Data Privacy Update

BKD CYBER

Everyone needs a trusted advisor. Who's yours?

Presenter

Rex Johnson, CISSPP, CISA, CIPT, PMP, PCIP, QSA

Director | IT Risk Services | BKD Cyber

- Over 25 years experience
- Cybersecurity governance & technical assessments
- Compliance (FFIEC, PCI, NIST, ISO)
- Help companies build or enhance cybersecurity programs
- Information & Operational Technology environments
- Retired Army Lieutenant Colonel

BKD CYBER

GDPR Recap

- General Data Protection Regulation (GDPR)
- Replaces the European Data Protection Directive, which was created in 1995
- Impacts organizations that collect & process personal data of EU data subjects
- Penalties of up to 20M € ($22.6M) or 4% of organization's annual global turnover, whichever is higher
- Data subjects can claim compensation for damages from breaches to their personal data – which is complaint driven
- Went into effect May 25, 2018

GDPR Data Subject Rights

- **Access to data –** Data subject must have access to the data that is provided to controllers/processors
- **Right to object –** Challenge the legitimacy of collection of certain data
- **Correct errors & omissions –** Has the right to have their data corrected
- **Restrict processing (consent)**
- **Data portability –** Allow data subject to transfer their data to another data controller, *e.g.*, a data subject should be able to transfer his/her personal data/profile from one health care provider to the other
- **Erasure –** Can request their personal data be erased from controller's database

What Has Happened Since…

- The International Association of Privacy Professionals (IAPP) hosted a retrospective panel in London mid-March
- More than 200,000 reported cases in the 31 countries
- Has been praised as a successful breach notification law

Sources:
https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html
https://www.itproportal.com/news/over-59000-data-breaches-reported-in-eu-since-gdpr/
https://www.theregister.co.uk/2019/03/14/more_than_200000_gdpr_cases_in_the_first_year_55m_in_fines/

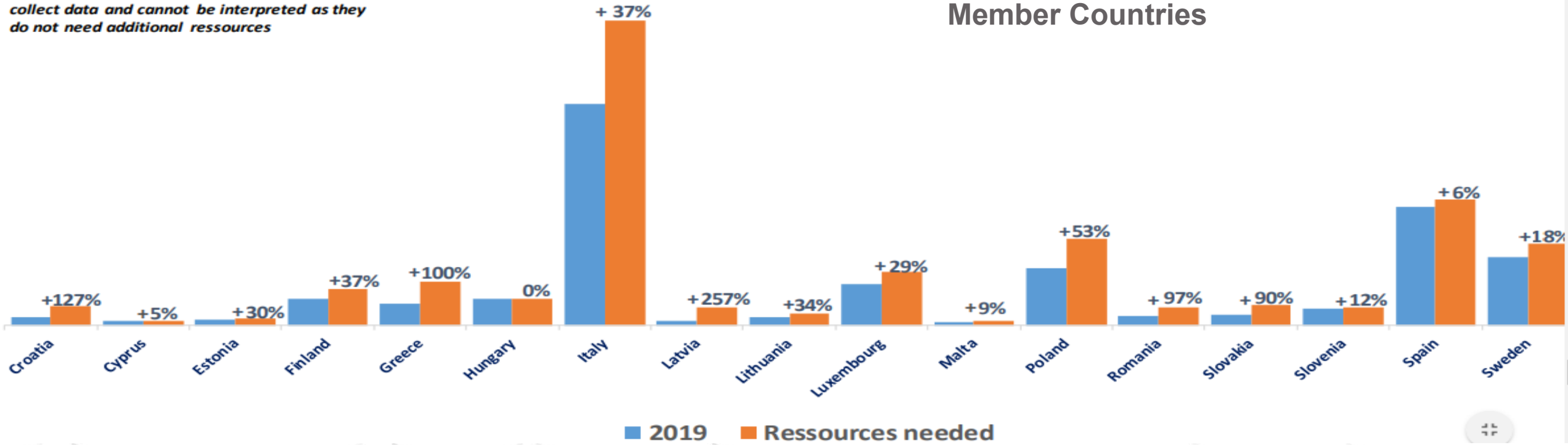
European Data Protection Board

BUDGET

Budget needed vs Budget received

The missing information from some EEA countries SAs is due to the short timeframe to collect data and cannot be interpreted as they do not need additional ressources

European Economic Area (EEA) Member Countries



Source: EDPR Report 2/25/2019

BKD CYBER

Takeaways from EDPR Report

- GDPR enforcement led to extra workloads, additional time dealing with cases & has an impact on the budget of the regulators
- Still trying to figure out **One-Stop-Shop**. *The handling of cross border cases takes time*
- Supervisory Authorities (SA) believes the workload is manageable for the moment
- Many in the EU want to consider this a transition year

Source: EDPR Report 2/25/2019

Impacts of GDPR

- Developed to strengthen & standardize data privacy protections
- Brought to a global stage the question of individual privacy
- Bringing data breaches more to the forefront than before
- Created reluctance of venture capitalist firms to invest in startups impacted by GDPR
- Created reduction in online ad revenues
- Brought potential slowing of digital transformation

Source: “The First Unintended Consequences of GDPR”, Feb. 2019, https://www.hpe.com/us/en/insights/articles/the-first-unintended-consequences-of-gdpr-1902.html

Polling Question

Which of the following is NOT true regarding GDPR:

a) There have been more than 200k cases in the EU

b) The budget required for each country was greater than what was planned

c) There is significant resistance in the EU over cross-border cooperation

d) It has had an impact on breach notifications

Polling Question

Which of the following is NOT true regarding GDPR:

a) There have been more than 200k cases in the EU

b) The budget required for each country was greater than what was planned

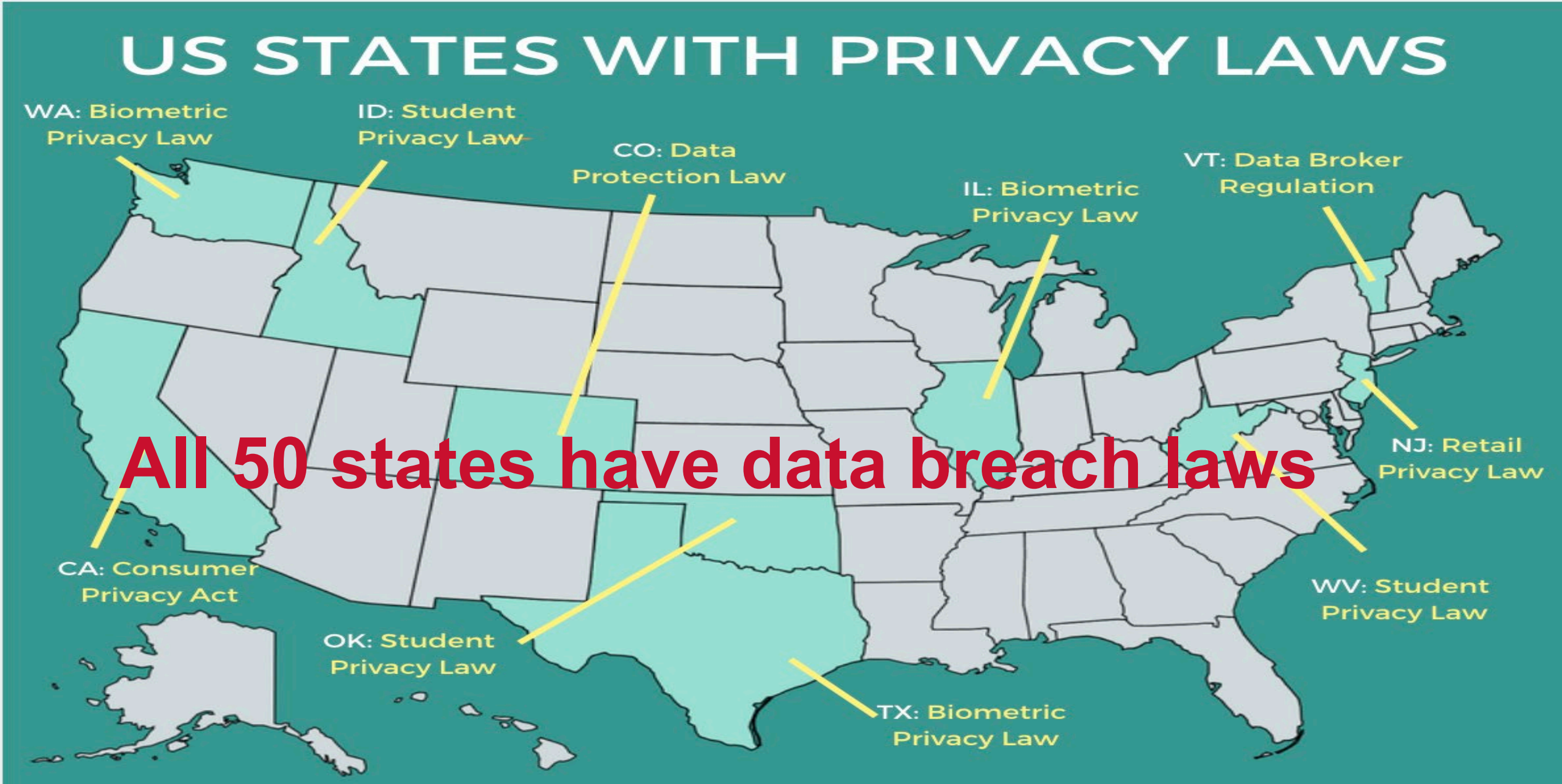
c) There is significant resistance in the EU over cross-border cooperation

d) It has had an impact on breach notifications

Privacy in the U.S.

- U.S. states are becoming more active in data protection & privacy
- At least 25 states have laws that address data security practices of private sector entities
- People are more aware of breaches and their impacts
- All 50 states have enacted data breach notice laws

Sources:
http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx
https://princelobel.com/part-i-domestic-u-s-businesses-can-no-longer-afford-to-ignore-the-gdpr-effect-as-states-change-laws-governing-personal-information/



Colorado House Bill 1128

- Went into effect September 1, 2018
- Requires businesses that maintain personal information on Colorado residents to maintain “reasonable” security practices
  - Appropriately dispose of data
  - Protection of data when transferred to third parties
  - Notification of breaches within 30 days
  - Designation of a responsible individual (DPO)
  - Develop & maintain a DR plan & BCP, tested annually

Source: https://www.americanbanker.com/list/the-states-at-the-forefront-of-consumer-privacy-legislation

Colorado House Bill 1128

- Defines personal information as a combination of a resident's first name or initial & last name with:
  - Social security number
  - Student, military, or passport ID number
  - Driver's license or identification card number
  - Medical information
  - Health insurance identification number
  - Biometric data

http://www.cobizmag.com/Trends/Colorado-Enacts-New-Data-Security-Law--Are-You-in-Compliance/

Kansas

K.S. § 50-6,139b

Applies To: A holder of personal information – a person who, in the ordinary course of business, collects, maintains or possesses, or causes to be collected, maintained or possessed, the personal information of any other person.

Security Measures Required: Implement and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect the personal information from unauthorized access, use, modification or disclosure.

BKD CYBER

Kansas

K.S. § 50-6,139b

Applies To: A holder of personal information – a person who, in the ordinary course of business, collects, maintains or possesses, or causes to be collected, maintained or possessed, the personal information of any other person.

Security Measures Required: Implement and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect the personal information from unauthorized access, use, modification or disclosure.

BKD CYBER

Polling Question

What is true about data privacy in the U.S.?

a) Every state has implemented data privacy laws

b) Breach notification laws are in all 50 states

c) The U.S. has no interest in data privacy & will not impose this

d) All of the above

Polling Question

What is true about data privacy in the U.S.?

a) Every state has implemented data privacy laws

b) Breach notification laws are in all 50 states

c) The U.S. has no interest in data privacy & will not impose this

d) All of the above

California Consumer Privacy Act (CCPA)

- Signed into law June 28, 2018; goes into effect January 1, 2020
- Grants consumers new rights in the collection of personal information
- Allows California employees and customers to see data a company has on them
- Limits selling of personal information

Sources: https://oag.ca.gov/privacy/ccpa
https://www.csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html
https://www.forbes.com/sites/tonymarks/2019/08/01/the-basics-of-the-california-consumer-privacy-act-ccpa-for-the-franchise-industry/

Impacts of the CCPA

- Applies to more than the state of California, & even the U.S.
- Expected to have a global impact
- California is considered to be the fifth largest global economy
  - GDP rose to $2.7 trillion in 2017
  - Surpassed the U.K.
  - 40 million people

Source: https://www.latimes.com/business/la-fi-california-economy-gdp-20180504-story.html

Similarities Between CCPA and GDPR

- Both allow individuals to request the deletion of their personal information
- Provisions that organizations must provide to individuals when collecting or processing their information
- A right for individuals to ask organizations to cease the processing of their information (opt out)
- Right of access to their information

Source: https://iapp.org/resources/article/comparing-privacy-laws-gdpr-v-ccpa/

Similarities Between CCPA and GDPR

- An authority to supervise the application of the law; to include helping organizations understand and comply
- Both provide for potential monetary penalties for non-compliance
- Cause of action to seek damages for violations of privacy laws; to include data breaches

Source: https://iapp.org/resources/article/comparing-privacy-laws-gdpr-v-ccpa/

Differences between CCPA and GDPR

CCPA

- Applies to “for profit” companies
- Annual gross revenues > $25M
- Personal data on at least 50,000 people
- Collect more than half of their revenue from the sale of personal data

GDPR

- Requires a “legal basis” for processing of personal data
- Applies to all organizations

Source: https://iapp.org/resources/article/comparing-privacy-laws-gdpr-v-ccpa/

Who is Considered

Both protect natural persons (individuals) but not legal persons

CCPA

- A **consumer** is a “natural person who is a California Resident”
- Every individual in CA for other than temporary or transitionary purposes
- Every individual domiciled in CA, even if temporarily outside

GDPR

- A **data subject** is an “identified or identifiable natural person”
- Must be living
- Does not cover processing of personal data of deceased persons

Source: https://iapp.org/resources/article/comparing-privacy-laws-gdpr-v-ccpa/

Geography Considered

CCPA

- Unclear if it applies to business established outside of CA if its collects or sells personal information while conducting business in CA
- What does conducting business in CA mean?

GDPR

- Any organization that offers goods, services, or monitors behavior of persons in the EU
- Does not have to be physically present in the EU

Both are not applicable in law enforcement and national security

Source: https://iapp.org/resources/article/comparing-privacy-laws-gdpr-v-ccpa/

Other Considerations

CCPA

- Collecting information is considered:
  - Buying
  - Renting
  - Gathering
  - Obtaining
  - Receiving

GDPR

- Processing is any operation on personal data:
  - Collection
  - Recording
  - Storage
  - Use
  - Disclosure

Source: https://iapp.org/resources/article/comparing-privacy-laws-gdpr-v-ccpa/

Exclusions

CCPA

- Excludes:
  - Medical and protected health information
  - Information collected as part of clinical trials
  - GLBA
  - Driver's Privacy Protection Act
  - Publicly available personal information that is lawfully available

GDPR

- Does not exclude specific categories of data from its scope

Source: https://iapp.org/resources/article/comparing-privacy-laws-gdpr-v-ccpa/

Polling Question

What is a key difference between CCPA and GDPR

a) GDPR only applies to “for profit” business

b) The CCPA does not allow for exclusions

c) The CCPA applies to the selling of data

d) The GDPR does not allow one to “opt out”

Polling Question

What is a key difference between CCPA and GDPR

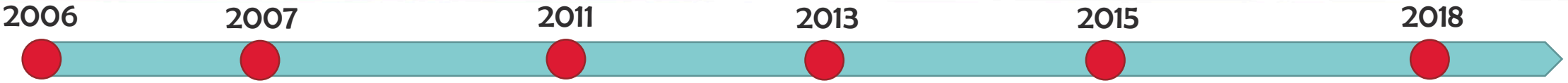
a) GDPR only applies to “for profit” business

b) The CCPA does not allow for exclusions

c) The CCPA applies to the selling of data

d) The GDPR does not allow one to “opt out”

Case Study: Facebook & Privacy



2006 — FB News Feed

Not all users happy with details of personal life being blasted into daily feeds

2007 — Beacon, Ad Privacy

Purchase notifications shared without consent.
FB provided Opt-Out, also talking with FTC on online privacy & advertising

2011 — FTC Settlement

Third-party apps had access to all personal data of users. FB agrees to undergo biannual independent privacy evaluation

2013 — Facebook Bug

White Hat hacker found bug that exposed email & phone numbers of 6M users to anyone who had some connection to the person

2015 — App Restriction

FB cut off apps from taking all data & limited access of developers.
Did not stop previously downloaded data.
Cambridge Analytica ban

2018 — GDPR, Belgian, & Data Theft

FB released privacy principles to users on how to control their data.
Belgian court ordered them to stop collecting data from its citizens & delete existing data.
FB faced pressure on massive data theft.
Developing tool for users to see what apps have access to their data

https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651

How to Prepare for Privacy Laws

- Establish privacy policies & procedures
  - Data classification
  - Data disposal
  - Data privacy
  - Data storage
- Identify personal data types & digital data types with your organization
- Understand IT systems, files & databases that process & store personal information
- Map personal data to the business functions which collect, process & store
- Dedicate a Data Protection Office (DPO)

Online Data Collection

- Include description of what the user is signing up for
- Ensure all forms & other data collection methods on websites are explicitly opt-in *(Note: A tick-box must not be pre-ticked)*
- Make it easy for users to opt-out or unsubscribe
- Add cookie alert banner
- Update privacy policy/terms & conditions to reference GDPR or relevant privacy terminology

Source: https://www.cmdsonline.com/blog/the-looking-glass/gdpr-us-websites/

Cookies

- Make transparent, providing clear & specific information about data types & purpose
- Appear prior to any processing other than the strictly necessary takes place, also known as “prior consent”
- Position them as an affirmative, positive action
- Document them; securely stored as evidence that consent has been given
- Allow users to withdraw consent whenever they want
- Review & renew them regularly (*the ePrivacy directive suggests once a year*)

http://www.spryideas.com/blog/gdpr-affect-business/

Other Considerations for Privacy

- Develop & annually test the Incident Response plan
- Consider how-to processes & respond to data requests from customers
- What third-party vendors process personal data on behalf of your organization or customers?
- What type of data transfer agreements are required?

Polling Question

What is a core element of data privacy?

a) Giving a user the right to know how information is being used

b) The ability to provide consent (opt-in)

c) Disposal of personal data when no longer needed

d) All of the above

Polling Question

What is a core element of data privacy?

a) Giving a user the right to know how information is being used

b) The ability to provide consent (opt-in)

c) Disposal of personal data when no longer needed

d) All of the above

“You have zero privacy anyway…Get over it.”

- Scott McNealy, former CEO of Sun Microsystems circa 1999

A lot has changed in the past 20 years

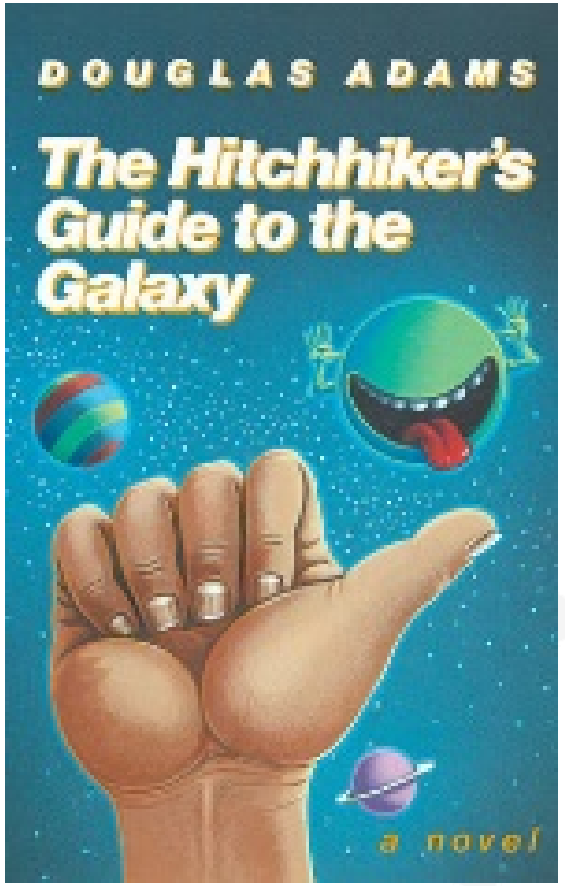
Summary

- Concerns over data privacy are not diminishing
- GDPR has brought this to the forefront
- Breach awareness & notifications are rising
- CCPA will have an impact nationally and globally
- Organizations need to consider how they will address the subject of data privacy

How We React to Change

1. “Anything that is in the world when you’re born is normal and ordinary and is just a natural part of the way the world works.
2. Anything that's invented between when you’re 15 and 35 is new and exciting and revolutionary and you can probably get a career in it.
3. Anything invented after you're 35 is against the natural order of things.”

Douglas Adams, author of *The Hitchhiker’s Guide to the Galaxy*



Source: *The Salmon of Doubt: Hitchhiking the Galaxy One Last Time* (2002)

Questions?

Thank You!

bkd.com | @BKDCyber @RexSecurity

BKDCYBER