GDPR,CCPA,... Privacy Data Protection Regulations - A Technologist's Perspective

Central Ohio InfoSec Conference, May 2019, Columbus Ohio

by

Hemant Sawant

hsawant@gmail.com

G-C-Privacy Data Protection: Agenda

- Who (am I)
- Who (this is applicable to)
- Why
- What
- When / Where
- How – opportunity
- How - strategies
- Takeaways

G-C-Privacy Data Protection: whoaml

- Disclaimer: I am NOT a lawyer
- Technical Manager with couple decades with Fortune 100 companies in Financial Services
- Extensive experience with making software compliant for InfoSec, cyber security, PCI, FFIEC, ...
- Strong interest in and practitioner of
  - Cyber security, Data Protection, Consumer Privacy
  - Application Architecture, Data Architecture, Management,
  - Cryptography – custom development of 3-layer security for E-bills
- Contact
  - hsawant@gmail.com
  - https://www.linkedin.com/in/hemantvsawant
  - @hsawant (not regular on Twitter, so prefer DMs)
- This deck on github: https://github.com/HemantSawant/Presentations

G-C-Privacy Data Protection: who this is applicable to...

- Any company that collects and stores customer information
  - GDPR – European Union resident, visitors included
  - CCPA - California Resident, includes employees
- Common (potentially misconstrued) exclusion – surprise!!!
  - B2B companies
  - Industrial manufacturers
  - Service Providers – think again about who your customers are (people)
- Private Customer Information – even more surprises, for example:
  - IP address
  - MAC Address
  - Images
  - Anything that can be used to directly or indirectly identify a person or household

G-C-Privacy Data Protection: Agenda

- Who
- **Why**
- What
- When / Where
- How – opportunity
- How - strategies
- Takeaways

G-C-Privacy Data Protection: Why

- 2018 was the year of privacy (some claim, the demise of it...)
  - Big Privacy Data Breaches
    - US – Mariott among many biz, Facebook every other week
    - International – India – Aadhaar ID cards including biometrics
- Led to these kind of quotes
  - Trust is dead (but trust is the only real foundation for action)
  - Surveillance Capitalism (term coined by a Harvard researcher Shoshana Zuboff)
  - If they really want and try they can get to your private data, whoever you are.
- Examples from consumer space
- Examples from corporate space

G-C-Privacy Data Protection: Why

- US is the most business innovation friendly in the world – that does not mean we need to remain "The Wild West"
- Europe is known to take the hard choices in regulation first in the world
- US follows, with California leading the way
- Jury is still out whether this kind of regulation is right and enough
- Everyone agrees we do need some type of regulation
- At least two CEOs from FANGAM (the tech giants) have concrete Proposals
- Federal level regulation makes more sense and probably 5-10 years out

G-C-Privacy Data Protection: Agenda

- Who
- Why
- **What**
- When / Where
- How – opportunity
- How - strategies
- Takeaways

G-C-Privacy Data Protection: What

- EU's General Data Protection Regulation (GDPR)
  - Right to request, correct, control processing, erasure of personal data
  - Report breach within 72 hours
  - Respond to customer request within 30 days
  - Max fine per infraction - 4% of annual global sales
- California Consumer Privacy Act (CCPA)
  - Considered GDPR+ includes employees
  - Jan 2020 enforcement launch
  - Any company with customers or employees in California
- Other states in the US – 30+ under way, Ohio has a different take
- Other countries in the world – Argentina, Canada, Iceland, Israel, Malaysia, New Zealand, Switzerland, Uruguay, ...

G-C-Privacy Data Protection: What – GDPR details

- Consumer Privacy Rights
  - Right to reuest (all data stored by a company about me) - 30 day turn-around
  - Right to rectification (corretion) and erasure (of data a company has about me)
  - Right to restriction of processing, or, object to processing of personal data
  - Right to data portability
- Max fines – 4% of global sales, 50,000 euros for smaller companies
- Data Protection Officer – new C-level officer with accountability
- Breach reporting – 72 hours to report to regulators and local law enforcement
- First fines issued by France to Google – 50 million euros for lack of proper user consent in android services opt-in and onboarding

G-C-Privacy Data Protection: What – CCPA details

- Provides California consumers with privacy rights
  - Right to know which personal information (PI) is collected
  - Whether PI is sold or disclosed and to whom
  - Say no to sale of PI
  - Access to their PI collected
  - Same price and access even if / after the above rights are exercised
- Applies to any company doing business in, or with employees in CA if
  - 25 million in annual revenue, OR
  - Buy/receive/sell/share PI of 50,000 or more consumers/households/devices, OR
  - Derive 50% or more of their revenue from selling PI of consumers

G-C-Privacy Data Protection: What – GDPR vs CCPA

	GDPR	***CCPA***
Enforced by	EU countries regulators	CA Attorney General
Enforced Since	May 2018	January 2020
Fines	Very big for big companies	Smaller, higher for intentional
Applies To	Companies with EU residents	Do biz or employees in CA
Breach Reporting	72 hour window	Not specified
Customer Request	30 day turn-around	30 day turn-around
Peculiar Coverage	IP address as PI DPO – new C-level officer	Any ID for consumer/household Link for "Do Not Sell My Info"

G-C-Privacy Data Protection: What – GDPR vs CCPA vs other states

- 31 states have some type of privacy data protection legislation under way
- Ohio Data Protection Act – ODPA – a different take by affirmative defence
  - Tries to promote data protection practices by companies. Those who bring up their cyber security practices to industry standard framework will be protected against tort claims from data breach lawsuits.
- Texas – very similar to CCPA, 2 bills, yet to pass and become law
- Vermont – specifically targets Data Brokers, makes them register annually, data security and fraudulent collection prevention, free credit freezes
- Colorado – lightweight compared to GDPR and CCPA, 30 day window for breach notification
- Massachusettes – lightweight, enryption and employee training, notify consumers about data breach
- Illinois – decade old Biometric Info Protection Act (BIPA) enforcement and interpretation under challenge/review in IL Supreme Court

G-C-Privacy Data Protection: Agenda

- Who
- Why
- What
- **When / Where**
- How – opportunity
- How - strategies
- Takeaways

G-C-Privacy Data Protection: When - time lines to remember

- GDPR – EU
  - In effect since May 2018, only Google fined so far, no small companies fined yet
  - 72 hour window for breach notification
  - 30 day turn around for customer requests
- CCPA – California
  - In effect from January 2020, AG is expected to act quickly and make examples
  - 30 day compliance window, fine comes after that
  - 30 day turn around for customer requests
- Vermont – targetting Data Brokers
  - In effect from January 2019
  - Has the promise to do the most good for all – EFF approves

G-C-Privacy Data Protection: Agenda

- Who (am I)
- Why
- What
- When / Where
- **How - opportunity**
- How - strategies
- Takeaways

G-C-Privacy Data Protection: How – the opportunity

- Like any other regulation, there is need for IT systems
- For GDPR alone:
  - To track collected data, protect it, and erase it for sure, we will need sophisticated tools
  - To track requests, complaints, we will need new work flow software
  - Incident response has new requirements
- For CCPA, let's add:
  - HR systems has new requirements
  - The state of CA has an economy ranked #5 in the world, ahead of UK
- Any new IT systems/apps will need to be protected with GRC items

G-C-Privacy Data Protection: How – the opportunity – projected GDPR Opportunity

- Very Conservative assumptions
  - 10,000 companies that are the potential targets – real number is much higher
  - Fines - Max: 4% of global sales / Min: 50,000 euros – per infraction
  - Average Exposure – 100,000 euros / year / company
- Assume willingness to spend half of the potential exposure
- Total Market Size comes to 10,000 x (100,000 / 2) = 500,000,000 euros
- Of course the above will be split among – legal support, GRC / InfoSec, App Dev or Buys from Vendors
- Neary a Y2K size opportunity, and just like Y2K it could grow bigger

G-C-Privacy Data Protection: Agenda

- Who
- Why
- What
- When / Where
- How – opportunity
- **How - strategies**
- Takeaways

G-C-Privacy Data Protection: How – the strategies

- Low hanging fruit – your state level regulations
- Lowest Common denominator for all national and international laws
- Train the leadership – make them "get it" about the exposure
- Make the communications team aware
- Get the InfoSec and GRC teams start on the plans

G-C-Privacy Data Protection: Agenda

- Who
- Why
- What
- When / Where
- How – opportunity
- How - strategies
- **Takeaways**

G-C-Privacy Data Protection: Takeaways

- GDPR, CCPA, International, State-level – know your total exposure
- Know your start dates for exposure – feeds into planning for the Program
- Better still, find the Lowest Common Denominator that's most effective
- Lawyers can and do help, but find the right ones, start with your in-house counsel getting up to speed on these laws and regulations
- Impacted Areas
  - App Dev
  - Data Architecture
  - InfoSec / GRC
  - Incident Response

G-C-Privacy Data Protection: Takeaways – a different take

- Identify the real business impact and usage for your company, asking
  - Why do we really need consumer privacy data ?
  - What do we actually use PI for ?
  - Can we make PI protection a business advantage ?
  - Can we make privacy a differentiating feature of our products/services ?
- Consumer Privacy as a business advantage
  - Tech giants are already taking steps in this direction – FANGAM
  - Many consumers are ready to "pay premium for privacy" – e.g. paid webmail instead of gmail/hotmail, consumer and family VPN solutions
  - Balance convenience and security – transparancy to customers always welcome
- At a Bare Minimum – guarantee no sale/release of PI outside

G-C-Privacy Data Protection: Wrap-up

- Who
- Why
- What
- When / Where
- How – opportunity
- How - strategies
- Takeaways

Thank you !

Questions?

- Slides on Github -- https://github.com/HemantSawant/Presentations
- https://www.linkedin.com/in/hemantvsawant
- @hsawant on Twitter (not regular, use DM)
- hsawant@gmail.com