

# **DATA PRIVACY AND CYBERSECURITY LAW**

## **New Developments and Practical Advice**

**SHAREHOLDER**

**NADEEM W. SCHWEN**

**P/** 612.604.6456

**E/** [nschwen@winthrop.com](mailto:nschwen@winthrop.com)

## DATA – THE NEW CURRENCY

---

**“The world’s most valuable resource is no longer oil, but data”**

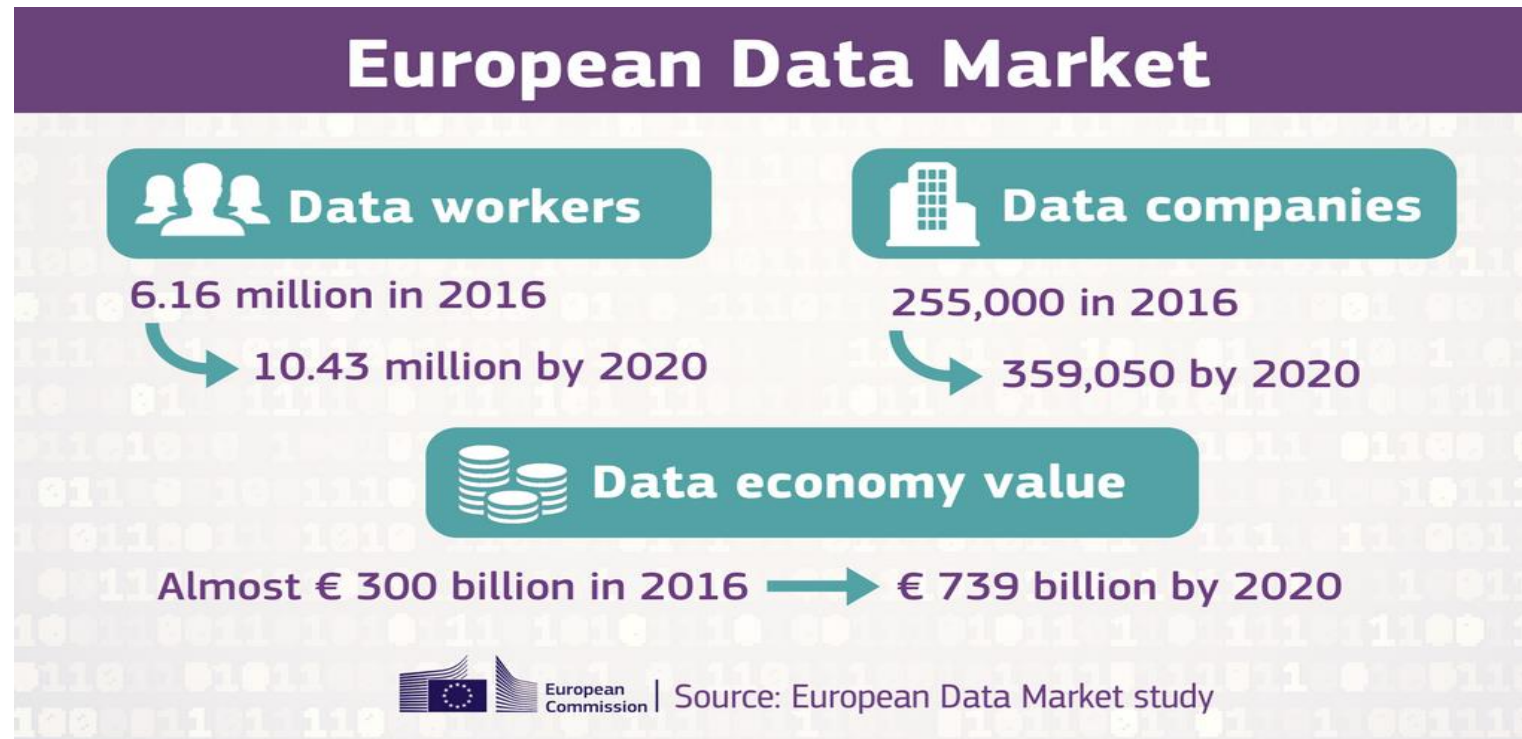
The Economist (May 6, 2017), *available at*

<https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

## DATA – MORE VALUABLE EVERY DAY

---

Value continues to trend upwards as better ways are developed to collect, generate, and monetize data



# HACKS DEMONSTRATE VALUE OF DATA

---



A LexisNexis® Company

Copyright © 2020 Portfolio Media, Inc. All rights reserved.

## Equifax Hack Shows China's Expanding Hunger For Data

---

February 11, 2020

Author: Ben Kochman

**Analytics Are A Source Of  
Competitive Advantage, If  
Used Properly**



Nitin Seth Forbes Councils Member

Forbes Technology Council COUNCIL POST | Paid Program

Innovation

***Marriott Data Breach Is Traced to  
Chinese Hackers as U.S. Readies  
Crackdown on Beijing***

**The New York Times**

## WHY NOW? UNPRECEDENTED VOLUMES OF DATA

---

- > More data is being generated
- > More data is being collected
- > More data is being derived
- > More data is being aggregated
- > More data is being shared



<https://blog.whistic.com/mo-data-mo-problems-6558440d775d>

## THE INTERNET OF THINGS (IOT)

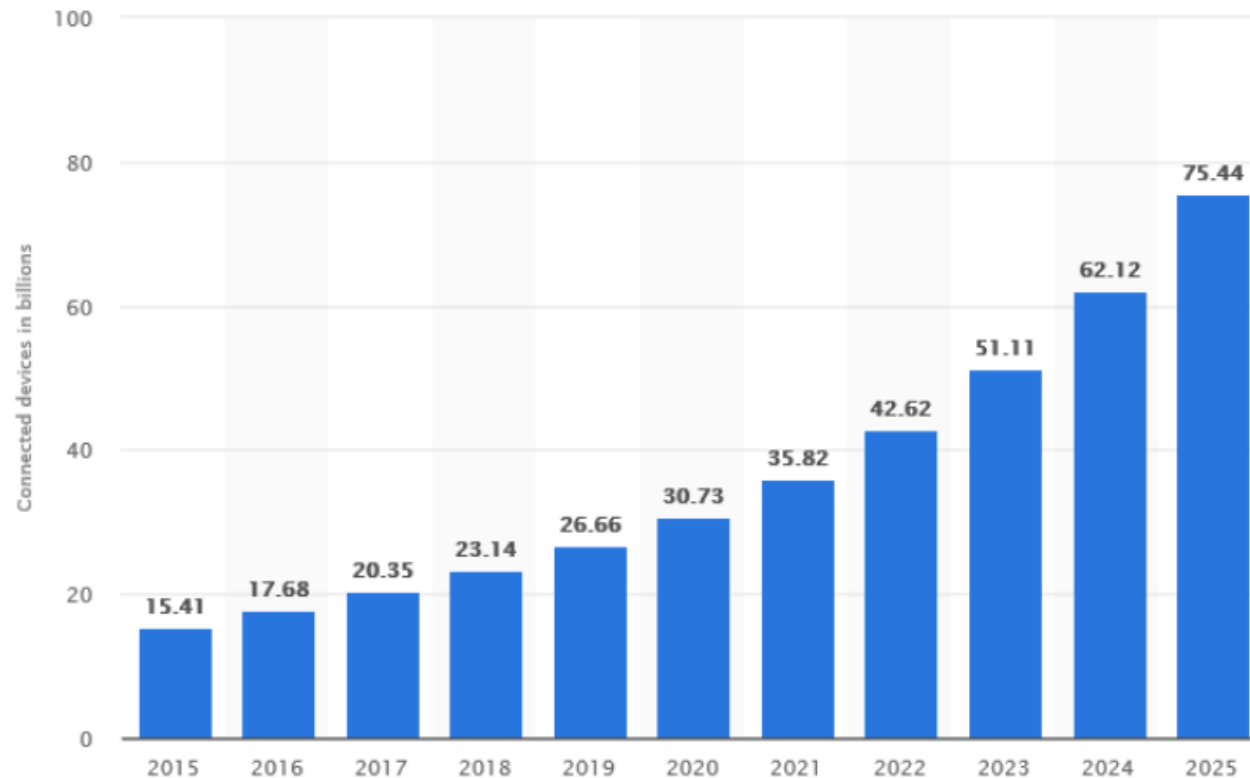
---

- > **Generalized Definition – Internet-connected physical objects embedded with electronics, software, and sensors which enables them to collect, monitor, and exchange data**
- > **Common examples**
  - Phone
  - Amazon Echo/Google Home, Doorbell Cams, Roombas, etc.
- > **More devices connected every day**

# RAPIDLY INCREASING NUMBER OF IOT DEVICES

---

**Internet of Things (IoT) connected devices  
installed base worldwide from 2015 to 2025 (in  
billions)**

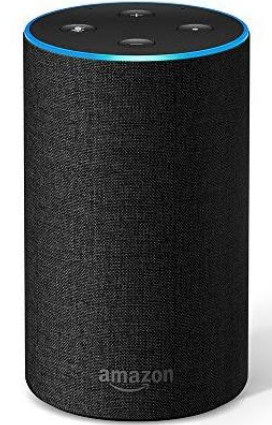


<https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>

## MORE DATA + BETTER ANALYTICAL TOOLS

---

- > Pros - More data can mean:
- Greater customer personalization
  - Better decision-making
  - More insights and discoveries
    - *Caveat: volume of data vs. quality of data*
  - Quicker and more convenient



Pcworld.com



## MORE DATA + WIDESPREAD USE OF TOOLS

---

> Cons - More data can also mean:

- More data to protect
- Greater regulatory risk
- Greater risk with disclosure
- Ethical risks associated with insights and decisions

> E.g.: EU Wants Apple And Google To Remove Privacy-Violating Contact Tracing Apps



Carly Page Contributor

*I cover Tech in Europe, including big tech, PC hardware and telecoms*

**MOTHERBOARD**  
TECH BY VICE

**DMVs Are Selling Your Data to Private Investigators**

# RISKS ASSOCIATED WITH IOT DEVICES

---

- Privacy risks of connected devices
- Cayla: The Kids' Doll Labeled an Espionage Device – Banned in Germany



IoT doll looks like regular doll, but gives no notice that it collects and transmits everything it hears:

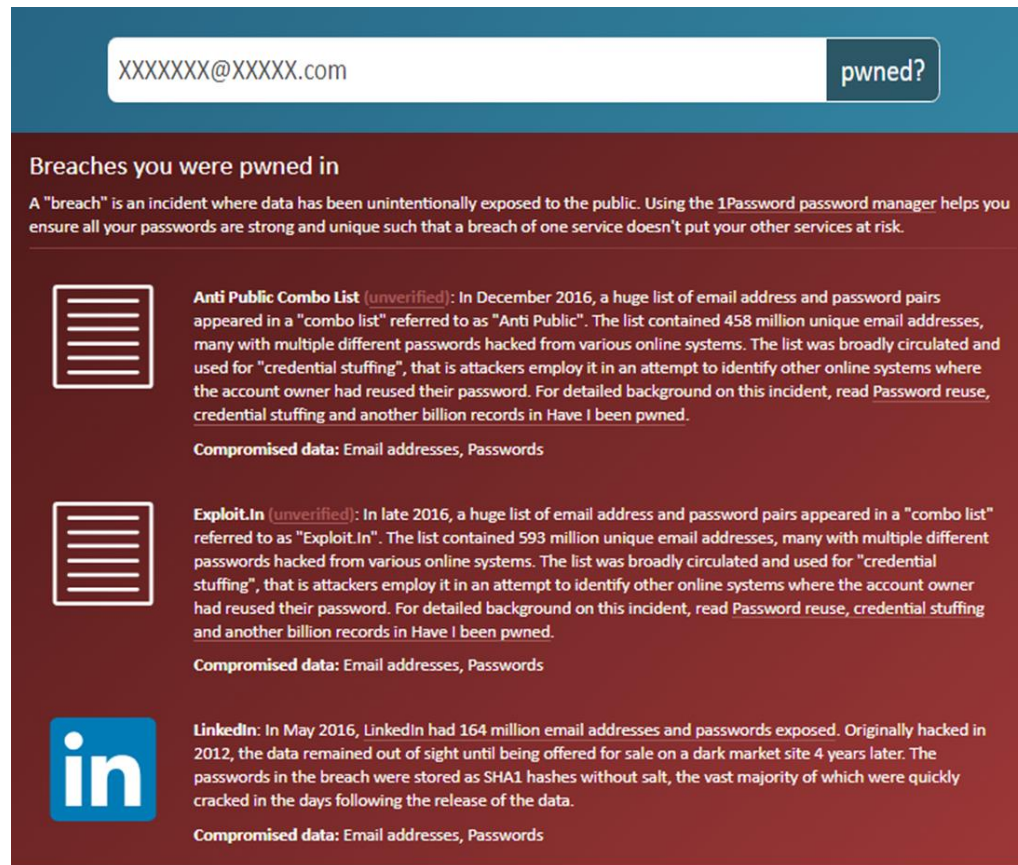
- Asking Cayla "**Can I tell you a secret?**" — brought this reply: "**Sure go ahead; be very quiet, though. I promise not to tell anyone; it's just between you and me because we are friends.**"
- See <https://www.npr.org/sections/thetwo-way/2017/02/17/515775874/banned-in-germany-kids-doll-is-labeled-an-espionage-device>

# RANSOMWARE EXAMPLE - NOTPETYA



# IT CAN AFFECT ANYONE: CHECK YOUR OWN EMAIL ADDRESSES




> [www.haveibeenpwned.com](https://www.haveibeenpwned.com)



XXXXXXX@XXXXX.com pwned?


### Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

- **Anti Public Combo List** (*unverified*): In December 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Anti Public". The list contained 458 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read [Password reuse, credential stuffing and another billion records in Have I been pwned](#).  
**Compromised data:** Email addresses, Passwords
- **Exploit.In** (*unverified*): In late 2016, a huge list of email address and password pairs appeared in a "combo list" referred to as "Exploit.In". The list contained 593 million unique email addresses, many with multiple different passwords hacked from various online systems. The list was broadly circulated and used for "credential stuffing", that is attackers employ it in an attempt to identify other online systems where the account owner had reused their password. For detailed background on this incident, read [Password reuse, credential stuffing and another billion records in Have I been pwned](#).  
**Compromised data:** Email addresses, Passwords
- **LinkedIn:** In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.  
**Compromised data:** Email addresses, Passwords

# THE COST OF A DATA BREACH: 2019 PONEMON INSTITUTE STUDY

---

Global Averages 	Average size of a data breach 25,575 records	
Average total cost of a data breach  \$3.92M	Cost per lost record  \$150	Time to identify and contain a breach  279 days
	Highest country average cost of \$8.19 million  United States	Highest industry average cost of \$6.45 million  Healthcare

Source: Cost of a Data Breach Study, sponsored by IBM, conducted by Ponemon Institute LLC (2019), available at <https://www.ibm.com/security/data-breach>.



# DATA PRIVACY AND CYBERSECURITY: WHAT IS THE DIFFERENCE?

---

## > Data privacy

- More legal: relates to individual rights and control over personal information, and how it is used and shared

## > Cybersecurity

- More technical: relates to how personal information is protected against unauthorized access

## > New laws covering service providers like print industry address both

- E.g., security regulations and privacy requirements

# DATA PRIVACY AND SECURITY LAWS

---

## > Examples:

- Omnibus data privacy laws (CCPA, GDPR, etc.)
- Sectoral data regulations (GLBA, HIPAA, etc.)
- Data broker and other laws restricting sale of data
- Consumer protection regs. (enforcement by FTC and AGs)
- Digital technology laws
  - E.g., AI, IoT, profiling, automatic decision-making, etc.
- Cross-border transfer restrictions
- Data breach notification and data security laws

# PRIVACY AND DATA PROTECTION: LEGAL LANDSCAPE OVERVIEW

---

## > US Privacy Legal Landscape

- Currently a patchwork of **federal laws and regulations** (e.g., CAN-SPAM, HIPAA, GLBA, FERPA, etc.) and **state laws** (e.g., data breach notification laws, minimum security standards etc.)
- Other states updating their laws (AL, AZ, CO, IA, LA, MN, NE, OH, OR, SC, SD, VT, VA, etc.) and more proposals

## > OUS Privacy Legal Landscape

- Dozens of new targeted and omnibus privacy and data protection laws, including the GDPR in the EU, including extraterritorial reach





# WHY SHOULD YOU CARE ABOUT NEW LAWS?

---

## > Fines and lawsuits:

- CCPA – Up to \$7,500 **per incident**,
  - or \$100-\$750 **per consumer affected** (for breaches)
  - Private right of action
- GDPR - Up to 20 Million Euros or 4% of global revenue, **whichever is higher**
  - Private right of action
- FTC and AG increased enforcement and fines
  - E.g., \$5B fine to Facebook



# US PRIVACY LAW RESURGENCE: THE CALIFORNIA CONSUMER PRIVACY ACT

---

- > Originally effective - January 1, 2020, Amended by California Rights Privacy Act effective January 1, 2023
- > New consumer rights to know what personal data is collected about them, access to data, deletion of data, and right to restrict sale of personal data
- > Specific disclosure requirements
- > Penalties with statutory damages and private right of action
- > Proliferation of CCPA class action lawsuits

# THE CALIFORNIA CONSUMER PRIVACY ACT

---

## > **When Does CCPA Apply ?**

- If doing business in California and meets any of following thresholds:
  - Annual gross revenues of \$25 million
  - Buys, sells, receives or shares personal information of more than 50,000 California residents, households or devices annually
  - Derives 50% or more of its annual revenue from selling California residents' personal information

## > **CPRA (CCPA 2.0)**

## CONCEPT OF PERSONAL DATA VS. PII

---

- > Personal data is a **much broader concept** than personally identifiable information, as most in the US understand PII
- > Directly v. indirectly identifiable information
- > Examples of personal data your business may have:
  - Employee data
  - Customer data
  - Potential customer / stranger / device data

## LEGAL LANDSCAPE: WHAT IS PERSONAL INFORMATION?

---

- > **CCPA** – “means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following: (A) Identifiers such as a real name, **alias**, postal address, unique personal identifier, **online identifier**, **Internet Protocol address**, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.

# RESTRICTIONS ON THE SALE OF INFORMATION AND OPT OUT RIGHTS

---

## > CCPA

- Sell means to sell, rent , release, disclose, disseminate, make available, transfer, or communicate orally, in writing or by electronic or other means for monetary or other valuable consideration

## > Nevada Online Privacy Law (effective October 1, 2019)

- “Sale” is the exchange of covered information for monetary consideration and to exchanges where the receiver will license or sell the information to additional persons

# OHIO DATA BREACH NOTIFICATION LAWS

---

- > **Ohio Data Breach Notification Law** (Ohio Rev. Code § 1347.12, 1349.19, 1349.191, 1349.192):
- > A data breach is an unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by an entity and that causes, reasonably is believed to have caused, or is reasonably believed will cause a material risk of identity theft or other fraud to the person or property.
  - Exceptions include good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity

## THE OHIO DATA PROTECTION ACT

---

- > **Purpose:** To incentivize businesses to implement “reasonable” cybersecurity measures
- > **When:** Went into effect November 2, 2018
- > **How:** Provides covered entities with an affirmative defense to data breach claims that allege a business’s failure to implement reasonable information security measures resulted in a data breach.
  - Carrot vs. Stick approach (compare to California’s approach)



## THE OHIO DATA PROTECTION ACT (CONT'D)

---

- > Requires businesses to “create, maintain, and comply with a written cybersecurity program” that “reasonably conforms” to one of several industry-recognized cybersecurity frameworks (e.g., NIST, ISO, HIPAA, GLBA, etc.)
- > Allows covered entities to tailor the scale and scope of the cybersecurity program according to their own business needs, considering the following factors:
  - The size and complexity of the business.
  - The activities of the business.
  - The sensitivity of personal information.
  - The cost and availability of tools to improve cybersecurity.
  - The resources available to the business.

## THE OHIO DATA PROTECTION ACT (CONT'D)

---

- > **Limitations: Only provides affirmative defense to claims that**
  - 1. Arise under tort law**
  - 2. Are brought under Ohio law or in Ohio courts, and**
  - 3. That allege that “failure to implement reasonable information security controls resulted in a data breach concerning personal information or restricted information.”**
- > **Does not apply to statutory or contract-based claims**

## PROPOSED: OHIO PERSONAL PRIVACY ACT (OPPA) – HB 376

---

- > **OPPA: a proposed comprehensive consumer privacy framework in the same vein as similar new privacy laws in California, Colorado, and Virginia**
- > **Provides Ohio consumers with certain data subject rights, including rights for data access and deletion, as well as an opt-out right for the sale of personal data.**
- > **More limited in scope than CCPA**
- > **No private right of action, instead relies on AG enforcement of civil penalties, attorneys' fees, and investigatory costs.**

## **PROPOSED: OHIO PERSONAL PRIVACY ACT (OPPA) – HB 376**

---

- > OPPA would apply to any business that:**
  - Has annual gross revenues generated in Ohio that exceed \$25 million;**
  - During a calendar year, controls or processes personal data of 100,000 or more Ohio consumers;**
  - During a calendar year, derives over 50 percent of its gross revenue from the sale of personal data and processes or controls personal data of 25,000 or more Ohio consumers.**
  
- > Sound familiar?**

## PROPOSED: OHIO PERSONAL PRIVACY ACT (OPPA) – HB 376

---

### > However:

- Introduced in July 2021
- Died in committee
- Still a likely blueprint for future developments in Ohio

# DATA PRIVACY LAWS & REGULATIONS

---

## > Proposed Comprehensive Federal Privacy Laws

- Many congressional proposals
- Countless industry/think tank proposals
- Key issues:
  - Data subject rights, especially right of access
  - Harmonize current patchwork
  - Regulatory authority (e.g., FTC)
  - Privacy right of action
  - Preemption

# AMERICAN DATA PRIVACY AND PROTECTION ACT

---

- > Bipartisan comprehensive federal privacy legislation passed through U.S. congressional committee for first time: American Data Privacy and Protection Act, H.R. 8152
- > U.S. House would not call floor vote over preemption of California Consumer Privacy Act
- > Key provisions of ADPPA
  - Private right of action
  - Nonprofits are covered by law
  - Data minimization requirements
  - Civil rights protections re: algorithms

# **PRIVACY POLICIES:**

## **PRACTICAL ADVICE FOR HANDLING COMMON REAL-WORLD SCENARIOS**



# PRIVACY POLICIES GENERALLY

---

- > Purposes
  - Fulfilling transparency obligations
  - Setting data subject expectations
  - Providing instructions
- > Terminology: Privacy policies vs. privacy statements vs. privacy notices
  - Consider your audience
  - One omnibus policy or multiple policies?
- > Reflective of reality and actual practices

# PRIVACY POLICY ORIGINS IN THE US

---

## > U.S. Privacy Timeline (Federal)

- U.S. Privacy Act of 1974
- Health Insurance Portability and Accountability Act (HIPAA) - 1996
- Gramm-Leach-Bliley Act (GLBA) - 1999
- Children's Online Privacy Protection Action (COPPA) - 2000

# PRIVACY POLICY ORIGINS IN THE US

---

## > U.S. Privacy Timeline (State)

- **California Online Privacy Protection Act (CalOPPA)**
  - Enacted in 2004 (amended 2013)
  - First state law in the US requiring commercial websites and online services to include privacy policy
  - Broad scope - all websites accessible by CA residents
  - For operators of commercial websites that collect PII

# PRIVACY POLICY PURPOSES

---

- > Meeting legal requirements
  - E.g., CCPA/CPRA, GDPR, GLBA, HIPAA, etc.
- > Setting expectations: communicating with customers, employees, B2B partners, visitors about a topic they care about
- > Putting data subjects on notice
- > But remember: also putting the rest of the world on notice about your practices and promises

# PROMISES COUNT

---

> Less Obvious Reason:

**FTC: “Think your company doesn't make any privacy claims? Think again — and reread your privacy policy to make sure you're honoring the promises you've pledged. Consumers care about the privacy of their personal information and savvy businesses understand the importance of being clear about what you do with their data.”**

See <https://www.ftc.gov/business-guidance/privacy-security/consumer-privacy>.

# WHAT HAPPENS WHEN PROMISES ARE BROKEN?

Case 3:23-cv-00460-DMR Document 1 Filed 02/01/23 Page 1 of 27

14 UNITED STATES DISTRICT COURT  
15 NORTHERN DISTRICT OF CALIFORNIA

16  
17 UNITED STATES OF AMERICA,

18 Plaintiff,

19 v.  
20

21 GOODRX HOLDINGS, INC., a corporation,  
22 also d/b/a GoodRx Gold, GoodRx Care,  
23 HeyDoctor, and HeyDoctor by GoodRx,

24 Defendant.  
25  
26

Case No. 23-cv-460

COMPLAINT FOR PERMANENT  
INJUNCTION, CIVIL  
PENALTIES, AND OTHER  
RELIEF

VI. GOODRX'S DECEPTIVE AND UNFAIR BUSINESS PRACTICES

A. Deceptive Statements about Privacy and Data Sharing in

GoodRx's Privacy Policies

2. Promises about Sharing Personal Information

33. GoodRx promised users that it would share users' personal information, such as name, phone number, and email address, with third parties only for the limited purposes of providing services to users or to contact them directly. Between at least October 2017 through December 2019, GoodRx's privacy policy informed users:

By providing your personal information, you agree to let us use such personal information in order to fulfill your requested service and to reach out to you about prescription savings opportunities.

# WHAT HAPPENS WHEN PROMISES ARE BROKEN?

---

- > **FTC complaint:** GoodRX made certain promises to customers in its privacy policy, including about data sharing and advertising
- > **“GoodRx repeatedly violated these promises...by sharing sensitive user information with third-party advertising companies and platforms []like Facebook, Google, and Criteo, and other third parties like Branch and Twilio.”**
- > **GoodRX FTC settlement:** GoodRX to pay \$1.5M fine, bans on marketing using certain PII, and more
- > **Takeaway:** Closely scrutinize all overt or implied promises made in privacy notices provided to consumers (particularly re: advertising and sharing).

# WHAT HAPPENS WHEN PROMISES ARE BROKEN?

---

- > Robinhood Privacy Notice**
  - Stated that Robinhood “take[s] privacy and security seriously” and is “[d]edicated to maintaining the highest security standards”
  - Sued under California’s Consumer Legal Remedies Act following data breach
  - Puffery vs. guarantees
- > Takeaway: Objective statements in privacy notices might be actionable, even without black letter law**



# CROSSHAIRS ON ADVERTISING AND DATA SHARING

---

- > **Facebook:** In 2019, FB received \$5B fine under settlement order for violation of 2012 FTC order.
  - *FTC: “Despite repeated promises to its billions of users worldwide that they could control how their personal information is shared, Facebook undermined consumers’ choices,”*
- > **Google:** In 2019, the French data protection authority (CNIL) fined Google 50 million euros for violating the because Google's privacy policy was not sufficiently transparent, and the company did not provide adequate information to users about how their data was being collected and used for personalized advertising.

# CONTENT: WHAT BELONGS AND DOESN'T BELONG?

---

- > **Mandatory vs. nice-to-have content**
  - **Commonly included but not strictly required info**
- > **Clarity: Clear, simple, and conversational vs. Legalese**
  - **Avoid poor or confusing structure, incoherent sentences, and a general confusing policy**
  - **Consider secondary benefits of clarity – fewer questions!**
- > **Format and structure**
  - **Consider use of technology (within reason)**

# CONTENT: WHAT BELONGS AND DOESN'T BELONG?

---

## > More Don'ts:

- Leftovers from other policies
- Legal definitions and citations (unless required)
- Future processing activities “just in case”
- Conflicting / duplicative language (e.g., multiple GDPR legal bases for processing same data)
- Lies

# METHOD OF DELIVERY AND ACCEPTANCE

---

- > **Delivery options may depend on legal requirements**
  - **E.g., GLBA, breach notification requirements, typeface, language**
- > **Recording customer acknowledgment not generally required**
  - **May be a good idea under some circumstances (retain evidence in a dispute, negating reasonable expectation of privacy)**
- > **Mechanics of providing notice (e.g., part of checkout, etc.)**
- > **Consider accessibility standards for disabled data subjects**

# METHOD OF DELIVERY AND ACCEPTANCE

---

## Don't Hide the Ball:

- > FTC charged Lending Club under GLBA for failing to provide its customers with a clear and conspicuous initial privacy notice before collecting customers' financial data and by failing to deliver the notice in a way that ensured that customers received it.
- > Instead, customers had to click on a link to the Terms of Use policy, and then further find a link to Lending Club's privacy policy.
- > Takeaway: Carefully consider location of link, particularly within apps

<https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf>

# REVIEW AND UPDATING PRIVACY POLICIES

---

- > Problem: What to do when your privacy policy needs to change?
- > What are the reasons for changes and updates?
  - New laws
  - Business growth
  - Acquisition
- > Consider “updateability” when revising
- > Nature of the change (impactful or “material” vs. minor)
  - Consider notice methods
- > Don’t forget changes that implicate “further processing”
  - Consider consent (implied vs express)
- > Effective Date

# REVIEW AND UPDATING PRIVACY POLICIES

---

- > Problem: How often do you need to update your privacy policy?
- > Factors:
  - General legal and regulatory environment
  - Specific applicable legal and regulatory requirements to you
    - GLBA and method of delivery changes
  - Industry (regulated vs. unregulated)
  - Location (California or Alaska?)

# ADDRESSING CHANGES

---

- > “We may change this Privacy Policy at any time. When we do we will post an updated version on this page, unless another type of notice is required by applicable law. By continuing to use our Service or providing us with Personal Information after we have posted an updated Privacy Policy, or notified you by other means, you consent to the revised Privacy Policy.”
  - See <https://openai.com/privacy/>
- > Communicating new policy
  - Don’t forget about non-customers (e.g., website visitors, employees, applicants)
  - Legal requirements may speak directly on this topic (GLBA)
- > Takeaway: Be careful to follow your own previous policy’s promises, take into account applicable regulatory guidance, but don’t make meaningless promises



# SPECIFICITY IN PRIVACY POLICIES

---

- > Issue: How detailed should the policy be?
  - Law may answer question
  - But often subjective
- > *Polar* - Finnish DPA Decision (December 2022):
  - Wearable device company gave privacy notice and sought consent for processing heart rate data and other health information
  - Did not get express consent for “other health information” (e.g., BMI)
  - DPA held statements that “we calculate the calories you burn” not enough

# VARIED AND CONFLICTING REQUIREMENTS

---

- > **Problem:** There are many varied, conflicting and/or mutually exclusive privacy policy legal requirements and legal concerns that may apply
- > **Considerations:**
  - **Omnibus vs. Sectoral privacy policy requirements**
    - E.g., HIPAA & CPRA—consider scope issues
  - **Patchwork of state privacy policy requirements**
    - **Draft MN Consumer Data Privacy Act: “A controller is not required to provide a separate Minnesota-specific privacy notice or section of a privacy notice if the controller's general privacy notice contains all the information required by this section”**

# VARIED AND CONFLICTING REQUIREMENTS

---

- > More considerations:
  - Conflicting national laws on privacy notices
  - Nonlegal country-specific issues
  - Consumer/user reactions to whatever you choose
- > Takeaway: First address hard legal requirements, then consider practical approach to potential conflicting requirements, but don't forget consumer reactions, publicity, and non-legal considerations

# CUSTOMER COMPLAINTS

---

- > Importance of providing clear avenues in policy for resolving customer complaints
- > Responsiveness to complaints matter (for several reasons)
- > Nature of the response matters (redirection vs addressing)
  - Emphasizes importance of complete privacy policy
- > Track complaints using metrics
  - Trace to potential ambiguities in policies
- > Can't please everyone!

# APPROACHES POST-DOBBS

---

- > Heavily depends on industry and location
- > Highly sensitive issue – get C-suite buy-in for policy wording
- > Privacy policy statements on topic (e.g., responding to law enforcement)
- > Anonymization references (careful!)
- > Ideally create strong policy that provides useful reference point

# REGULATORY ENFORCEMENT

---

- > **Scenario: CPPA comes knocking after July 1, 2023**
- > **CPPA enforcement vs. AG enforcement**
  - **Often focused on simple compliance – often a call or a letter first vs. pitchforks**
- > **Remember: CPPA ability to enforce via administrative fine**
  - **Fines go to privacy fund**
  - **Somewhat perverse economic incentive to enforce**
- > **Privacy notice context**
  - **Black letter violations vs. something else**

# REGULATORY ENFORCEMENT

---

- > **CCPA/CPRA: notices of non-compliance from consumers**
  - **Made easier - Consumer Privacy Interactive Tool**
  - **30-day CCPA cure period**
  - **Track**
- > **Takeaway: Pay attention to consumer notices, have a system set up to track them, promptly address/update policy as needed**

# REGULATORY ENFORCEMENT

---

- > **Benefit of foresight: What could you have stated differently in privacy notice?**
- > **Avoiding overstatement and puffery**
- > **Avoid “convenient” vagueness**
  - **Requirement is clear and conspicuous notice regarding selling or sharing personal information**
  - **E.g., Sephora CCPA enforcement for failure to clarify (2022)**
- > **Takeaway: Don’t play the vagueness game**



# REGULATORY ENFORCEMENT

---

- > **Scenario: FTC investigation following data breach**
  - **Investigatory authority**
  - **Enforcement authority**
  - **Litigation authority**
- > **Focused on “unfair or deceptive acts or practices”**
- > **Vast majority of privacy-related FTC actions settle**
- > **Broad deference to FTC interpretation of FTC Act**
- > **Takeaway: Closely consider privacy policy statements**

# EMPLOYEE PRIVACY POLICY ISSUES

---

- > Many subjects to cover in employee privacy notices
  - Monitoring and bossware
  - Potential access to personal data on employee-owned devices
  - BYOD policies for employee-owned devices
  - Surveillance
- > CCPA requires “notice at collection”
  - Don’t forget about possibility of California employees and contractors – particularly since WFH expansion
- > Not just employees - job candidates, contractors too
- > Employee handbook or separate notice?

# EMPLOYEE PRIVACY ISSUES

---

## > Consider:

- Risks of creating expectations of privacy in the workplace
- Employees in different jurisdictions, and perceptions of unfair rights across workforce
- Location, timing, and form of notices

# NEW PRODUCT LAUNCHES AND PRIVACY POLICY

---

- > **Scenario: Wearable device company decides to implement new feature that allows communication between users**
- > **Considerations:**
  - **Separate policy or modify existing policy?**
    - Are new laws implicated?
  - **What other notices might need edits?**
  - **How to address user-to-user communication within policy?**
  - **Consider interplay with opt-in/opt-out**
  - **Address in privacy policy or T&C?**

# THANK YOU!

---

## QUESTIONS?



**SHAREHOLDER**

**NADEEM SCHWEN**

**P/** 612.604.6456

**E/** nschwen@winthrop.com