Protecting Your IP: Don’t Forget a Privacy Program

Sharon Anolik
President, Privacy Panacea

Sharon Anolik

- President/Founder of Privacy Panacea
  - Privacy Panacea provides strategic, customized privacy solutions to help businesses protect and enable their data
- 15 years of Privacy Officer experience
- Judge, 2015 & 2016 CODiE Awards in the "Best Big Data Solution" and "Best Health & Medical Information Solution" categories
- Numerous privacy advisory roles
  - Data Privacy & Integrity Advisory Committee, Dept. of Homeland Security
  - El Camino Hospital Board of Directors: Vice Chair, Privacy, Audit and Compliance Committee
  - Future of Privacy Forum
  - Internet of Things Privacy Forum

Data *is* IP

- Privacy is concerned with protecting information that is personal, confidential, or private

Company Information	Individuals' Information
Confidential/proprietary company information	Employee/workforce data held by company
Trade secrets	Data assets gathered by company (e.g., customer info)

- Many ways to protect IP: Contract, limit knowledge, police activity, register, programs

More data = more risk

- Loss of proprietary information / trade secrets can be fatal to business
- Loss of customer information can result in:
  - Bad press
  - Loss of customers or potential customers
  - Expense of dealing with breach
  - Investigation / fines from regulators
- Breaches are estimated to cost $154 per record *
- Average breach costs $3.79 Million *

* Ponemon, 2015 Cost of Data Breach Study: Global Analysis

A privacy program helps:

- Define a company's goals, mission and guiding principles around privacy
- Educate employees about privacy standards
- Inform management decisions related to data
- Prioritize internal resources and budget
- Mobilize and delegate staff for privacy matters
- Inform the public/customers about the company's privacy policies
- Document response strategies in case of breach or other incident
- Develop and document accountability measures
- Identify, mitigate and manage risk

Building a privacy program

- Every company has different:
  - Data practices
  - Levels of risk
  - Appetite for risk
- A successful privacy program considers all three factors for the business

Building a privacy program

- Several frameworks can help inform a privacy program:
  - AICPA Generally Accepted Privacy Principles (GAPP)
  - National Institute of Standards & Technology (NIST) standards
  - Fair Information Practice Principles (FIPPs)
  - Organization for Economic Co-operation and Development Privacy Framework (OECD)
  - Federal Sentencing Guidelines (FSG)

Building a privacy program

- Key components of a successful and effective privacy program:
  - Policies and procedures
  - Program governance, culture, and resources
  - Communications
  - Training
  - Monitoring and auditing
  - Enforcement and incentives
  - Investigation and response
  - Risk assessment

Stages of building a privacy program

1. Plan:
   - Develop overarching privacy principles / mission
   - Involve stakeholders from all relevant departments:
     - Legal
     - Compliance
     - Marketing/PR
     - Sales/Business Development
     - Product Development
     - Administration (HR, sourcing/procurement)

Stages of building a privacy program

2. Assess:

- Benchmark current privacy policies and procedures
- Inventory data collected and held
- Document data flows and where data resides
- Determine what practices need remediation to align with mission / principles
- Determine gaps where practices need to be developed
- Make decisions based on risk appetite of company

Stages of building a privacy program

3. Remediate/build:

- Develop a roadmap: A plan of action that lays out projects and target dates based on priorities and maturity goals
  - Get buy in from the top!
- Delegate individuals responsible for carrying out and overseeing projects
- Implement accountability measures

Stages of building a privacy program

4. Implement:

- Roll out new policies and procedures to relevant departments and personnel
- Ensure personnel are trained on new or changed policies and procedures

5. Monitor:

- Assess privacy practices on a continuing basis
- Consider undergoing ongoing audits / risk assessments at planned intervals

Then you can take your privacy program to the next level…

© MARK ANDERSON, WWW.ANDERTOONS.COM

"Before I write my name on the board, I'll need to know how you're planning to use that data."

Data Minimization

- Do not collect more data than necessary
- Do not use data outside the stated purpose of the product/process and not extend beyond consent and authorization agreements
- Implement least privilege and limit access to data to those who are appropriately authorized and have a business need to access the information

Privacy by Design (PbD)

- Include privacy and security in product development decisions
- Make privacy the "default" setting for consumer-facing products
- Ensure privacy and security of information throughout the data lifecycle

Remember…

- Data is IP; IP is data
  - Privacy is concerned with protecting data that is private or confidential, including a company's IP
- Building a privacy program will protect a business's IP and its customers
  - Like a strategic IP program, a privacy program will help streamline, prioritize, and maximize privacy protection efforts
  - Privacy programs should take into account practices and levels/appetites for risk unique to the business
- Maintaining good privacy practices is an ongoing process—as the business matures, consider more advanced models such as data minimization and PbD

Questions?

Thank you.

Sharon Anolik, Esq., CIPP
President, Privacy Panacea

datastrategy@yahoo.com
@PrivacyPanacea