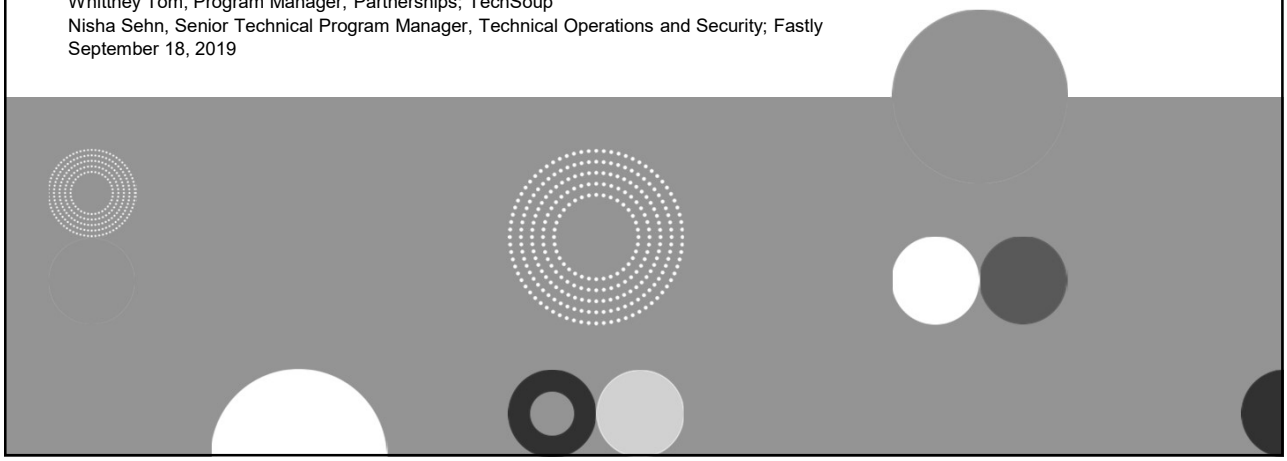
techsoup
fastly

Managing Data and Promoting Privacy

A deliberate peer-to-peer exchange of ideas on how to comply with rapidly changing cybersecurity and privacy compliance obligations.

Whittney Tom, Program Manager, Partnerships; TechSoup
Nisha Sehn, Senior Technical Program Manager, Technical Operations and Security; Fastly
September 18, 2019



1

PRIVACY NOTICE

This session is recorded. While we want you to have detailed conversations about your current and/or previous companies' data management and privacy practices, please only share what is not confidential and/or compromising.

2

Session Objectives

1. Provide people with info and tools to create or bolster their own data management and privacy posture practices
2. How to encourage cross-team collaboration
3. Share learnings and connect with your colleagues

3

3

Agenda

1. Setting the Scene
   - Findings from the Field (2018 - 2019)
2. Facilitated Dialogue
   - Live polling
   - Pairs and small group discussion
   - Scenario exercise
3. Tactful Tech Tools
4. Key Learnings

4

4

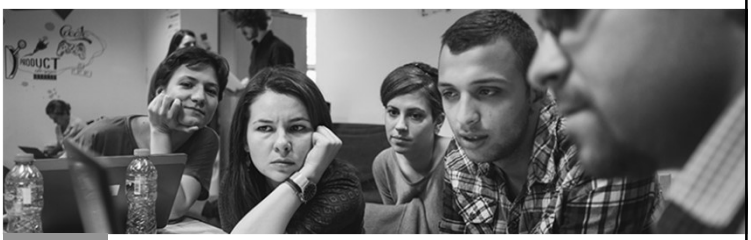
Setting the Scene

5

Fact Finding Process and People

Methodology

Focus group discussions, key informant interviews, secondary research, and primary experience.



Thank you to the subject matter experts at the following organizations:

- Baker Tilly
- DocuSign
- International Associate of Privacy Professionals / EQI
- Schmidt Futures
- Symantec
- TechSoup
- Veritas

techsoup

6

Landscape of Constant Change

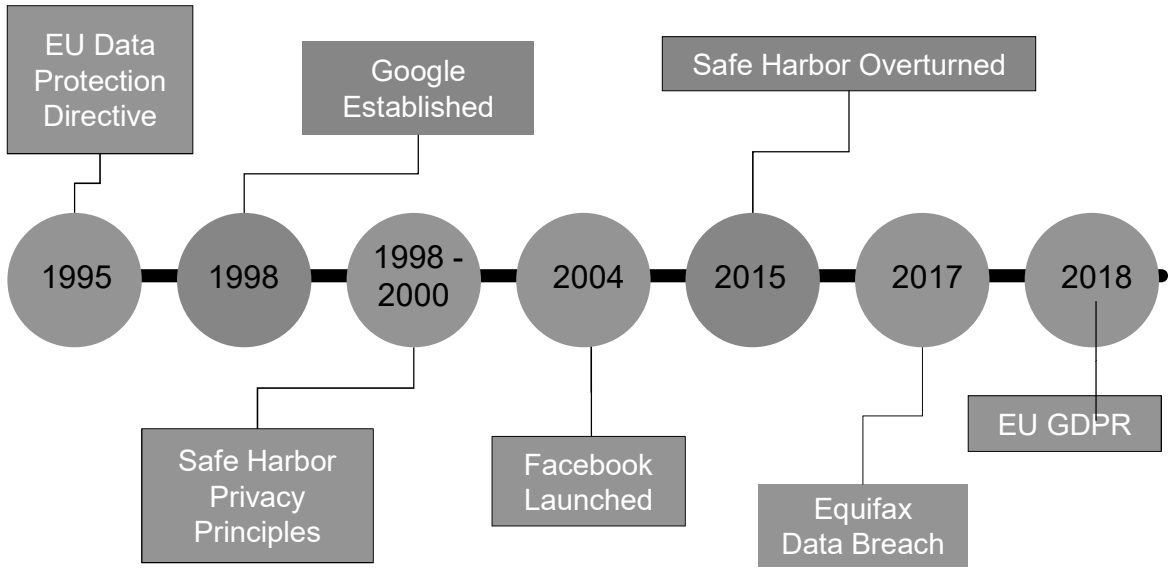
Global Trends

- Multinational nature of information sharing
- Global dependency on third parties (e.g. Google, Facebook + WhatsApp, etc.)
- People's willingness to provide information
- Expanding technology capabilities, both the good and the bad
- Regulation updates and enforcement

techsoup

7

Blast from the Past



techsoup

8

Landscape of Constant Change

Changing/Reinforced Regulations in the Past Two Years

- **Australia** - February 2018
  - Fines up to $2.1 million
- **Canada** - November 2018
  - Fines up to $100,000
- **China** - June 2017
  - Cybersecurity Law of China
- **India** - August 2017
  - Supreme Court Recognition; Pending Data Protection Bill
- **Israel** - May 2018
- **Japan** - May 2017
  - Expanding PII definition to include biometric data
- **Mexico** - January 2017
- **Singapore** - February 2018
- **United States**
  - New Mexico
  - Alabama
  - California's Consumer Privacy Act of 2018

techsoup

9

Last Year's Findings

No matter how big or small you are, we found that we all need to take the same four steps

STEP 1: **Map the landscape** - Know what data you have, where it is, and who has access to it.

STEP 2: **Assign ownership** - Who is responsible for knowing where PII flows within your organization or company and how to monitor it and delete it if necessary?

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.

STEP 4: **Train staff** on how/what data to erase/disclose.

techsoup

10

How Much to Invest: Small Companies/Nonprofits

- Nonprofits
- Small Companies
- Start-ups

Do the basics:

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

techsoup

11

How Much to Invest: Mid-Size Enterprise

- Mid-enterprise size companies
  - 250 + employees

Invest in your priorities

1. Technology that maps your data
   a. E.g. Veritas 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 PII.
3. Training on data security per job function

Source: Johns Hopkins University

techsoup

12

Setting an Example

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 PII.

1. **Think before you send** - does it have PII in the email or attachment? Does the receiver need the PII you are able to send?
2. **Think before you sign** - Read privacy policies and fine prints on contracts before you sign.

techsoup

13

14

LIVE POLL

On a scale from 1-5, how confident are you that you understand your company's data flows AKA data management reality?

15

Data Mapping Exercise

- Bilateral neighbor chat: Share how you map your company's data (if you can, try and draw it out) and explain it briefly (barring confidentiality clauses) or share why you don't have a data flow map, how you have tried to do it and failed, or what you do instead.
- Find another pair
- Room read-out

Pro Tip: Differentiate between data that is **processed vs. controlled** in a **private, public, or both types of, cloud**.

techsoup

16

Cybersecurity Regulations Monitoring

***Bilateral neighbor chat**: How do you monitor cybersecurity obligations? (such as India's Article 21, CCPA, etc.)*

- Is your approach manual, automated, or a hybrid approach?
- Find another pair
- Room read-out

Source: Johns Hopkins University

techsoup

17

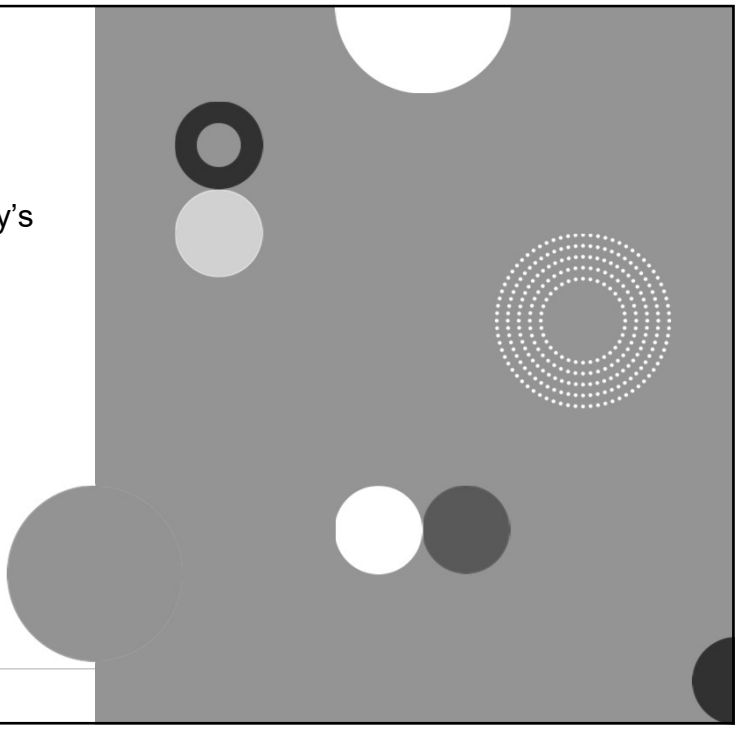
LIVE POLL

Who is legally accountable for compliance with your company's data management and/or privacy policies?

- *Legal*
- *Information Technology (IT)*
- *CEO/President*
- *Ethics and Compliance*
- *Finance*
- *Two or more functions listed above*
- *It's not clear at my company, we are still figuring that out…*
- *Other - fill in*

18

Raise your hand if you are **accountable** for your company's data management.



19

19

Build an ARCI Exercise (Independently)

	Accountable	Responsible	Consulted	Informed
Data Management Globally (Controller)				
FILL IN				

Source: Johns Hopkins University

techsoup

20

ARCI Exercise
Facilitated Discussion in Pairs

1. Who is responsible for data management?
   In other words, who is actually implementing or working on your company's compliance with your data management policy?

2. Discuss with a new neighbor about whether the answer to the last two questions (who is accountable vs. who is responsible) is the same person, different, or if it's complicated. Discuss how that impacts your role at the company.

techsoup

21

ARCI for Cross-Team Collaboration
Facilitated Group Discussion

In groups of 4-5 people, discuss the following questions:

1. What teams are consulted or responsible for any change management when there is a data management regulation change?
   - Examples: IT (development/internal IT), Human Resources, Legal, Finance, Compliance

2. Who is responsible for ensuring this cross-team collaboration?
   For example:
   - Who starts this conversation?
   - Who sets up and leads the meetings?
   - Who documents the plans and evidence of determined compliance?
   - What technology do you use to support this cross-team collaboration for complying with data management?

techsoup

22

Scenario: 5-8 minutes

On the two year anniversary of GDPR, the EU announces that all companies must have a mandatory external-facing tool that users can check their opt-in or opt-out status as a “self-serve” function.

Instead of the usual approach of scrambling in the background to comply with customers opt-in/out requests, it’s now external facing. What teams would you/your company involve to address this new obligation?

techsoup

23

Raise your hand if any of your solutions required technology changes or developments.

24

Tactful Tech Tools

25

Tactful Tools

Privacy Notification and Tracking of External Parties

- With so many users accessing most of your websites, we recommend enlisting a service to help ensure all visitors read and accept your privacy policy.

Automating Access Management

- Internal access management: identity-based or device-based.
- Machine learning to predict staff behavior.

Automate/Standardize Workforce Training

- With high turnover in a lot of companies and nonprofits, generally, we recommend you base your workforce training on an automated schedule.

techsoup

26

Key Learnings

27

Key Learnings
Proposed Strategies to Address Data Management and Privacy

What did we come up with?

techsoup

28

29