Welcome to Digital Footprints, module nine.

In this module, we will learn how legislation affects digital footprints.
The Internet is global, but privacy laws are not. The Internet ecosystem is complex and regulating it is a challenge.
Most privacy laws and guidelines focus on “personal data” or “personal information”, often defined as “information relating to an identified or identifiable individual.”
However, the definition of “online personal data” is evolving. There is a growing awareness of the potential privacy impact of any information that can be used to single out or treat an individual differently, even if the individual cannot be identified by name.
Combined with advances in data linking, storage, retrieval, correlation and analysis, ever increasing amounts and categories of data are likely to fall within the scope of privacy and data protection laws.

As a result, there are proposals to make this explicit, either in the language of privacy regulations or in explanatory materials.
Generally speaking, privacy and data protection laws only apply to information about living individuals, but some countries extend the application of the law to information about deceased individuals. The more “digital” and online our lives become, the more significant the question of managing an individual’s “digital legacy” after death becomes.
Some countries have laws that are designed to protect pre-defined classes of data that are traditionally considered more sensitive, including medical data, financial data, and government issued identifiers.
| Article 12 | Universal Declaration of Human Rights |
| Article 8 | European Convention for the Protection of Human Rights and Fundamental Freedoms |

Individual’s right to respect for their privacy or private life

Article 12 of the Universal Declaration of Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms both refer to the individual's right to respect for their privacy or private life, but there is no privacy or data protection law that applies everywhere in the world: no single set of data processing rules that covers all Internet services and users.
Since the Internet does not respect national boundaries, we need to find ways of increasing the consistency of legal protection, while respecting national and cultural differences. There is fairly widespread international agreement on a set of key principles but the practicalities of privacy law and enforcement vary widely by country.
Some countries and regions, such as Europe, take a rights-based approach towards data protection and privacy.
Others, even if they do not take a rights-based approach, have adopted a “comprehensive” approach to privacy.
Yet, others, such as the United States, rely on more industry-specific laws, self-regulated best practice and codes of conduct. Then, there are the countries that have no (or only rudimentary) privacy laws.
These differences all increase the challenge of bridging the gap between country-specific laws and the frontier-less nature of the Internet. To enable cross-border flows while protecting privacy, a number of groups of countries have reached binding or non-binding agreements. Click the image to view a list of such agreements.
Here is a list of some binding and non-binding agreements adhered to by some countries.

- OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, specifically Part 3
- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, specifically Chapter 3
- APEC Privacy Framework and APEC Cross Border Privacy Rules system (a voluntary accountability-based system)
- U.S. EU & U.S.-Swiss Safe Harbor Frameworks
- EU Binding Corporate Rules (for multinational companies).
Now let’s take a look at the pros and cons of having technology-specific laws.

In some cases technology-specific laws can genuinely improve the users’ browsing experience and/or security (for instance, if cookies are used in support of a two-factor authentication protocol).

However, technology-specific laws may also have the unintended consequence of shifting the unwanted activity outside the scope of the law. This kind of approach may, perversely, give service providers an incentive to look for other, unregulated means to monitor or profile users, such as browser fingerprinting and server-based storage which may prove harder (or impossible) for the users to detect.
A critical regulatory factor is the issue of consent. User consent plays an important role in extending collection, use and disclosure of “personal data” beyond what is strictly necessary to provide a product or a service. One approach is to insist that decision-making must rest with the individual most likely to be affected, but putting this into practice can be more problematic than one might expect.
This is because, Internet users: rarely have the information or understanding they need to make an informed decision. They are often given choices that are binary (i.e. say “yes” or you don’t get the service). The users may have only uncertain knowledge and incomplete information on the potential consequences of consenting. Users are increasingly asked to disclose personal data of other people, such as when a service asks for your contact list.
In summary: There is no single set of rules, and no single definition of what data needs to be protected. Regulating at the technology level is generally unsuccessful – but regulating for behaviour makes the law highly culturally-dependent, and harder to reconcile with other jurisdictions.

The issue of user consent seems simple on the surface, but conceals deep technical and even behavioural complexity.

Thus realistically, we cannot hope for a one-time legislative fix to the privacy problem: we should expect to have to engage in a continuous process of evaluation and adjustment.
Congratulations! You have completed Digital Footprints module nine How Does Legislation Affect Digital Footprints.

Remember, you can always find more information, whitepapers and other training modules via the Internet Society's Identity and Privacy pages.