Data Regulations

A Jumble of Regulations

Technology changes and advances at a much faster pace than the law. Technology also seamlessly crosses borders and areas of activity in a way that laws cannot. This makes it challenging to regulate technology. Data privacy, for example, is regulated by a complex and fragmented landscape of laws that can be hard to understand and even harder to comply with.

In this lesson, you'll take a tour of some of the types of regulations that might impact your work.

Laws and Regulations that Impact Data

Laws and regulations are used by governments to control the actions of individuals and organizations. Subtle differences exist between how laws work and how regulations work that aren't important for our purposes. What's important is that both laws and regulations will almost certainly impact the work that you do with data. So, in this lesson, we'll generically refer to both laws and regulations as rules.

Unfortunately, not everyone has agreed on one simple rule for how data can be used. Instead, the rules that dictate how you work with data will vary, depending on the following:

- The source of the data
- The industry that you're working in
- The location of you or your company
- The location of the people that you and your company work with

An exorbitant number of rules impact companies. If you've ever tried to read any sort of legal document, you probably know that they can be convoluted. The good news is that it probably won't be your job to ensure that your company complies exactly with these rules, so you don't need to know every detail.

Note that many companies have an entire department that's devoted to **legal compliance**. This refers to making sure that the company follows all these rules exactly. Smaller companies might outsource this work to a company that specifically handles compliance.

Still, it's important that you have an awareness of the common, basic types of rules and the names of the most important ones. This will help you in two ways. First, it will help you act in accordance with the rules as you work. Second, it will enable you to flag any potential compliance issues that you notice at your company to those who are responsible.

Major Areas of Data Regulation

Most of the important rules for data regulation center around three key concepts: data security, data privacy, and automated decision-making. Let's learn more about each area.

Data Security

Data security rules deal with the ways that data might unintentionally be shared. One way that this occurs is malicious hackers accessing a company's data. An example of this is the famous 2017 Equifax data breach. Any time that you store data about people, you're likely subject to data security rules.

These rules require that companies have certain types of security protections in place. They also usually specify what companies must do if a data security issue occurs and customer data is compromised.

Data Privacy

Data privacy rules deal with the ways that data gets intentionally collected or shared. One way that this occurs is a company building a customer database and then selling it to another company. Any time that you collect or share data about people, you're likely subject to data privacy rules.

These rules typically limit how companies can share customer data with others, which usually entails one or more of the following:

- Limiting how data can be shared
- Requiring consent for data sharing
- Setting standards for transparency so that customers are informed about how their data is shared

Automated Decision-Making

Automated decision-making rules deal with algorithms making decisions that impact people. An example is a product that automatically determines if a person is likely to commit a criminal offense. Any time that you use an algorithm to make a decision, you might be subject to automated decision-making rules.

Automated decision-making rules have been established more recently than data security and data privacy rules. They typically specify the rights that people have to do the following:

- Know about the automated decisions that are being made about them.
- Contest these decisions by involving a person who is appointed to audit the algorithm's decision-making process.

To summarize: almost anytime that you do something meaningful with data, rules determine how you can do it. But, how do you know which rules apply to you?

This isn't always an easy question to answer. But to help you do so, we'll now provide a tour of the rules that might apply to your work. We'll start with the major US federal rules and then move on to the major regional rules.

Major US Federal Laws and Regulations

Let's start our tour with the major federal rules in the US. **Federal** means that these rules apply to anyone working in the US, regardless of the state. This is important, because states often have their own rules. We'll get to some of those later.

Federal Trade Commission (FTC)

The Federal Trade Commission (FTC) is a government agency for protecting consumers, or people who buy goods and services, in the US. The FTC was one of the first government agencies to start policing how companies use customer data. It has the power to investigate companies who have practices that deceive consumers. For more information, refer to A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority.

In the 1970s, the FTC began to consider data security and data-privacy violations as deceptive commercial practices. For example, if a company says to its customers that it won't sell their information but does so anyway, the FTC will consider that a deceptive practice. Note that the primary concern of the FTC is the honesty of companies with their customers. So, if a company says to its customers, "We plan to sell your information to anyone who's interested in buying it," and they do so, the FTC will most likely find that acceptable.

To read more about the history of the FTC enforcing data security and data privacy, refer to Privacy and Security Enforcement on the official FTC website.

Finance

The FTC enforces two major rules that impact the handling of financial data. The first is the **Gramm-Leach-Bliley-Act of 1999 (GLBA)**, which is also known as the Financial Services Modernization Act of 1999. This rule tells financial institutions how they can collect and share the personal financial information of their customers. It also requires financial institutions to protect financial data from malicious hackers and other types of data breaches. Finally, it tries to prevent people and companies from accessing financial information under false pretenses, which is called **pretexting**.

To read a summary of the GLBA, which includes links to the full text of the rule, refer to the Gramm-Leach-Bliley Act on the official FTC website.

The second major rule that impacts financial institutions is the **Fair Credit Reporting Act of 1970 (FCRA)**. This rule primarily impacts agencies that collect information about consumers, such as credit bureaus, medical information companies, and businesses that screen tenants for landlords. The FCRA controls how these agencies can share the information that they collect about consumers—by specifying the conditions under which people and companies can request access. It also requires that agencies investigate any complaints that consumers make about the accuracy of a report. Furthermore, it requires that agencies let consumers know if any adverse actions, such as a denial of credit, are taken based on a report.

To read a summary of the FCRA, which includes links to the full text of the rule, refer to Fair Credit Reporting Act on the official FTC website.

Children

The FTC enforces a rule to protect information about children, called the **Children's Online Privacy Protection Act of 1998 (COPPA)**. This rule gives parents the right to control the information that's collected from children online. Companies that either have services directed at children under 13 or collect information about children under 13 must do the following:

- Notify the parents of those children about the information that they're collecting.
- Obtain parental permission to collect, use, or share their children's data.
- Give parents access to their children's data.

- Limit the information that they collect about children to the minimum that's needed for participation in the activity.
- Set up security safeguards to prevent the unauthorized sharing of children's information.

To read a summary of COPPA, which includes a link to the full text of the rule, refer to Children's Online Privacy Protection Act on the official FTC website.

Healthcare

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes the **HIPAA Privacy Rule**. This rule dictates how Protected Health Information should and should not be handled. **Protected Health Information**, or **PHI**, refers to any information that can be used to identify a person, and information that a health or medical organization (or any of its associates) holds or transmits. Organizations can use this information to treat patients and obtain payment without a patient's written consent. However, all other uses of PHI require written consent from the patient. This rule also gives patients the right to correct any inaccurate PHI, and it requires organizations to notify patients about how their information is being used.

To read a summary of the HIPAA Privacy Rule, which includes links to the full text of the rule, refer to The HIPAA Privacy Rule on the U.S. Department of Health & Human Services website.

Education

The **Family Educational Rights and Privacy Act (FERPA)**, enacted in 1974, protects the privacy of student education records. **Education records** refer to the records that a school maintains, which FERPA gives parents and students the right to access and review. They also have the right to correct any inaccuracies that they find in those records. In most cases, FERPA requires schools to have written consent from a parent or student to share information from the student's education record. However, the rule lays out some exceptions. For example, schools can share student education records with officials who are auditing the school—without explicit consent. Schools can also share these records with financial aid organizations. Finally, schools can share **directory information**, such as students' names, addresses, and telephone numbers.

To read a summary of FERPA, refer to Family Educational Rights and Privacy Act (FERPA) on the U.S. Department of Education website. For the full text of the rule, refer to FERPA | Protecting Student Privacy.

Communications

The **Electronic Communications Privacy Act of 1986 (ECPA)** protects the privacy of certain types of communications that are made on computers. This rule has some specific provisions. One, the **Wiretap Act**, prevents electronic communications from being intercepted. Another, the **Stored Communications Act (SCA)**, specifies how service providers, such as internet and telephone companies, can store and share information about their subscribers. The ECPA also requires the government to have a court order before installing communication surveillance devices.

To read a summary of the ECPA, which includes a link to the full text of the rule, refer to Electronic Communications Privacy Act of 1986 (ECPA) on the Bureau of Justice Assistance website.

Now that we've learned about the major US federal rules, we'll move on to the major regional rules.

Major Regional Laws and Regulations

We learned that, in the US, data protection is handled in many ways. However, many people find the myriad of rules around data to be a problem. Complex rules are hard to follow and even harder to enforce. And with the internet, data sharing is not neatly bound by industry or by country or region. Many organizations are working to centralize and standardize the rules around how data gets used, so the rules won't be as tightly bound by industry or by country or region. So, let's now switch gears to explore this more comprehensive approach.

The OECD Privacy Framework

The Organisation for Economic Co-operation and Development (OECD) is an organization of 38 countries that work together to form ideas and frameworks. Specifically, these address economic, social, and environmental challenges that cross borders. In 2013, the OECD developed the OECD privacy framework, which consists of guidelines around privacy. This framework was intended to be used as a basis for privacy rules in different countries and includes eight principles of privacy:

- **Collection Limitation Principle:**
    - The personal information that can be collected about people should have limits.
    - People should be able to consent to sharing the information that's collected about them.
    - Organizations should collect information in legal ways.
- **Data Quality Principle:**
    - Organizations should have a reason for collecting information about people.
    - Information that's collected about people should be maintained so that it's always accurate and up to date.
- **Purpose Specification Principle:**
    - Organizations should determine why they're collecting information when they initially collect that information.
    - They should use the information that they collect for that initial purpose and not for other purposes.
- **Use Limitation Principle:**
    - Information about a person should not be shared without the consent of that person.
    - However, cases might exist for which information about a person must be shared according to the rule.
- **Security Safeguards Principle:**
    - Information about people should be secured to prevent the unauthorized access, sharing, destruction, or modification of that information.
- **Openness Principle:**

    - Organizations should share information about their policies and practices around information about people.
    - People who interact with an organization should be able to find out what information that organization has stored and how that information is being used.
- **Individual Participation Principle:**
    - People should be able to:
        - Confirm whether an organization has information about them.
        - Request all the information relating to them that an organization has stored.
        - Receive that information within a reasonable timeframe, at a minimal cost, and in a format that they can understand.
        - Request changes to the organization's information that relates to them.
        - Request that personal information be deleted from the organization's record.
        - Be provided with reasons if any of the preceding requests are denied.
- **Accountability Principle:**
    - Organizations should be held accountable for following all the preceding seven principles.

The OECD privacy framework also includes recommendations for how to implement these principles in an international setting—and in a way that balances protecting data security and data privacy with the creation of environments that support business and industry growth.

To read a helpful summary, refer to OECD Privacy Principles. To access the full framework, refer to The OECD Privacy Framework.

The OECD privacy framework has served as the basis for some incredibly impactful rules, and more rules that are based on this framework are in the process of being passed. Furthermore, both the European Union (EU) and the State of California have created rules based on the principles of privacy that have had a tremendous impact on the way that companies collect and use data. Next, we'll learn about two of those rules: the General Data Privacy Regulation (GDPR) and the California Consumer Privacy Act of 2018 (CCPA). We'll then consider rules that might exist in other regions, like the ones where you currently live or work.

General Data Privacy Regulation (GDPR)

The **General Data Privacy Regulation (GDPR)** is a set of rules that's based on the OECD privacy framework. Specifically, the GDPR dictates how organizations can interact with citizens of EU member states. The EU adopted it in 2016, and organizations were required to comply with its rules by May 2018. It's had a monumental impact on how organizations do business online. Although it focuses on how organizations interact with information from citizens of the EU, its rules have reshaped the internet for everyone in many ways.

Pretty much anyone who's been online has had to acknowledge a question or notification about cookies when going onto a website. You have the GDPR to thank for this. That's because cookies provide a way of

tracking information about people online, and the GDPR requires that people consent to sharing their information with organizations.

The GDPR is complex. In fact, the full text of the GDPR consists of 88 dense pages of legalese. You should know three main things:

- It implements the same basic ideas as the OECD privacy framework.
- Any organization that processes data associated with EU citizens and that doesn't comply with the GDPR can receive huge fines. So, organizations are incentivized to follow it.
- In addition to implementing the eight principles of the OECD privacy framework, the GDPR has rules about automated decision-making. These require transparency around decisions that an algorithm or computer program makes—and the right to contest those decisions.

If you're interested in more details of the GDPR, refer to The principles from the Information Commissioner's Office (ICO) of the United Kingdom (UK). This site will guide you through the most important aspects of the rule.

California Consumer Privacy Act (CCPA)

In 2018, the State of California passed the California Consumer Privacy Act (CCPA), which is also based on the OECD privacy framework and resembles the GDPR. The CCPA gives California consumers specific privacy rights around the personal information that businesses collect about them. They have the right to know what information gets collected and how it gets used, shared, or sold. They also have the right to delete that personal information and to opt out of it being shared. Finally, this rule states that companies can't discriminate, in terms of either price or service, against consumers who exercise these rights.

Unlike the GDPR, the CCPA does not require that consumers consent to the collection of personal information. But, it does require that businesses give consumers notice of that collection. Businesses must also allow users to opt out of the sale of personal information. Note that depending on the specifics of the transaction, third-party cookies might be considered a sale of personal information. In this case, websites need to provide a clear way for California users to opt out. Specifically, they must include a link on the homepage that goes to a page or a set of pages that are specifically titled and that allow users to opt out of the selling or sharing of personal information. The law also places limits on the use of sensitive personal information.

The CCPA is hugely important for personal data rights in the US. The EU has a long history of regulating how companies use personal information, but this has not been the case in the US. California, however, is a large state; most companies who do business online in the US have customers based in California and, consequently, have to comply with this rule.

Other Regional Laws and Regulations

California has one of the most comprehensive rules around data privacy, but other states in the US have started catching up.

Before moving on, practice finding your regional rules. Go to the State Laws Related to Digital Privacy website. Then search for any state of your choice, such as Colorado or Virginia, to find out if they have rules around how data can be used. You can also do an internet search for the name of a state and the phrase "data laws" to discover more.

You might have noticed that many new rules are in progress, which will impact the way you use data. Be sure to stay up to date on the rules that relate to your work. To do so, we'll provide a checklist that you can use to navigate the data regulatory environment.

A Checklist for Navigating the Data Regulatory Environment

- Consider your industry and the types of data that you process. Research the rules that are specific to these. Look up cases of other companies in your industry facing legal charges as a result of their use of data.

- Research the data and technology rules for your location. If you're in the US, look up all the relevant federal and state rules. If you're outside the US, look up the rules for your region.

- Figure out where your customers are located. If you have customers who live in places with comprehensive data security and data privacy rules, like EU member states, the UK, or the State of California, you'll need to adhere to those rules.

- Determine if you process the data of children or if children will likely use your product. If so, you'll need to handle their data in accordance with the relevant rules based on the locations of you and your customers.

Congratulations on navigating a vast and tangled web of data privacy rules! Familiarity with these rules will prepare you for working with the many organizations that they impact.
