Building a Defensible Privacy Program

ACC NCR Privacy Summit
Tuesday, September 20, 2016
Introductions

• Toke Vandervoort - VP & Deputy General Counsel, Under Armour

• Randy Sabett, J.D., CISSP – Vice Chair, Privacy & Data Protection Practice, Cooley LLP

• Jessica Geller - Commercial & Privacy Counsel, Blackboard, Inc.
Agenda

• Part 1 – Global Privacy Today

• Part 2 – New Product Privacy Bingo

• Part 3 - Privacy Program Building Blocks
Part 1

Global Privacy Today
Global Privacy Laws
around the globe

Source: Forrester Research
http://heatmap.forrestertools.com
Global Privacy Laws by the numbers

109 Countries have data privacy laws
22 Countries with new laws proposed
32 Country increase since 2011

Some US Laws, Regulations and Industry Standards That May Apply to Your Business

- EU Directive – General Data Protection Regulation (GDPR)
- COPPA (Children’s Online Privacy Protection Act)
- Sarbanes-Oxley Act (SOX)
- Gramm-Leach-Bliley Act (GLB) Act
- Electronic Fund Transfer Act, Regulation E (EFTA)
- Federal Information Security Management Act (FISMA)
- NLRB and State Workplace Privacy Standards
- Customs-Trade Partnership Against Terrorism (C-TPAT)
- Free and Secure Trade Program (FAST)
- Code of Federal Regulations regarding Electronic Records
- U.S. SAFE Web Act
- Controlling the Assault of Non Solicited Pornography and Marketing (CAN-SPAM)
- Standards for Safeguarding Consumer Information
- Identity Theft Assumption and Deterrence Act
- FERPA (Family Educational Rights and Privacy Act)
- Graham-Leach Bliley (GLB)
- Video Privacy Protection Act
- Fair Credit Reporting Act (FCPA) and the Red Flags Rule
- Telecommunications Act Section 222 and Customer Proprietary Network Information (CPNI) Regulations
- Secure Flight & Secure Flight Passenger Data Rules
- Family & Educational Rights and Privacy Act (FERPA)
- U.S. Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act
- Health Insurance Portability and Accountability Act (HIPAA)
- Genetic Information Nondiscrimination Act (GINA)
- Patient Safety and Quality Improvement Act (PSQIA, Patient Safety Rule)
- Fair and Accurate Credit Transactions Act (FACTA) & the Red Flags Rule
- Dodd-Frank Wall Street Reform and Consumer Protection Act
- Electronic Communications Privacy Act (ECPA)
- Stored Communications Act (SCA)
- Telephone Consumer Protection Act (TCPA) and Junk Fax Prevention Act (JFPA)
- Telemarketing & Consumer Fraud and Abuse Prevention Act, Telemarketing Sales Rule (TSR)
- Do Not Call (DNC)
- Computer Fraud and Abuse Act (CFAA)
- Anti-Money Laundering Laws
- Protection of Pupil Rights Amendment (PPRA)
- Voter Privacy Laws
- State Laws: e.g., Breach Notification; Biometric Data protection; Mandatory data encryption laws; Reasonable security measures
- Privacy Shield
- Federal Rules of Civil Procedure (FRCP)
- ABA and other professional ethics rules
Some International Laws and Standards That May Apply to Your Business

- European Union:
  - Data Protection Directive, General Data Protection Regulation and EU member states’ specific implementation
  - EU Right to be Forgotten
  - Privacy Shield
  - The Strasbourg Convention for the Protection of Individuals and Automatic Processing of Personal Data (ratified by 47 members countries in the Council of Europe)
- Canada: Personal Information Protection and Electronic Documents Act (PIPEDA) and Personal Information Protection Act (PIPA)
- Japan: Act on the Protection of Personal Information
- China:
  - National Standard of Information Security Technology Guideline for Personal Information Protection within Information Systems for Public and Commercial Services;
  - Law of Consumer Rights and Interests;
  - Decision on Strengthening Protection of Online Information (“the Decision”)
- Australia: Federal Privacy Act, National Privacy Principles and territory laws
- Brazil and Chile: Constitutional recognition of privacy rights
- Argentina and Peru: Personal Data Protection Law (PDPL)
- Mexico: Law on the Protection of Personal Data Held by Private Parties
- South Africa: Protection of Personal Information Act
- Egypt: Constitutional recognition of privacy rights
- India: Information Technology Act with specific provisions intended to protect electronic data
- Russia: Law No. 242-FZ “Order to Clarify the Procedure for Personal Data Processing in Information and Telecommunications Networks”
Some Industry Standards and Guidelines That May Apply to Your Business (often incorporated by reference – WATCH OUT for this)

- Payment Card Industry Data Security Standards (“PCI”)
- Financial Industry Regulatory Authority (FINRA)
- Voluntary FTC Guidelines (e.g., Privacy by Design guidelines)
- National Institute of Standards & Technology (NIST) various guidelines
- North American Electric Reliability Corp. (NERC) standards
- The Chemical Facility Anti-Terrorism Standards
- National Association of Insurance Commissioner’s (NAIC’s) Model Regulation on Privacy of Consumer Financial and Health Information
Some Self-Regulation Standards That May Apply to Your Business

- Better Business Bureau – online privacy program
- Trustee and other trust certification
- Digital Advertising Alliance
- Network Advertising Initiative
- Direct Marketing Association
- Online Privacy Alliance
- Individual Reference Service Group
- Privacy Policies
Emerging Technologies - New Privacy & Security Trends
-or-
new stuff that may regulate your business

• IP and Edge technologies (search engine, social media; content delivery)
• Mobile Apps
• Location Tracking
• Social Networking
• Indirect marketing techniques
• Cloud Solutions
• Internet of Things
• Wearables
• “Indirect” marketing techniques
New Product Panic: A Dramatization

- or -

“Why does my refrigerator tweet that I’m out of meat?”
New “Smart” Refrigerator

Shipping to retailers in the US, EU, Canada and Russia in a month

*Is there a problem here?*
Refrigerator Role Play - Recap

• **BINGO - Issue Spotting**

• **STANDARDS CAN BE HARD, EVEN IMPOSSIBLE, TO HARMONIZE**

• **PENALTIES** for failures to protect data from misuse or security breach range from:
  - Fines
  - Audits
  - Ongoing governmental oversight
  - Potential litigation
  - Business disruption and cost
  - Loss of customer trust and business
  - Loss of stock value
  - Possible criminal sanctions

• **BUILDING A DEFENSIBLE PRIVACY PROGRAM IS KEY**
Part 3

What Should a Privacy and Information Security Program Look Like?
Roadmap of New Privacy Program

1. Know your company’s business and how data is collected
2. Understand where your Company’s Data is located and how your Business Processes use that data
3. Determine what Rules/Laws/Regulations apply
4. Assess Risk
5. Engage with the Business and establish High Level Privacy and Security Principles
6. Develop Strategic Vision with Cross Functional Decision Makers
7. Create clear Policy statements
8. Train
9. Harmonize practical Guidelines
10. Determine Applicable Compliance Regimes
11. Expand Training
12. Audit
Privacy Program Building Blocks: A Governance Structure

- Integrate business into privacy and security program ownership

- Privacy and Security Champions and/or Information Governance Review Board

- “Tone from the top” – everyone in company needs to buy in to the privacy and security program
Security and Privacy are Co-joined

The attackers are getting in faster and it takes a significant amount of time to find and get rid of them

Verizon, “Data Breach Investigation Report”
2012 v 2016
Privacy Program Building Blocks: Knowledge of Company’s Business and Regulatory Environment

• How personal information is managed, used, secured by the business?

• What rules apply?

• Where is your data located?
Privacy Program Building Blocks: A Risk Assessment Methodology

- High level privacy risk assessment
- Privacy Impact Assessment
- Focus attention first on what matters most to move the ball forward
- Develop an Inventory of Applicable Law and Regulation Policies, Procedures and other Guidance
Privacy Program Building Blocks: Identify Major Compliance Areas

Know your enforcement authorities and the penalties they can impose on your business for privacy and security failures
Examples of Increased Oversight and Expanded Enforcement by FEDERAL Regulators

- **On July 29, 2016, the FTC announced its decision in LabMD case**
  - A company's mere public exposure of sensitive consumer information can constitute a substantial consumer injury supporting a Section 5 "unfairness" violation, without evidence that anyone ever misused the consumer information.
  - A company may violate Section 5's prohibition on "unfair" practices if its data security practices risk a consumer injury of large magnitude, even if the likelihood of the injury occurring is low.

- **On April 5, 2016, NTIA asked for public comment on role of government in IoT**
  - NTIA issue a "green paper" that will identify “possible roles for the federal government in fostering the advancement of IoT technologies”
  - NTIA doesn’t have authority to adopt regs; expectation would be for FTC to enforce

- **On June 30, 2015, FTC released a “10 Lessons” guidance document:**
  - (1) Start with security. (2) Control access to data sensibly. (3) Require secure passwords and authentication. (4) Store sensitive personal information securely and protect it during transmission. (5) Segment your network and monitor who is trying to get in and out. (6) Secure remote access to your network. (7) Apply sound security practices when developing new products. (8) Make sure your service providers implement reasonable security measures. (9) Put procedures in place to keep your security current and address vulnerabilities that may arise. (10) Secure paper, physical media, and devices.
Increased Oversight

SEC: Division of Investment Management

- Recommendations concerning three broad areas of a firm’s cyber posture:
  - Conduct regular assessments of cyber activities (including cataloging of information, threat analysis, security controls, and governance structure)
  - Create a cybersecurity strategy for the firm
  - Implement the strategy, including policies, procedures, and training
- Language from the NIST Framework (“take into account these obligations when assessing their ability to prevent, detect and respond to cyber attacks”)

DOJ: Cybersecurity Unit

- Before an attack: identify crown jewels, put actionable plan into place, ensure legal counsel is familiar with cyber issues, engage with LE, and do info sharing
- Once an attack occurs: assess and contain damage, collect all relevant information, and notify all required parties
Increased Oversight and Enforcement by STATE Regulators

California AG

- Analysis of info provided to AG pursuant to breach notifications
- 60% of Californians (approx 24M) affected by a data breach in 2015, six times the 4.3M Californians affected the year before
- AG has made four recommendations:
  - Implement the 20 CIS Critical Security Controls
  - Expand the use of multi-factor authentication
  - Use strong encryption to protect PII on portable devices
  - Encourage consumers use of fraud alerts on their credit files
- **WARNING**: “failure to implement all the [applicable] Controls … constitutes a lack of reasonable security”
Privacy Program Building Blocks: Operationalize Privacy

- Integrate into Existing Processes
- Build awareness
- Forge cross functional relationships to address privacy questions (include Product Development, Procurement, Vendor Management, IT, Marketing, Customer Care, HR, etc.)
- Train!
- Test - Internal checks to test policies, practices, personnel and plans
- Train some more
Privacy Program Building Blocks: Testing, Audit and Other Verification

• In the supply chain
  • Independent certifications
  • Self assessment programs
  • Standard self assessment questionnaires
  • Self certification
  • Audit rights
Privacy Program Building Blocks: Incident Response

**Preparedness is Essential**

- **Mission**
  - A sound, tested plan should enable quick, confident action to protect brand value, preserve customer trust, mitigate financial losses and penalties, notify, etc.

- **Scope**
  - Map out everything from initial detection and analysis > team activation > reporting and communication strategy > engagement of resolution partner, law enforcement, legal, and other third parties > post event analysis, correction and training > updating of IRP

- **Team**
  - Identify the right contributors in advance who will bring with the right experience, skills and responsibilities to engage appropriately at the right time – Legal & Privacy, Response Partner, IT & Security, PR, Law Enforcement
Recognize that a Privacy and Security Program is a *living, breathing* thing that needs to adapt to ever-changing business, technology, legal, cultural, risk and threat environments.
Additional Materials

- International Data Control Checklist
- Privacy Shield Checklist
- Incident Response Plan Development Checklist
- Client Alerts
Contact Information

- Toke Vandervoort - VP & Deputy General Counsel, Under Armour
  tvandervoornt@ua.com

- Randy Sabet, J.D., CISSP – Vice Chair, Privacy & Data Protection Practice, Cooley LLP
  rsabett@cooley.com

- Jessica Geller - Commercial & Privacy Counsel, Blackboard, Inc.
  jessica.geller@blackboard.com
Building a Defensible Privacy Program

ACC NCR Privacy Summit
Tuesday, September 20, 2016