PRIVACY ISSUES FOR THE SECURITY PROFESSIONAL

National Cyber Summit

June 5, 2019

PRIVACY COUNSEL LLC

Who: Paige Boshell, Privacy Law Specialist, Fellow of Information Privacy, ANSI-certified: Certified Information Privacy Manager, Certified Information Privacy Professional/ US Law, Certified Information Privacy Professional/European Law, Best Lawyers of America https://www.linkedin.com/in/paige-boshell-76209910/ pboshell@privacycounselllc.com

What: Virtual legal services provider for cyber and privacy law https://privacycounselllc.com @PrivacyCoLLC

Why: Provide commercial clients legal strategies to innovate, protect data, and respond to cyberthreats and privacy vulnerabilities

How: *S*ophisticated legal counsel to clients of a variety of sizes in financial services, fintech, adtech, start-up, big data, healthcare, education, retail, non-profit, construction, and manufacturing, including privacy and cyber compliance, vendor contracting and management, data breach preparedness, response and resiliency, complex tech transactions, delivery of services online and via mobile apps, and emerging tech

No representation is made that the quality of the legal services to be performed is greater than the quality of legal services to be performed by other lawyers. Attorney advertising.

WHAT IS THE PURPOSE OF THIS TALK?

- Impact of various Big Tech privacy scandals
- Secondary data market
- Impact of the EU's General Data Protection Regulation
- Need for consumer engagement

privacy counsel℠

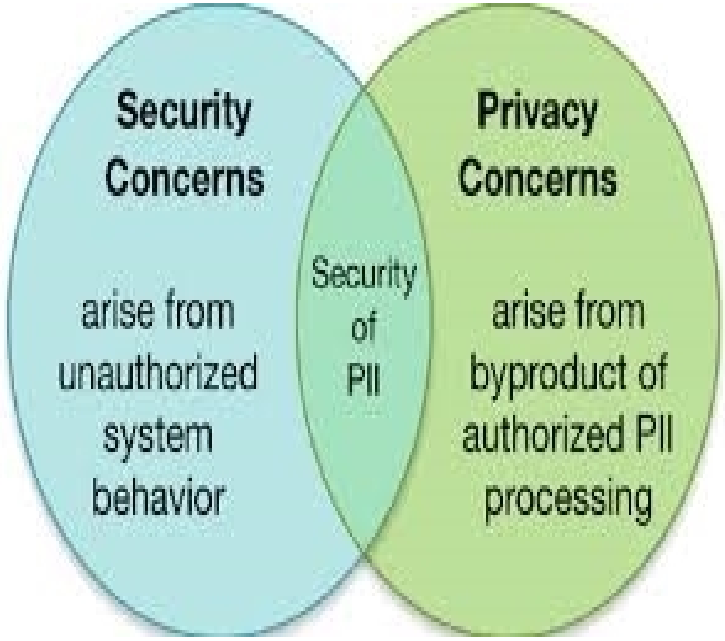
PRIVACY: WHY NOW?

- Scandals and data leaks
- European law and enforcement actions
- Legal uncertainty and lack of privacy standards
- Big data and rapidly evolving tech

= Consumer alarm

privacy counsel℠

PRIVACY & SECURITY FUNCTIONS



- *Data Privacy*: Assignment of value to data and governance designed to ensure that valuable data is collected, accessed, used, disclosed, protected and destroyed legally and fairly. Who? What? Where? Why? How?

- *Data Security*: Procedures and controls intended to protect valuable data and systems, in any form, so that the data's confidentiality, integrity, and availability are maintained.

Privacy breach/breach of trust v. data security breach/cybercrime

FEMA breach

privacy counsel℠

PRIVACY SCANDALS

UBER: 2016

- 57 million users' and drivers' info hacked (DL #s, lax security)
- Third party cloud
- In process of negotiations with FTC
- Paid hackers $100k ransom to destroy data and sign NDAs
- No alleged misuse, info secured, system secured
- Uber disclosure late 2017
- IS success? Privacy failure

PRIVACY SCANDALS

UBER: 2016 - 2018

- 9/18 settlement with AGs of all 50 states and DC- record $148 mil
- Cover up violated state data breach notification laws and constituted UDAP (along with weak security and misrepresentations that Uber protected customer information)
- Lack of security, transparency

privacy counsel℠

PRIVACY SCANDALS

FACEBOOK: 2010- ?

-Disclosure to academic, app consent? collection exceeded scope, 300k consented, 87 million

-NDA with academic who sold to CA

-Lack of monitoring, actual knowledge?

-3 party apps generally

privacy counsel℠

PRIVACY SCANDALS


The New York Times

TECHNOLOGY

Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens

Collection exceeded purpose, use and disclosure exceeded consent, absence of consent or knowledge by most users

Scope of consent: use of info by academic for personality quiz
Type of info: included timeline and PMs
Also collected: user's friends' info
80+ million users

CA: Combined FB data with other data to compile comprehensive profile of each user/voter and sold them to political campaigns – Cruz, Trump, Brexit, 2018 Mexican election
Purpose: influence votes
Data still on open Internet

Follow-up: Many app developers out of business or unresponsive- FB does not know status of data

privacy counsel℠

PRIVACY SCANDALS

A software glitch in the social site gave outside developers potential access to private Google+ profile data between 2015 and March 2018, when internal investigators discovered and fixed the issue, according to the documents and people briefed on the incident. A memo reviewed by the Journal prepared by Google's legal and policy staff and shared with senior executives warned that disclosing the incident would likely trigger "immediate regulatory interest" and invite comparisons to Facebook's leak of user information to data firm Cambridge Analytica.

The internal memo from legal and policy staff says the company has no evidence that any outside developers misused the data but acknowledges it has no way of knowing for sure. The profile data that was exposed included full names, email addresses, birth dates, gender, profile photos, places lived, occupation and relationship status; it didn't include phone numbers, email messages, timeline posts, direct messages or any other type of communication data, one of the people said.

Google+
-user names, emails, birthdates, gender, photos, places lived, occupation, relationship
-exposed to developers by a software "glitch" (API public channel to apps)
-duration: 3 years
-500k+ users affected
-followed by second leak late 2018

privacy counsel℠

PRIVACY SCANDALS

- No evidence of misuse by third parties
- No consumer harm
- Developers and users could not do anything about it
-Could not ID users exposed

Lack of transparency, excessive collection

TECH

Google Exposed User Data, Feared Repercussions of Disclosing to Public

Google opted not to disclose to users its discovery of a bug that gave outside developers access to private data. It found no evidence of misuse.

Google Chief Executive Sundar Pichai was briefed on a plan not to notify users of a software glitch that gave outside developers potential access to private data.

DAVID PAUL MORRIS/BLOOMBERG NEWS

As part of its response to the incident, the Alphabet Inc. GOOGL -2.57% ▼ unit plans to announce a sweeping set of data privacy measures that include permanently shutting down all consumer functionality of Google+, the people said. The move effectively puts the final nail in the coffin of a product that was launched in 2011 to challenge Facebook Inc. FB -0.99% ▼ and is widely seen as one of Google's biggest failures.

- Google+ shuttered
- Continuing privacy audits

privacy counsel℠

PRIVACY SCANDALS

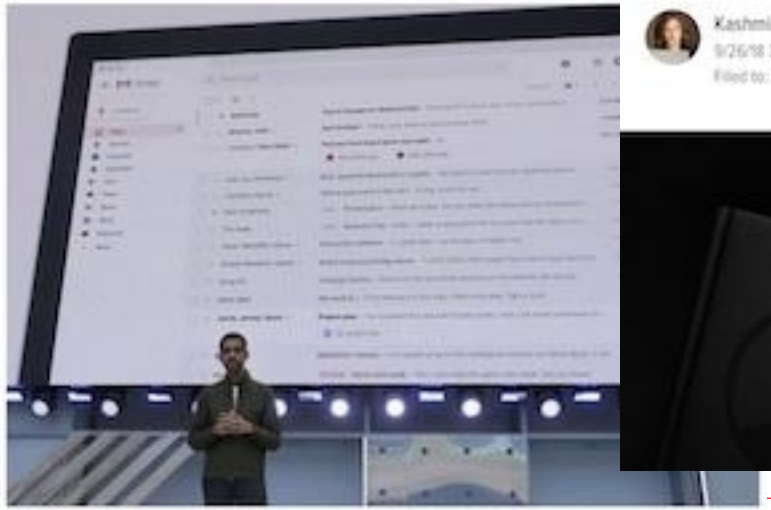
NOW: app developers and behavioral advertising and predictive analysis – *use of data exceeds purpose of collection, lack of transparency*

THE WALL STREET JOURNAL.

POLITICS

Google Says It Continues to Allow Apps to Scan Data From Gmail Accounts

Lawmakers had asked company to explain in wake of WSJ report



Facebook Is Giving Advertisers Access to Your Shadow Contact Information

Kashmir Hill

9/26/18 3:30pm

Filed to: FACEBOOK

The Times of London

@thetimes

People's medical records will be combined with social and smartphone data to predict who will pick up bad habits and stop them getting ill, under radical government proposals

NHS will use phone data to predict threats to your health

Mobile Privacy: What Do Your Apps Know About You?

Just how much personal information are your apps gathering? And do they really need so much?

privacy counsel℠

LOCATION TRACKING IN THE NEWS

Connected Car Technology Can Enable Abusers to Track Their Victims

A growing number of automakers are enabling location tracking in internet-connected cars, a technology that experts say can be misused by abusers to track their victims.

By Tracey Lindeman | Aug 14 2018

android-developers.googleblog.com

Developers Blog

Discontinuing support for Android Nearby Notifications

25 October 2018

Posted by Ritesh Nayak M, Product Manager

AP

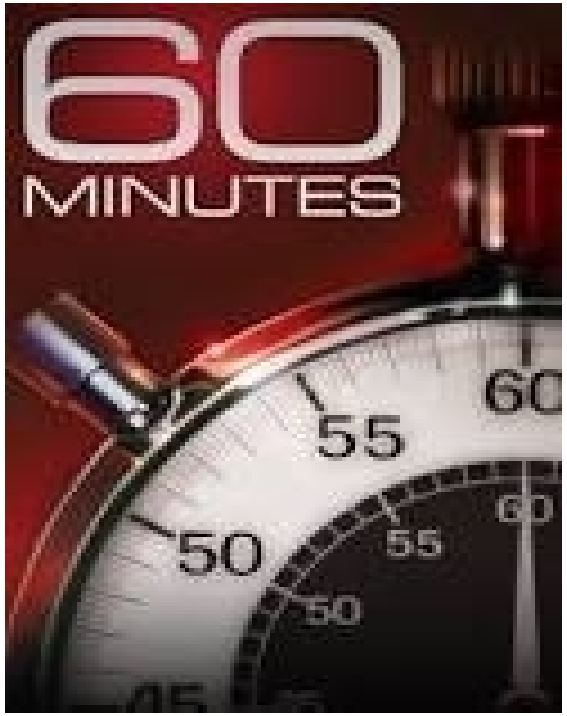
'Location history' off? Google's still tracking you

An AP investigation found that Google saves your location history even if you've paused "Location History" on mobile devices. This map shows where Princeton privacy researcher Gunes Acar travelled over several days, from data saved to his Google account despite "Location History" being off.

Implications of tech not fully-realized

privacy counsel℠

CONSUMER AWARENESS



Lead Story on 60 Minutes

Focus on Big Tech and failure to self-regulate

Senator quotes about need for regulation due to privacy failures

Tim Cook's call for regulation of data "surveillance"

"Americans have no control today about the information that is collected about them every second of their lives."

privacy counsel℠

CONSUMER PERCEPTION

Data breach fatigue v. privacy scandals

Privacy + Security = Safety

Confusion and mistrust breeds anxiety

Who? What? Where? Why? How?

privacy counsel℠

Fair Information Principles/FIPS

Collection limitation
Data quality (relevancy, accuracy)
Purpose specification
Use Limitation
Security safeguards
Openness (transparency)
Individual participation (access, correction)
Accountability

privacy counsel℠

CURRENT US LAWS

NOTICE & CHOICE MODEL

- Current federal laws- HIPAA, GLBA, FCRA, DPPA, FERPA, COPPA, TCPA, CAN-SPAM, VPPA, UDAP/UDAAP, CRA, GINA, ECOA, EEOA, PDA, CALEA, postal regs, FISA, PATRIOT Act, BSA, Fourth Amendment (this list while exhausting is not exhaustive)
- State UDAP, negligence (case law), state data breach laws, IL BIPA
- All 50 states have data breach notification and consumer protection statutes
- State privacy statutes – CA, VT, CO, WA?
- CCPA (California Consumer Privacy Act), SB-327 Information privacy: connected devices

There is no comprehensive nationwide privacy law. Privacy requirements are primarily sectoral. State laws vary among and within states. There is a trend towards a variety of more protective state laws. This patchwork complicates privacy compliance.

privacy counsel℠

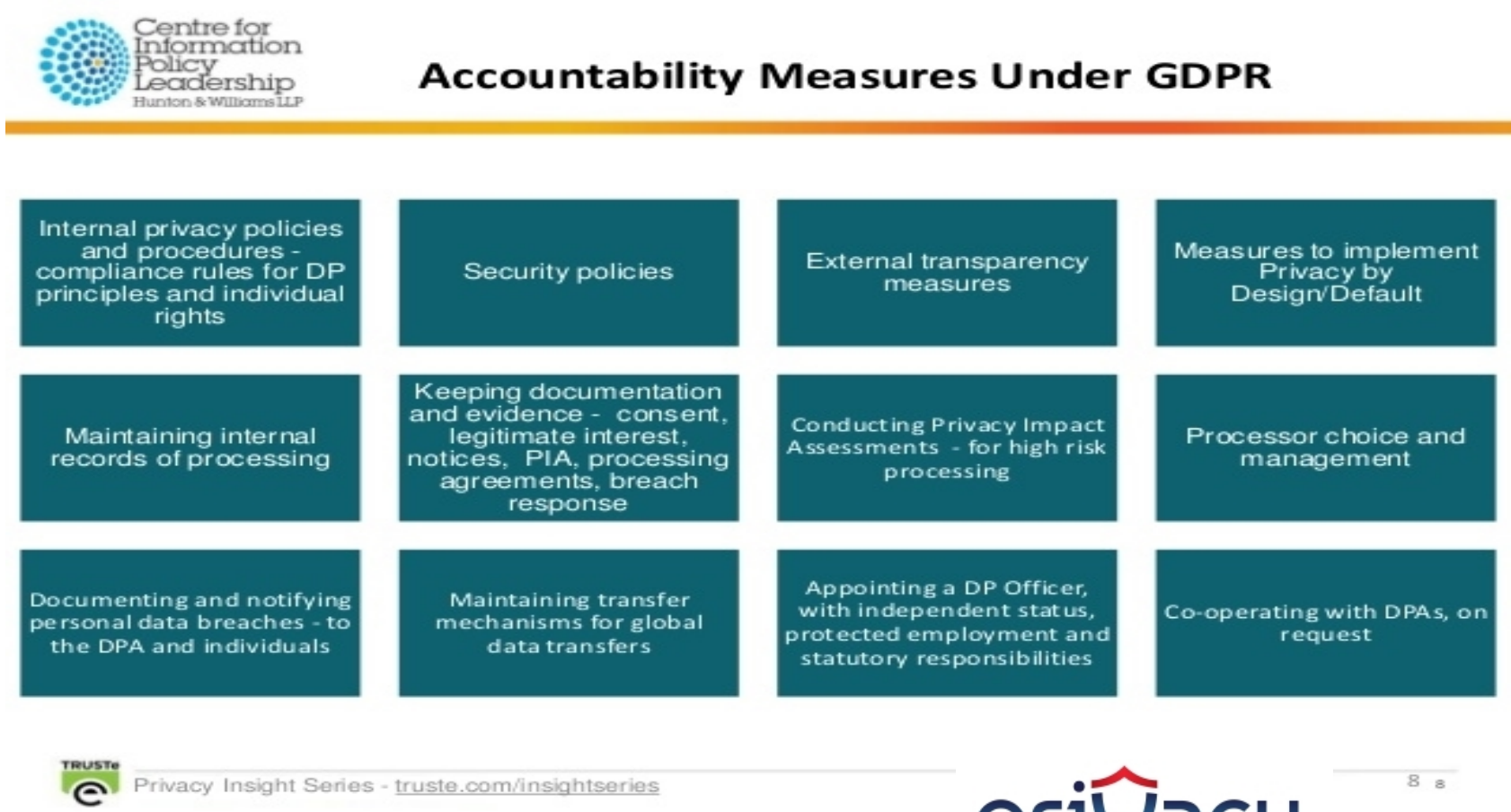
GDPR – EU GENERAL DATA PROTECTION REGULATION

Privacy as human right
Data subject v. data object – ownership

What? Where? Why? How?

FIPs
-Transparency
-Data portability
-Objection to automated decision-making/profiling
-Access
-Correction and erasure
-Restriction of use
-Accountability

*graphic reproduced for educational purposes only



privacy counsel℠

CCPA - CALIFORNIA

What? Where? Why? How?

FIPs

-Transparency
-Use limitation
-Access
-Correction and erasure
-Data portability
-Accountability

*graphic reproduced for educational purposes only

privacy counsel℠

HOW DOES THIS IMPACT BUSINESS?

- Compliance/regulatory risk
- Adverse reputational impact leads to

  increased class action and enforcement risk (Judge in FB data breach case stated that the discovery would be “bone-crushing”)

  decrease in market value

  stifling of innovation and expansion (FB banking)

It’s a matter of trust

privacy counsel℠

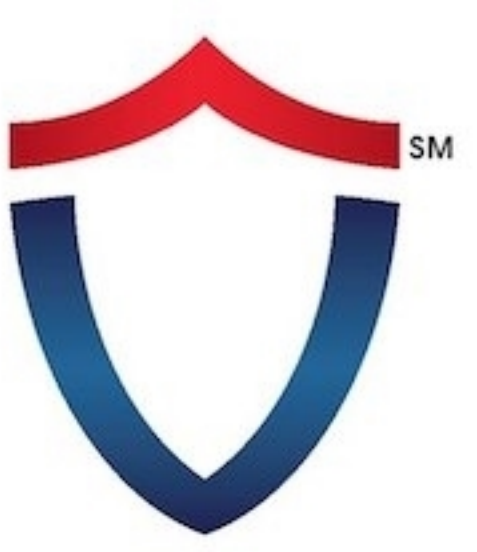
LEGAL DEVELOPMENTS AND UNCERTAINTY

- State
  - Statutes
  - State AG enforcement actions – Uber, FB
  - Class actions
- Federal
  - Obama FIPs, Big Tech baseline with preemption
  - Sectoral
  - FTC/UDAP

Uncertainties in where the law is headed makes privacy compliance difficult.

privacy counsel℠

PRIVACY STANDARDS



- Legal
  - Current domestic law
  - GDPR and other nations
- FIPs, Future of Privacy Forum, International Association of Privacy Professionals, industry groups – DMA, CARU, ABA
- Pending NIST RMF Privacy Framework and NTIA principles – “voluntary tool for organizations to better identify, assess, manage, and communicate about privacy risks so that individuals can enjoy the benefits of innovative technologies with greater confidence and trust.”

privacy counsel℠

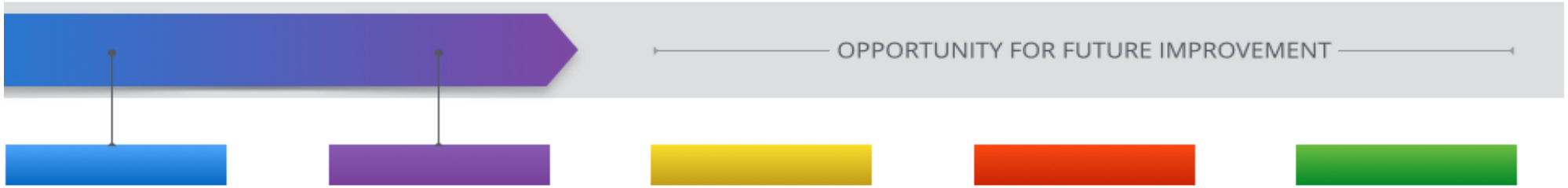
NIST RMF - PRIVACY

- **Why good cybersecurity doesn't solve it all:** While good cybersecurity practices help manage privacy risk by protecting people's information, privacy risks also can arise from how organizations collect, store, use, and share this information to meet their mission or business objective, as well as how individuals interact with products and services.

- **What is the NIST Privacy Framework:**
  - NIST aims to collaboratively develop the Privacy Framework as a voluntary, enterprise-level tool that could provide a catalog of privacy outcomes and approaches to help organizations prioritize strategies that create flexible and effective privacy protection solutions, and enable individuals to enjoy the benefits of innovative technologies with greater confidence and trust.
  - It should assist organizations to better manage privacy risks within their diverse environments rather than prescribing the methods for managing privacy risk.
  - The framework should also be compatible with and support organizations' ability to operate under applicable domestic and international legal or regulatory regimes.

privacy counsel℠

NIST RMF - PRIVACY



IDENTIFY

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

PROTECT

- Access control
- Awareness and training
- Data security
- Information protection and procedures
- Maintenance
- Protective technology

DETECT

- Anomalies and events
- Security continuous monitoring
- Detection process

RESPOND

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

- Recover planning
- Improvements
- Communications

privacy counsel℠

NIST RMF - PRIVACY

- Transparency: Organizations should be transparent about how they collect, use, share, and store users' personal information.
- Control: Users should be able to exercise control over the personal information they provide to organizations.
- Reasonable Minimization: The collection, use, storage and sharing of personal data should be reasonably minimized in a manner proportional to the scope of privacy risks.
- Security. Organizations should employ security safeguards to protect the data that they collect, store, use, or share.
- Access and Correction: Users should be able to reasonably access and correct personal data they have provided.
- Risk Management: Organizations should take steps to manage the risk of disclosure or harmful uses of personal data.
- Accountability: Organizations should be accountable for the use of personal data that has been collected, maintained, or used by its systems.

privacy counsel℠

PRIVACY STANDARDS

Privacy Standards – International Organization for Standardization

- ISO/IEC 29100:2011
  - provides a privacy framework which specifies a common privacy terminology; defines the actors and their roles in processing personally identifiable information (PII); describes privacy safeguarding considerations; and provides references to known privacy principles for information technology.
  - is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.
- Pending
  - new ISO project committee, *Consumer protection: privacy by design for consumer goods and services*
  - “The standard will be of use to those providing digitally connected consumer products, such as home appliances and wearable devices, mobile application developers, online service providers and more.” (IOT)

PRIVACY STANDARDS

Security Standards

- Legal
  - States – laws, AGs
  - Federal - laws, FTC and HHS consent orders
- Standards
  - Industry groups
  - ISACs (Information Sharing and Analysis Centers)

Lack of comprehensive privacy standards results in a lack of clarity in privacy compliance guidance.

privacy counsel℠

RAPIDLY EVOLVING TECH AND COMPLEX USE OF DATA

- Big Data and Big Tech: Martech, Adtech, Edtech, Fintech, Medtech
- AI, blockchain, and augmented reality
- IOT – rise of connected devices
- Geolocation – cell phones, tablets, laptops, cars, anything mobile and connected

Focus: *Consumer experience, innovation, efficiencies of scale*

Current legal and standards framework: *Innovation in tech is outrunning requirements and guidance*

FIPS and Who? What? Where? Why? How?

How do you disclose use and get consent, opt-in, opt-out? Or should we adopt another model?

privacy counsel℠

WHAT'S HERE OR COMING IN PRIVACY

- Greater consumer awareness
- Increased regulation, state AG attention, class action litigation
- More U.S. laws
- Privacy-by-design: Who? What? Where? Why? How? Assess and address risk as process

privacy counsel℠

IT'S AN EXCITING TIME TO WORK IN PRIVACY

- Rapidly developing and deployed tech
- Complex tech and data use
- Business confusion
- Consumer anxiety
- The laws don't fit
- The legal landscape is uncertain
- The privacy standards are not mature

privacy counsel℠

WHAT CAN SECURITY PROFESSIONALS DO?

- Education and training for IS re privacy/educate privacy function re tech and data use
- Data inventory – know the value, sources, access vectors (internal and external), and uses of all data- Who? What? Where? How? Why?
- Consult privacy function whenever there is a proposed new type of data, source, access vector, use or consumer-facing tech, change in Who? What? Where? How? Why?
- Use privacy-by-design/NIST RMF

privacy counsel℠

QUESTIONS?

pboshell@privacycounselllc.com

https://twitter.com/PrivacyCoLLC

https://www.linkedin.com/in/paige-boshell-76209910/

https://privacycounselllc.com

privacy counsel℠