**LPRO**: LEGISLATIVE POLICY AND RESEARCH OFFICE

# PROTECTING PERSONAL INFORMATION

## ISSUE BRIEF

The collection, storage, sale, and use of personal information has contributed to the current array of services, including transportation, health care, information, small business advertising, convenience, and entertainment services. Most current regulations focus on keeping personal information secure from malicious actors, but privacy advocates warn about the power that even benign actors wield by collecting and analyzing vast amounts of personal information.[1] Regulators worldwide are evaluating how to best protect individual privacy in light of the widespread commodification of personal information.

## PERSONAL INFORMATION

Internet-enabled devices, sometimes called "smart devices," gather and share personal information. Smart devices include mobile phones, tablets, computers, televisions, fitness trackers, and even some common household appliances like refrigerators and thermostats.

These devices collect and share a wide range of personal information, including our browser history, phone and e-mail contacts, location, personal health, and conversations. Manufacturers may provide platforms that facilitate access to this information by applications, or directly share the information gathered by these smart devices with data brokers, entities who purchase and sell personal information. Information sold to a data broker may contain specific personally identifiable and sensitive details. People are often unaware of whether their personal information is sold to a broker, and if so, what information is included.

## CURRENT PROTECTIONS

Regulations at both the state and federal level dictate how personal information may be gathered and used and provide standards for data security.

### Oregon Regulations

***Oregon Consumer Identity Theft Protection Act* (OCITPA)**[2] The OCITPA requires entities that collect, share, and keep personal information to maintain reasonable

[1] Shoshana Zuboff, professor emerita of the Harvard Business School, has coined the term "Surveillance Capitalism" to describe the "unilateral claiming of private experience as free raw material for translation into behavior data…and sold into behavioral futures markets."

[2] Senate Bill 684 (2019) changes the name to the Oregon Consumer Information Protection Act (OCIPA), amends definitions for "covered entity" and "personal information," requires vendors to provide notice of

safeguards to ensure the security, confidentiality, and integrity of personal information. Entities that experience a data breach must notify consumers within 45 days, and consumer reporting agencies must offer services like placing a security freeze on a consumer report free of charge.[3]

***Oregon Student Information Protection Act* (OSIPA)** The OSIPA prohibits online education sites, services, and applications from compiling, sharing, or disclosing K-12 student information for any purpose other than educational purposes.

***Unlawful Trade Practices Act*** Legislation enacted in 2017 establishes that it is an unlawful trade practice for an entity to use, disclose, maintain, delete, or dispose of information in a manner not in accordance with a statement or representation by that entity.[4] Legislation enacted in 2019 requires the manufacturer of a connected device to install reasonable security features to protect information collected, contained, stored, or transmitted by the device from unauthorized access, modification, use, or disclosure.[5] A violation of this requirement is an unlawful trade practice.

**Federal Regulations**

***The Children's Online Privacy Protection Rule* (COPPA)** Administered by the U.S. Federal Trade Commission (FTC) and enforced by both the FTC and state Attorneys General, COPPA imposes requirements on operators of websites or online services directed to, or that have actual knowledge they are collecting the personal data of, children under 13 years of age. Regulated entities must:

- Post a privacy policy on the website;
- Provide notice directly to parents under specified circumstances;
- Obtain verifiable parental consent;
- Allow parents to review personal information collected from their children;
- Allow parents to revoke their consent;
- Delete information collected from children at the request of the parents;
- Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of children's personal information; and,
- Not condition a child's participation in certain activities on collection of more personal information than is reasonably necessary.

Earlier this year, the FTC assessed a $5.7 million fine against karaoke application Musical.ly for collecting personal information from children without parental consent. Enforcement action against YouTube may be forthcoming.

***The Gramm-Leach-Bliley Act* (GLBA)** The GLBA requires companies that offer consumers financial products or services like loans, financial or investment advice, or insurance to explain their information-sharing practices to their customers, safeguard sensitive data, and offer opt-outs in some circumstances. The FTC and other regulatory

specified security breach, and allows parties to assert an affirmative defense by showing compliance with specified federal acts. Senate Bill 684 becomes effective January 1, 2020.

[3] Sections 2 and 4, Chapter 10, Oregon Laws 2018.

[4] House Bill 2090 (2017).

[5] House Bill 2395 (2019) becomes effective January 1, 2020.

entities recently entered into a $575 million settlement with Equifax over allegations that the credit monitoring agency failed to properly secure data in advance of the 2017 data breach that affected 147 million consumers.

***The Health Insurance Portability and Accountability Act* (HIPAA)** Administered by the U.S. Department of Health and Human Services, HIPAA protects the privacy and security of health information held by health care providers, insurers, and other covered entities. HIPAA grants patients the right to examine and obtain a copy of their health records and to request corrections.

## DATA BROKER REGISTRATION

The state of Vermont requires Data Brokers to register with the state. Similar measures were introduced, but not enacted, in California and Illinois.

### Vermont Data Broker Regulations (DBR)

The DBR establishes regulations for data brokers and prohibits the malicious acquisition or use of personal data. For the purposes of the DBR, "data brokers" are entities who knowingly collect and sell the personal information of individuals with whom the business does not have a direct relationship. The DBR requires data brokers to:

- Register annually with the Secretary of State;
- Maintain certain minimum security standards; and,
- Provide specific information on how a consumer can opt-out of the data broker's collection of information or sale of data.

## BIOMETRIC PRIVACY

Three states guard against the unlawful collection and storage of biometric information like facial scans and fingerprints, and several cities have moved to protect biometric privacy by prohibiting the use of facial recognition technology.

### Illinois Biometric Information Privacy Act (BIPA)

The BIPA regulates the collection, possession, sale, and disclosure of biometric information, including a retina scan, fingerprint, voiceprint, or scan of hand or face geometry. Companies must obtain consent for the storage or use of biometric information, destroy biometric identifiers in a timely manner, and securely store biometric identifiers. The BIPA establishes a private right of action for violations, making Illinois a popular forum for class action lawsuits against major technology companies. Texas and Washington also regulate the collection and use of biometric information, but neither state offers a private right of action.

#### Facial Recognition Bans

Several cities now prohibit city agencies from using facial recognition software in public spaces. Statewide regulations on the use of facial recognition have been proposed in Washington and Massachusetts.

## INDIVIDUAL DIGITAL RIGHTS

The European Union (EU) and the state of California have enacted legislation that declares affirmative individual rights regarding personal information, and establishes standards for companies that gather, store, and disseminate personal information.

### General Data Protection Regulation (GDPR)

The GDPR protects the personal data of people residing in the European Union (EU) by establishing individual rights and standards for the collection and use of personal data. The GDPR is administered in each EU nation by a data protection authority (DPA) authorized to investigate data practices and levy fines on public or private entities for violations.

The GDPR establishes principles to guide the use of personal data. Personal data must be:

- Processed lawfully, fairly and in a transparent manner for consumers;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to the explicit purpose;
- Accurate;
- Kept for no longer than necessary;
- Processed in a manner that ensures integrity and confidentiality.

Individuals located in the EU have the right to:

- Information about who is gathering their data, what data is being gathered, and how that data is used;
- Access any of their personal data held by a public or private entity free of charge;
- Rectification of incorrect or incomplete personal data held by a public or private entity;
- Restrict Processing of personal data held by a public or private entity under specified circumstances;
- Erasure of personal data held by a private entity that is no longer needed or used unlawfully;
- Object to the collection, use, and storage of personal data for specified purposes including direct marketing;
- Explanation of how personal data was used in automated processes such as algorithms;
- Data Portability to move personal data from one service to another.

Individuals in the EU can assert these rights by contacting the entity that holds their personal data, filing a complaint with their DPA, or filing a case in court.

### California Consumer Privacy Act of 2018 (CCPA)

The CCPA grants individuals rights with respect to the collection of their personal information. The California Attorney General is currently in the process of adopting rules to establish procedures to facilitate individuals' rights under the CCPA and provide guidance to businesses.

Under the CCPA, Californians have the right to:

- Know what personal information is collected;
- Know whether personal information is sold or disclosed and to whom;
- Say no to the sale of personal information;
- Access their personal information; and,
- Equal service and price, even if they exercise their privacy rights.

## OREGON CONSUMER PRIVACY TASK FORCE

The Oregon Department of Justice is hosting a Consumer Privacy Task Force that includes privacy advocates and industry representatives. Interested parties should contact Cheryl Hiemstra, Assistant Attorney General.