. Klein
215.640.8535
jklein@clarkhill.com

Scott B. Galla
215.640.8512
sgalla@clarkhill.com

ACC Association of Corporate Counsel
GREATER PHILADELPHIA