PUTTING PEOPLE FIRST
Protection of Personal Identifiable Information (PII) in a Landscape of Constant Change

Whitney Tom
Program Manager
Corporate Partnerships

Nahla Sahra
Senior Program Manager
Corporate Partnerships

October 22, 2018

---

Agenda

1. Fact Finding Process & People
2. PII Definition
3. Landscape of Constant Change
4. How Much to Invest
5. Proposed Strategies to Address Risks

---

Fact Finding Process & People
Methodology
Focus group discussions, key informant interviews, secondary research, and primary experience.

Thank You to Subject Matter Experts at the Following Companies
Baker Tilly
Dentons
UK Country Lead for International Association of Privacy Professionals (IAPP)
Netflix
Schmidt Futures / Former White House Policymaker
Symantec
TechSoup
Veritas

What is Personal Identifiable Information (PII)?
"Any data that could potentially be used to identify a particular person." — Evannlee acute

"Any information about an individual that can be used to distinguish or trace an individual's identity and any other information that is linked or linkable to an individual." — Regulation of the Internet and Technology (RIT)

Examples

Jane Doe
VS.
Jane Doe
Date of Birth
Address

U.S. PI Definition
EU: GDPR Core Philosophy of Personal Data

Landscape of Constant Change

Global Trends
- Multinational nature of information sharing
- Global dependency on third parties (such as Google, Facebook and WhatsApp, etc.)
- People's willingness to provide information
- Expanding technology capabilities, both the good and the bad
- Regulation updates and enforcement
- Data and IP ownership: Control vs. ownership
Global Trends

People's Willingness to Provide Information

1. How many companies have you provided the last four digits of your social security number to in the last six months?
   - a. 1–5
   - b. 6–10
   - c. 10+  

2. When was the last time you allowed access to your personal information in order to register or sign up for an online service?
   - a. Less than a month ago
   - b. Within the last six months
   - c. Within the last year
   - d. Never

Sociopolitical Factors

- Historical context in Europe: Authoritarian governments' use or potential use of PII
- World War II
- Balkans War
- Increasing pressure on governments to respond to businesses' control and access to PII
- Changing consumer expectations or concerns
  - Personalization of advertisements
  - Internet of Things

Case Study: Europe

- EU Data Protection Directive
- Google Established
- Safe Harbor Privacy Principles
- Facebook Launched
- Safe Harbor Overturned
- EU GDPR

2004
2015
2019
Changing or Reinforced Regulations in the Past Two Years

Australia (February 2018)
The Notifiable Data Breach (NDB) scheme under Part 11C of the Privacy Act 1988 (Privacy Act)

Canada (November 2018)
New data breach disclosure rules in the Privacy Act, Chapter 37

China
June 2017: Partial implementation of 2016 Cybersecurity Law for data localization and export
October 2017: General Provisions of the Civil Law (personal information as civil right)

India (August 2018)
Article 35 of the Indian constitution stipulates that privacy is a fundamental right

Changing or Reinforced Regulations in the Past Two Years

Israel (May 2018)
The Privacy Protection Regulations (Data Security), 5778/2018

Japan (May 2018)
Japanese Act on Protection of Personal Information

Mexico (January 2018)
Federal Law on Data Protection for the Public Sector

Singapore (February 2018)
The Cybersecurity Act

United States (March 2018)
Clarifying Lawful Overseas Use of Data Act (CLOUD Act)
- Alabama Data Breach Notification Act in May 2017
- California Consumer Privacy Act in June 2018
- New Mexico Data Breach Notification Act in June 2017
- South Dakota Senate Bill 62 in July 2018

California’s Consumer Privacy Act of 2018

- Who? Any for-profit company with California-based assets or customers
- What? Expanded definition of “personal information” that includes almost any consumer-related data that a for-profit company collects or maintains
- Different from GDPR? Nonprofit fall outside of the Act’s ambit, and potentially stricter consumer-facing compliance mechanisms and protocols

Economic Factors

- The cost of doing business
- Tech companies = businesses
- IoT as a currency
- Data is in the new oil
- Globalized markets and trade
- “The cloud” = Software as a service (SaaS)
- Outsourcing of work or rather, an expanded breadth of a globalized workforce
How Much to Invest

But First, Why Invest?
1. TRUST
2. TRANSPARENCY
3. $$$

No Matter How Big or Small You Are, We Found That We All Need to Take the Same Four Steps

STEP 1
Map the Data Flow
Know what data you have, where it flows to and from, and who has access to it.

Do you know where your company or organization has PII?
- Yes
- Most of it
- Some of it
- Not really
- Definitely not

While you wait, take a piece of paper and try to draw the data flows for where your company stores, processes, and shares PII (if any).
STEP 2
Assign Ownership
Who is responsible for knowing where PII flows within your organization or company and how to monitor it and detect it if necessary?

POLL
Who is responsible for ongoing ownership over your organization's protection of PII?
- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Human Resources
- Data Security Officer
- Privacy Officer
- Chief Technology Officer
- Other

STEP 3
Monitor Regulations
Many partners struggle with keeping up to date with the changes and new regulations due to the complexity of the regulations, lack of resources, or budget restrictions.

POLL
How do you keep up with regulation changes?
- Paid legal service or monitoring service
- Listerves
- News outlets
- Ad hoc research
- I don't know, it's not my responsibility

RECOMMENDATION
Establish a system based on the most strict regulation. Different geographies create new and interesting challenges.

STEP 4
Train Staff
On how and what data to erase or delete.

POLL
Does your company or organization have mandatory data security training programs?
- Yes, annually
- Yes, but not regularly
- Sometimes
- I'm not sure
- Not that I'm aware of
How Much to Invest: Small Companies and Nonprofits

- Nonprofits  
- Small Companies  
- Startups

Do the Basics

1. MAP YOUR PI DATA FLOWS:  
   Understand if you have PI and what it is, where it is coming from, and where it is stored.
2. Read the fine print on contracts with third parties.
3. Limit access to applications that use PI.
4. Create clear rules internally on data security and train your team.

How Much to Invest: Mid-Size Enterprises

- Mid-size companies (500 – 1,000 employees)

Invest in Your Priorities

1. Technology that maps your data
   a. For example, Vertex Data Insight
   b. Automated deletion; minimize the data you store
   c. Dig into why you need that data
2. Access management
   a. Enterprise-wide automation to manage access to applications that use PI
3. Training on data security per job function

How Much to Invest: As an Individual

Whether you're a compliance officer or an individual contributor, there are basic steps you can take or questions you can ask to contribute to protection of PI:

1. Think Before You Send
   a. Does the email contain PI or a file?
   b. Can the receiver verify the email?
2. Think Before You Sign
   a. Has anyone verified the content of the email?
   b. Are the terms agreeable to you?
How Much to Invest: TechSoup as a Case Study

- Privacy policy — clearly state how information is shared (no legal jargon please)
- Be honest about where your organization is in its digital transformation with partners
- Surprising actions taken by companies
  - Sharing information about fraud trends
  - Increased demand for preemptive action before integration with partners

Proposed Strategies to Address Risks to PII

- Understand the regulations you need to comply with
- Do the basics — access management, restrict access to PII, password management
- Map your data as best you can in any way you can — whiteboard, PowerPoint, etc.
- Train employees on PII and how to protect their and their customers’ PII
- Don’t rely on third parties to “take care of it”
Proposed Areas of PIIRisk That Tech Can Help With

- **Data Mapping**
  - Where do you process and store PIIR?

- **Access Management**
  - How do you remember who needs access and how often?

- **Data Classification**
  - How do you identify PIIR?

- **Automated Training**
  - How do you remember who can edit, process, view, or delete?

- **Third Party Management**
  - Who has access to your PIIR for your customers or partners?

---

**How Can Technology Help?**

1. **Privacy Notification and Tracking of External Parties**
   - With so many users accessing most of your websites, be sure to add a notice to help ensure all online users accept your Privacy Policy.

2. **Automating Access Management**
   - Internal access management
   - Machine learning to predict behavior

3. **Automate and Standardize Workforce Training**
   - Given widespread use of automation, we recommend you leverage your workforce training on an automated system, rather than on a periodic or batch-based basic training.

4. **Map Data Flows**
   - Map data flows to map simple data flow diagrams using Microsoft Visio or LucidChart.com

---

**Exception**

- If your personal information is encrypted when it’s stored and transmitted, there is also no chance of a privacy breach.

---

**Thank You from TechSoup!**