RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **IDP-F05V**

Build Privacy into Your Products and Gaining User Trust

Sara Gerber

Privacy & Security
Chan Zuckerberg Initiative

Agenda

1. Regulations – they aren't going away
2. What is User Trust? – *OR* how do I explain cookies to someone who doesn't understand how the internet works?
3. Framing the problem
4. How we approached it
5. Lessons and Learnings!
6. Your turn!

RSAConference2020 APJ

A Virtual Learning Experience

Part 1: Regulations

Problem or Opportunity

Regulations

Everyone has an approach!

- European Union – **General Data Protection Regulation**
- HIPAA – **Health Insurance Portability and Accountability Act**
- Japan – **Act on the Protection of Personal Information**
- Korea – **Personal Information Protection Act**
- Singapore – **Personal Data Protection Commission**

Regulations

Data Types

- Sensitivity levels
- Notification requirements
- Age restrictions

User Rights

- Access
- Preferences
- Deletion
- Marketing

RSAConference2020 APJ
A Virtual Learning Experience

Part 2: User Trust

Add transparency

User Trust

- What do users want?
  - The service you're offering (clearly)
  - To understand what it 'costs' them even if your offering an open source or free product (people are skeptical of a free service)
  - How to start and stop use of the service
  - To understand what is being collected versus what is being provided Policies / FAQs

User Trust

- Why is it so hard to communicate about data?

  We built systems and products to work and provide services – without thinking about individual components.

  - Data Collection
    - Cookies
    - User Agents
    - Authentication
  - Data Locations
    - Databases
    - Connectors
    - Servers
    - Raw Logs
  - Data Access
    - Centrally managed SSO
    - One person with Credit Card

RSAConference2020 APJ
A Virtual Learning Experience

Part 3: Framing the Problem

Stakeholder Engagement

Framing the Problem

- **Ideally, we should be able to answer:**
  - What data we collect
  - Where our data is stored
  - Where our data in sent
  - Who has access to that data
  - Why we are collecting that particular data point

RSAConference2020 APJ
A Virtual Learning Experience

Part 4: One Approach

Framing the Solution

Framing the SOLUTION

Forming the Trust team

- It must be a **priority** – top down
  - Buy-in is guaranteed if it's on everyone's radar
- Get **help** from internal teams
  - We didn't want do this in a vacuum
    - Legal
    - Policy
    - Product
    - Engineering

Framing the SOLUTION

Trust Team Formation

- Shared responsibility
  - Everyone on the team had some level of responsibility towards the project's success
    - Data validators
    - Documenting
    - Certifying
- Branding
  - The Trust team sounds cool and means more swag

Framing the SOLUTION

Trust Team

- Shared planning and alignment on timing
  - Everyone had to align on priority order
  - Everyone had to be honest about competing projects and goals

RSAConference2020 APJ

A Virtual Learning Experience

Part 5: Lessons and Learnings

What is HARD and what works

Lessons and Learnings

Lessons

- Time! This took a lot of time the first go around.
- Scope differs according to Stakeholders
  - Legal had a different idea of success than Product Security
  - How do you compromise and support everyone's motivation?
- Everyone has a different idea of PII and what that means

Lessons and Learnings

Learnings

- This will spur cleaning up of legacy – naturally!
  - People don't want to waste time documenting systems and tools not in use!
- Differing teams on the same product have to communicate directly
- Documentation
  - Data Flow diagrams end-to-end
  - Helpful for Incidents! Now everyone knows where different types of data are and how they connect

RSAConference2020 APJ

A Virtual Learning Experience

Part 6: Your Turn!

APPLY IT

Your Turn! – APPLY IT

- Next week you should:
  - Ask the questions – determine importance within your Products and Org
  - Make Friends*!!!*
    - Legal
    - Engineering
    - Product
    - Policy

APPLY IT

- In the first three months following this presentation you should:
  - Pick a pilot product
  - Grab a excel sheet or google sheet and start documenting identifying data points collected currently in product
  - Identify who on the product can help verify and add to your findings
  - Identify who on the engineering side can verify and add to your findings
  - Identify third party vendors used

APPLY IT

- In the six months following this presentation you should:
  - Identify third party vendors that contain identifying information
  - Work with engineering to draw data flow diagrams
  - Work to document how access to each system works
    - MFA
    - SSO
    - SSH