Privacy Law: Global Concepts

What is the Difference Between Privacy and Data Security?

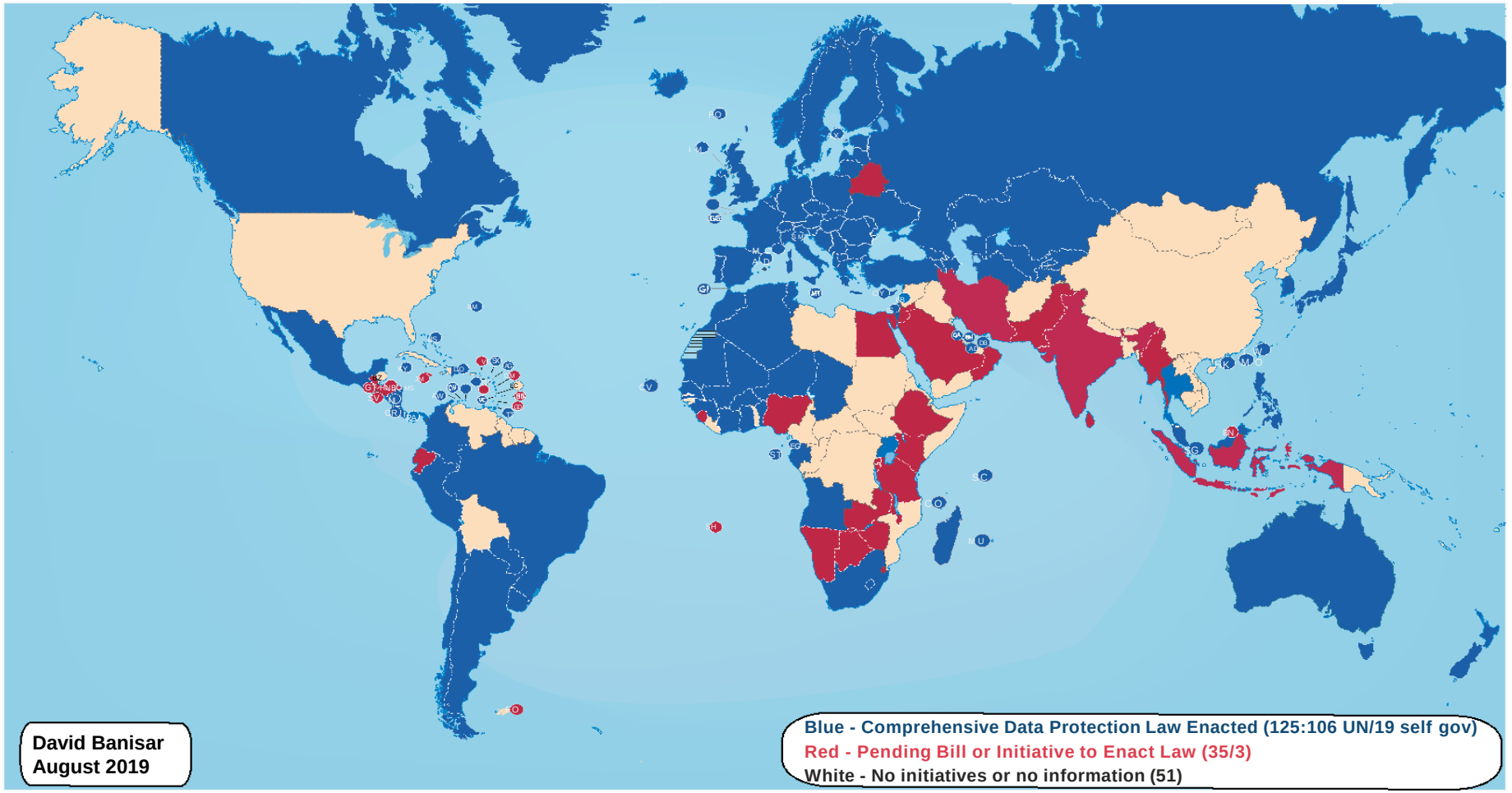
HUNTON ANDREWS KURTH

- Privacy is the appropriate use of personal information as defined by:
  - Laws and regulations
  - Individuals' expectations
- Security is the protection of information and systems
  - CIA (Confidentiality, Availability, Integrity)

Global Legislative Footprint

HUNTON ANDREWS KURTH

National Comprehensive Data Protection/Privacy Laws and Bills 2019



Global Privacy Principles

HUNTON ANDREWS KURTH

Global privacy laws often embed the following data protection accountability principles:

- Lawful, Fair and Transparent Processing
- Collection and Purpose Limitation
- Individual Rights
- Data Integrity
- Data Minimization
- Service Provider Management
- Data Security
- Enforcement and Redress

Differing Approaches in the U.S. and EU

HUNTON ANDREWS KURTH

- U.S. regulation of privacy is a patchwork quilt
  - No overarching federal law
  - Series of subject matter-specific federal laws
  - Hundreds of state laws
  - But change is coming

- The EU regulates data protection comprehensively
  - One data protection law regulating every industry
  - Original Data Protection Directive enacted in 1995
  - General Data Protection Regulation (GDPR) became operative on May 25, 2018

U.S. Privacy Law Update

Major U.S. Federal Privacy Laws

HUNTON ANDREWS KURTH

Sectoral federal approach in the U.S., including:

- **FTC Act**: Consumer protection
- **GLB**: Financial institutions
- **HIPAA**: Health care entities and business associates
- **Fair Credit Reporting Act (FCRA/FACTA/FTC Disposal Rule)**: Consumer reporting agencies and others
- **CAN-SPAM**: Commercial email
- **Video Privacy Protection Act**: Video rental records
- **Driver's Privacy Protection Act**: Department of Motor Vehicles records
- **Telephone Consumer Protection Act**: Telemarketing
- **Children's Online Privacy Protection Act**: Children's data collected online
- **Privacy Act of 1974**: Federal government

State Privacy and Data Security Laws

HUNTON ANDREWS KURTH

- Hundreds of state privacy laws
- Examples:
  - California Consumer Privacy Act of 2018
  - Biometric privacy laws (IL, TX, WA)
  - Website privacy notices (CA, CN)
  - Health privacy laws
  - SSN use restrictions
  - Marketing restrictions (e.g., telemarketing)
  - Restrictions on third-party information sharing for marketing purposes (CA)
  - Child protection registry laws (MI, UT)
  - Radio frequency identification (RFID)
  - Anti-spyware
  - Credit reports
  - Privacy torts
  - Data brokers (VT)
  - Data security and breach notification laws

California Consumer Privacy Act of 2018: Overview

HUNTON ANDREWS KURTH

- The CCPA changes the privacy landscape in the U.S.
  - First general U.S. privacy law
- Grants California "consumers" certain rights over their personal information
  - Right to access
  - Right to delete
  - Right to opt out of sale
- Requires businesses subject to the law to disclose specified, detailed content in the business's privacy policies
- Requires businesses to contractually restrict the activities of service providers that process personal information
- Mandates specific CCPA training of relevant personnel
- Compliance deadline: January 1, 2020
- Enforceable by California Attorney General and limited private right of action

2019 U.S. Legislative Explosion

HUNTON ANDREWS KURTH

State Bills

- Hawaii – SB 418
- Illinois – HB 3358
- Louisiana – HB 465
- Maryland – SB 0613
- Massachusetts – SD 341
- Minnesota – SF 2912
- Nevada – SB 220, Chapter 603A (passed)
- New Jersey – S 2834
- New York – S 224, SB 8641, S5642
- Pennsylvania – HB 1049
- Rhode Island – SO 234
- Texas – HB 4518

Federal Bills

- Privacy Bill of Rights Act (Markey)
- American Data Dissemination Act of 2019 (Rubio)
- Social Media Privacy Protection and Consumer Rights Act (Klobuchar)
- Digital Accountability and Transparency to Advance Privacy Act (Cortez Masto)
- Information Transparency & Personal Data Control Act (Del Bene)
- Online Privacy Act (Eshoo & Lofgren)

Coming:

- Senate Commerce Committee bill
- House Energy & Commerce Committee bill

Private-Sector Bills

- Intel Innovative and Ethical Data Use Act of 2018
- CDT Federal Baseline Privacy Legislation
- ITI Framework to Advance Interoperable Rules on Privacy Act of 2019
- IAF Model Bill
- U.S. Chamber of Commerce Federal Consumer Privacy Act

Principles/ Frameworks

- CIPL: Ten Principles for a Revised US Privacy Framework
- US Chamber of Commerce Principles
- Google Framework for Responsible Data Protection Regulation
- Business Roundtable Framework for Consumer Privacy Legislation
- IA Privacy Principles For A Modern National Regulatory Framework
- BSA Privacy Framework
- ALI Principles of the law, Data Privacy

FTC Authority and Enforcement

HUNTON ANDREWS KURTH

- Section 5 of the Federal Trade Commission Act is the principal U.S. consumer protection law enforced by the FTC
  - Prohibits unfair or deceptive trade practices
- Enforcement
  - Late-1990s: FTC began to use Section 5 authority to examine online privacy issues
  - Early 2000s: FTC's approach began to shift to specific consumer harms
  - Since 2001, the FTC has used its authority to bring numerous cases against businesses that allegedly misused or failed to protect consumers' personal information

EU's General Data Protection Regulation Update

EU General Data Protection Regulation (GDPR): Overview

HUNTON ANDREWS KURTH

- The GDPR became operative on May 25, 2018
- The GDPR modernizes data protection law in the EU
- The jurisdictional reach of the GDPR expands coverage of EU data protection law
- The law imposes new obligations on data controllers and requires statutory compliance by data processors

Key GDPR Themes

HUNTON ANDREWS KURTH

Harmonization

- Harmonized rules, but not fully (e.g. employee data, children's data)
- One Stop Shop: Lead DPA for pan-European matters, in cooperation with other DPAs; Local DPA for local matters and redress for individuals
- Risk-based approach
- Some reduction of administrative burden (no national registration of processing or prior authorization)
- BCRs, seals and certifications

Increased obligations

- DP principles tightened (consent, transparency)
- Privacy Impact Assessment
- Privacy by Design
- Breach notification – to DPAs and individuals
- Direct obligations and liability for processors
- Accountability – Privacy Program
- Internal record of processing
- Data Protection Officer

Strengthened rights of individuals

- Access rights
- Rectification rights
- Right to erasure
- Data portability
- Right not to be subject to automated profiling/right to object

Increased enforcement, fines, liabilities

- Regulatory fines up to 4% of annual worldwide turnover
- Individual action
- Class action
- Criminal sanctions (in national laws)
- Larger role for European Data Protection Board (EDPB)

GDPR: One Year Later

HUNTON ANDREWS KURTH

- GDPR has had a massive impact
  - For both organizations and regulators
  - Significant resources have been invested in compliance
- Emergence of GDPR-inspired laws in important economies
  - GDPR themes have spread beyond Europe
  - Transparency, individual rights/participation, vendor management are no longer just best practices, but instead are legal requirements
  - Compliance on a global scale requires privacy and data security to be woven into the fabric of the organization

GDPR: One Year Later (continued)

HUNTON ANDREWS KURTH

- 200,000 cases received by EU Data Protection Authorities
- 64,000 data breach notifications
- 500,000 organizations with registered Data Protection Officers
- Average of $3 million spent to comply with the GDPR

GDPR Enforcement Actions

HUNTON ANDREWS KURTH

- **Google**: French DPA (CNIL) imposed a fine of €50 million in connection with alleged consent issues in the context of targeted advertising on the Android platform
  - CNIL alleged:
    - Google failed to provide adequate notice in an easily accessible form using clear and plain language
    - Consent obtained was invalid due to insufficient notice because Google used pre-checked boxes to obtain consent
  - Google is appealing

GDPR: Enforcement Actions (continued)

HUNTON ANDREWS KURTH

- **British Airways**: UK ICO fined BA $230 million for a data breach that occurred in June 2018 when traffic to BA's website was directed to a fraudulent site
  - 500,000 customers were affected
  - Payment card data, travel bookings, names, addresses and log-in details were harvested
  - ICO blamed the incident on poor security
- **Marriott**: UK ICO imposed a $124 million fine for cyber incident involving personal data of 340 million guest records
  - Vulnerability began in 2014

Update on Other Global Privacy and Cybersecurity Laws

Global Update

HUNTON ANDREWS KURTH

- Significant privacy and data security updates in other countries in the past year, largely influenced by the GDPR:
  - Brazil
  - China
  - India
  - Japan
  - Other countries (Chile, Kenya, Thailand, Vietnam)

Privacy Update: Wrap Up

HUNTON ANDREWS KURTH

- Given the patchwork of privacy and data protection laws across the world, businesses increasingly are taking a global approach to managing their privacy program
- Global convergence is necessary in light of the fragmented rules globally
- The U.S. is currently out of step with global privacy laws, and state laws will become increasingly difficult to manage
- Cambridge Analytica created a line in the sand - U.S. privacy law is rapidly evolving and major changes are afoot
- Privacy will be a key issue in the 2020 presidential election

2019 Cybersecurity Update

How are Cybersecurity Incidents Identified?

HUNTON ANDREWS KURTH

41%

of victims were notified by external entity

59%

of victims discovered breach internally

64%

of victims subsequently retargeted

78

Median # of days until adversary presence was discovered on victim network

Source: Mandiant Consulting, M-Trends 2019 Special Report, March 2019

U.S. Data Security Rules

HUNTON ANDREWS KURTH

- **Federal Data Security Requirements**
  - Consumer personal information (FTC)
  - Financial data (Gramm-Leach-Bliley)
  - Health information (HIPAA/HITECH)
  - Cybersecurity risk disclosure (SEC)
  - Cybersecurity information sharing (CISA)
  - Electric and Nuclear Reliability (NERC, DOE, NRC)
  - Telecom and cable customer data (FCC)
- **State Data Security Requirements**
  - Data security laws (CA, CO, MA, NV, NY, OH, OR and progeny)
  - Data breach notification laws (50 states + DC, Guam, PR and USVI)
    - CCPA's new liability scheme for data breaches
  - Financial institution/insurer cyber regulations (e.g., NY, SC, NH, NAIC)
  - Internet of Things law (CA)
  - Biometrics laws (IL, TX, WA)
- **Industry Standards**
  - NIST Cybersecurity Framework
  - Payment Card Industry Data Security Standard (PCI DSS)
  - ISO 27000-series standards
  - CIS's Top 20 Critical Security Controls

Proactive Measures: Preparing for the Worst

HUNTON ANDREWS KURTH

- Identify and classify sensitive data
- Ensure written information security policies are state-of-the-art
- Maintain incident response plan
- Prepare incident response team through tabletop exercises
- Manage vulnerabilities and monitor for threats to products and systems
- Continually audit and assess the status of security measures
- Search the dark web for company data
- Manage vendor, employee and supplier risks
- Train employees and increase cybersecurity awareness
- Evaluate cyber insurance needs

The Final Perspective

HUNTON ANDREWS KURTH

- What can you do?
  - Understand and manage your privacy risk
  - Impose a strong data governance framework
  - Regularly assess information practices, test systems and review policies
  - Focus diligently on data security
  - Proactively monitor the legal climate
  - Be sensitive to individuals' expectations -- and fears