EXperimental Learning

MIT BDA Module 1 Unit 1 Video 8 Transcript

Speaker key

CK: Cameron Kerry

HY: HapYak

CK: In this video, we're going to look at some of the ways that law and public policy affect data analytics. The goal here is to make you aware that the laws of several countries can have an impact on using data about people.

Different types or sources of data, about people, can trigger the laws of many countries. I'm going to focus on two sets of laws, the European or the EU for short, and the United States. The EU has the most comprehensive set of laws being adopted in many other countries. The US has the most distinct alternative.

The foundation of most privacy laws is a set of fair information practice principles, or FIPPs. These principles have been expressed in various ways, but I'll lay them out, as we did when I led the White House Consumer Privacy Bill of Rights work that was put out in 2012. That Bill of Rights laid out seven principles.

00:01:30

Number one, individual control. Consumers have a right to exercise control over what personal data companies collect from them, and how the companies use it. Number two, transparency. Consumers have a right to easily understandable and accessible information, about privacy and security practices. Number three, respect for context. Consumers have a right to expect that companies will collect, use and disclose personal data in ways that are consistent with the context in which the consumers provide that data.

Number four, security. Consumers have a right to secure and responsible handling of their personal data. Number five, access and accuracy. Consumers have a right to access and correct personal data in usable formats, in a way that's appropriate to the sensitivity of the data about them, and the risks of adverse consequences to them if the data is misused.

Number six, focused collection. Consumers have a right to reasonable limits on the personal data that companies collect about them. And number seven, accountability. Consumers have a right to have personal data handled by companies with appropriate measures in place to make sure that they comply with the Fair Information Practice Principles of the Consumer Privacy Bill of Rights.

00:03:10

The Fair Information Practices Principles are the basis of the EU's comprehensive law, the European Privacy Directive of 1995. Europe is in the process of coming up with a new regulation that will be binding on all of the EU member countries, and add to privacy protections. Here are some particular things to be aware of about these EU laws.

First, they apply to all personal data. Personal data is defined as any information relating to an identified or identifiable natural person. An identifiable person is a person who could be identified directly or indirectly.

00:04:00

This is a broad definition, especially as aggregation and correlation make it increasingly possible to identify individuals, even if there are no obvious identifiers in the data. So, you should be conscious that many kinds of data could be personal data, even without those obvious identifiers.

Second of all, processing of data must have a lawful basis. The key lawful basis is the consent of the data subject, the person that the data is about, but there are other provisions and exceptions from the general environment of consent.

Third, processing of sensitive data such as race, political or religious beliefs or information about sexuality is generally prohibited, with some exceptions. Fourth, decisions based on automated processing, i.e. algorithms is limited if they have legal effect or significant legal effects on an individual. Fifth, transfers of personal data outside the European Union are restricted. Data of people in the EU can't be transferred outside the EU, except to countries that the European Union has deemed adequate when it comes to privacy and data protection. The United States is not one of those countries. The US and EU have agreed to a new privacy shield arrangement that would allow transfers across the Atlantic, but as of the time that this is being recorded, that is still going through the approval process.

00:06:06

The United States does not have a comprehensive law like the EU Directive or Regulation. Instead, it has a body of laws that features federal laws for business sectors that handle sensitive information such as financial services. In addition to these specific laws, the Federal Trade Commission broadly enforces the privacy promises that companies make, and states, and other federal agencies also have privacy laws and regulations.

In addition to financial services, the sectors covered by specific laws are credit reporting, the Fair Credit Reporting Act, medical records, HIPAA, or the Health Insurance Portability Act, communications data and ISP data, under the Communications Act and the Federal Communications Commission's Net Neutrality Decision, student records, under the Federal Education Records Privacy Act, and state laws, and data of children under thirteen, under the Children's Online Privacy Protection Act.

In addition, most states have data breach notification laws, and Massachusetts, where MIT is based, has a data security law that requires measures to protect the security of sensitive personal information. Most US laws focus on personally identifiable information, or PII.

Data reflected in specific identifiers like names, social security numbers, and other unique data. HIPAA, the Health Law, lists eighteen different specific categories of identifiers.

To look at how these legal regimes might affect their work, let’s imagine that you’re a researcher at an institution that wants to work with MIT on this course, and analyze data generated by students at your institution. Think for a moment about some of the questions that you might want to ask.

HY: If you were a researcher wanting to work with MIT to analyse data generated by students, what are some of the questions you might have related to data privacy policies?

Thank you for your reflection. Keep watching to learn what would be the most pertinent questions to ask.

CK: Here are a few to consider. Is the data involved personal information? How could it be used to identify individuals? Is the data subject to FERPA, the student records law, if so, what does that law require?

00:09:00

Have the students involved consented to the kind of use and analysis that you’re thinking about? Now suppose your participating institution is located in Europe. What additional questions might you have? Here are a few. Have the students involved consented to the transfer of their data to MIT? Are there agreements in place to ensure that the data is protected, consistent with EU law, is there sensitive information involved, as that’s defined in the EU? Will the data lead to algorithmic judgements and how will those judgements affect the students?

In a later module, we’ll explore how these rules and principles affect some of the practical choices affecting privacy in the context of data analytics.

00:10:09