Welcome to the

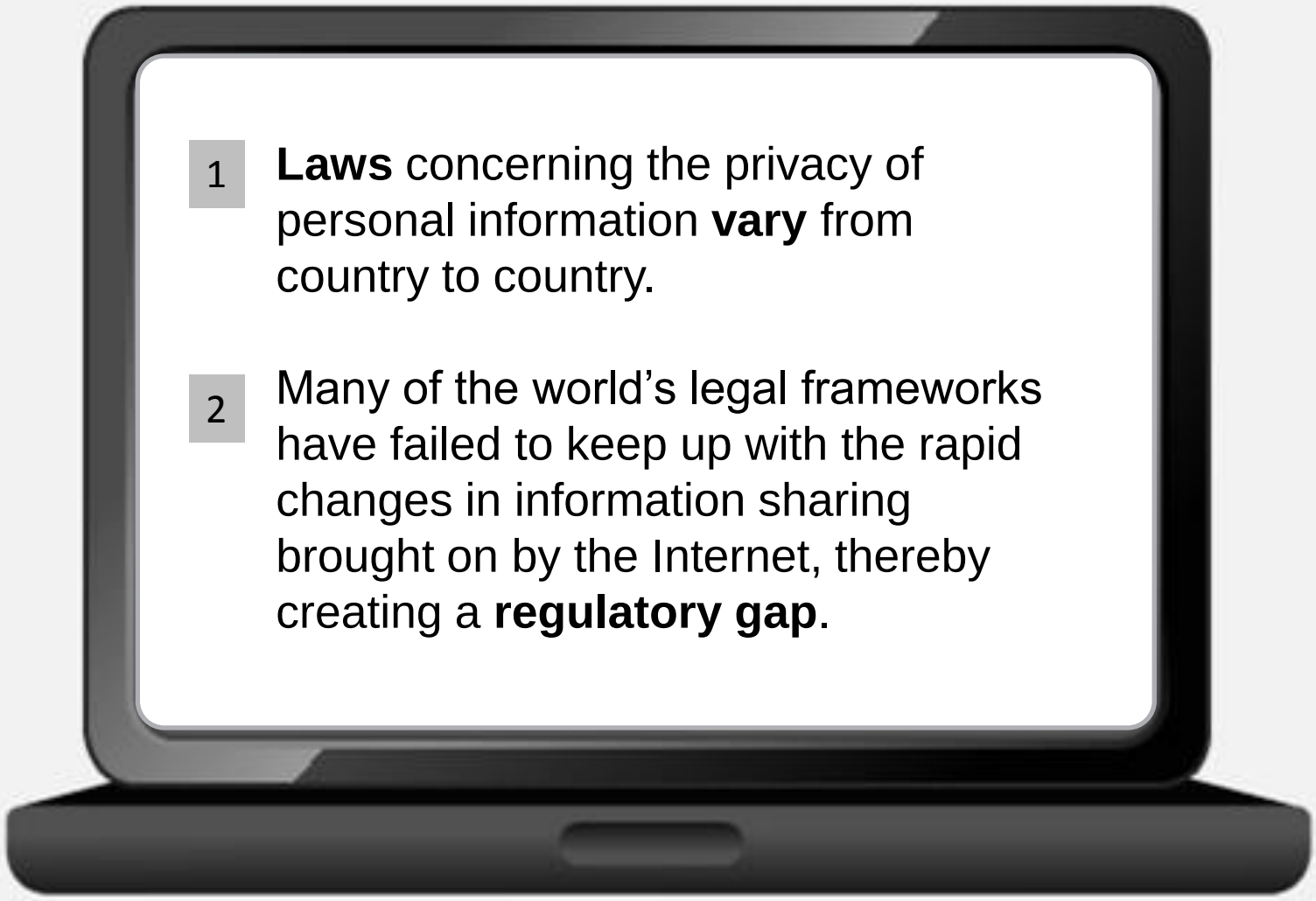
Protecting Your Privacy

Training Module

Internet Society

Introduction

Introduction



Objective

By the end of this module, you will be able to:

- Understand the key concerns related to online identity and privacy
- Recognise what kind of user information is collected and why
- Identify the ways of controlling the privacy of your online identity

Privacy on the Internet

Since it is hard to identify what can be termed as personal data, there is no universally agreed definition of privacy, whether offline or online. Privacy is contextual.

Perspectives on privacy are influenced by culture, economics, society, politics, religion, history, experience, education, etc.

What is Online Privacy?

Online privacy can be defined as consensual sharing of personal data within a specific context with an expectation of scope.

Key Concerns Related to Online Identity

Internet users are naturally concerned about how their personal information is stored, collected, and used. In a word, it is their privacy that concerns them.

In addition to the problems of **identity theft**, users have questions about the widespread practice of having information about them shared among services traded to third parties.

E-commerce and Criminal Activities

Criminals have stepped up their efforts to steal:

- Personalized identifiers
- Passwords
- Associated information

The motivation for identity theft is often simple economic gain.

By impersonating you, criminals may be able to:

- open lines of credit in your name
- engage in online actions that damage your reputation
- gain access to systems and online resources without legitimate authorisation

Is Sharing Online Information Safe?

The simple act of sharing online information is a source of concern for many Internet users.

Voluntary

Within social networks.

For example, you may have willingly shared your location, age, gender, and personal interests on your Facebook page.

Involuntary

When your information is traded by online advertising networks.

Online advertising networks may deduce much of this information, based on the trail of websites you visit and the searches you make.

Internet Society

Why is it difficult to have Control Over Shared information?

- There are few industry standards or regulatory frameworks available.
- There is little agreement regarding what is proper and improper.
- Users want to be able to decide what information is private and control what is shared.
- Regional differences make global solutions difficult.

Many Web pages you visit include a (hidden) Commercial Transaction

The websites you visit may be free to you, but each has its own costs that have to be paid somehow.

The most common method of doing that is through **advertising**, wherein a third party pays the website owner for the privilege of putting advertisements near information they believe you want to see.

How is a Partial Identity Created?

An in-depth online partial identity of a person can be created based on information gathered from the following three sources:

Actively disclosed data

Where the user has the intention of disclosing. For example, location check-in, social network posts.

Passively disclosed data

Third party location tracking, CCTV images, Automatic Number Plate Recognition (ANPR), stealing browser history without the user's knowledge or consent.

Data mining, statistical profiling and inference

For example, inference from location/travel patterns, social graph, or purchase patterns.

Internet Society

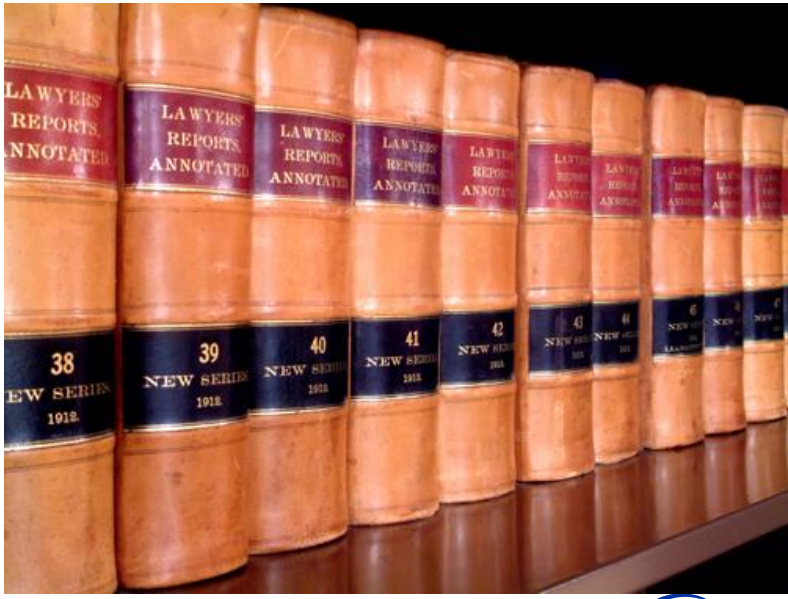
Who Controls Private/Personal Information?

Most online information about an individual is beyond the individual's control.

Most countries have some form of legislation that defines personal data and regulates its collection and use of personal data: however, that does not necessarily mean the individual has substantial control over data that affects their privacy.

Example:

- Governments of many countries differ and are in some cases incompatible.
- The law has a hard time keeping up with developments in data capture and exploitation.
- Not many data protection regimes are particularly well enforced.



Internet Society

Forces at Work

Three forces are at work to return control of your personal information to you.

1

2

3

Click each tab to learn more.

Forces at Work

Three forces are at work to return control of your personal information to you.

1

2

3

Many **countries** are considering amending or introducing new laws that would require user consent for the collection and use of personal information.

Forces at Work

Three forces are at work to return control of your personal information to you.

1

2

3

Businesses and organizations are seeing an economic incentive in giving you more control over your personal information, as doing so can increase data accuracy and reduce the costs of collecting and updating the information.

Forces at Work

Three forces are at work to return control of your personal information to you.

1

2

3

New technologies are being developed that will allow companies to share information about users' identities securely, while allowing users to exercise greater control over who has access to their information and what types of information can be shared.

Evolving Technologies

The technology used to control identity information was based on centralized solutions.

Over time, control of identity information shifted to federations; groups of organizations that wanted to extend services to each other's users.

These federations are able to use a wide variety of technologies to share identity information in a controlled way. These include:

- Security Assertion Markup Language (SAML)
- OpenID Connect
- OAuth

KNOW MORE

Internet Society

Evolving Technologies

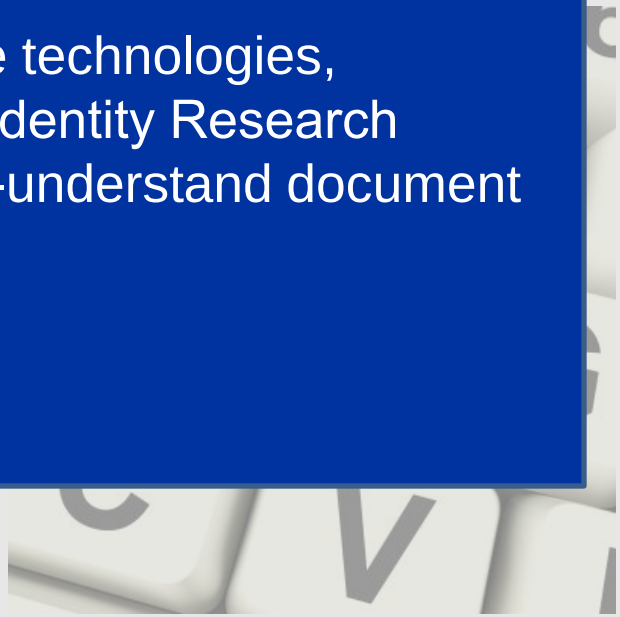
The technology used to control identity information was based on centralized solutions.

Over … of orga…

Thes… varie… inform…

- Se… (S…
- O…
- Inf…
- OAuth.

KNOW MORE



If you want to know more about these technologies, **click here** to view Google's Internet Identity Research project that has produced an easy-to-understand document on these technologies.

Internet Society

Making Online Transactions Safer, Faster, and More Private

The National Strategy for Trusted Identities in Cyberspace (NSTIC) envisioned ***Identity Ecosystem*** aims at creating a cyber world where individuals, businesses, and other organizations would enjoy greater trust and security as they conduct sensitive transactions online.

The Identity Ecosystem is tasked with improving upon the passwords currently used to log-in online.

The key benefits of this user-centric online environment include privacy, convenience, efficiency, ease-of-use, security, confidence, innovation, and choice.

EXAMPLE

Making Online Transactions Safer, Faster, and

The
envis
indiv
and

The
log-i

The
conv
choi

EX

Example

Jane Smith, a student, could get a digital credential from her cell phone provider and another one from her university and use either of them to log-in to her bank, her e-mail, her social networking site, and so on, all without having to remember dozens of passwords. If she uses one of these credentials to log into her Web email, she could use only her pseudonym, "Jane573." If however she chose to use the credential to log-in to her bank she could prove that she is truly Jane Smith.

People and institutions could have more trust online because all participating service providers will have agreed to consistent standards for identification, authentication, security, and privacy.

rust

to

cy,

and

Society

Enabling End-user Privacy Controls

Enterprises and governments are engaging with each other on the topic of enabling end-user privacy controls in the online environment.

International efforts such as regulatory guidance from the **Organisation for Economic Co-operation and Development (OECD)** and technical standards from the **Internet Engineering Task Force (IETF)** will continue to be part of the effort to ensure that the Internet is a safe place for all its users to interact.

Knowledge Check

Select all that apply.

Malicious use of your personal data exposes you to risk of:

- [ ] Fraudulent purchases
- [ ] Credit fraud
- [ ] Theft of goods
- [ ] Embarrassing hair loss
- [ ] Reputational damage
- [ ] Computer misuse
- [ ] All of the above

Knowledge Check

State if the following statement is true or false.

Just by viewing or clicking through information or services on a website, you are divulging information about yourself that can be used to create a fairly significant partial identity of you.

- True
- False

Knowledge Check

Which of the following are stakeholders in the privacy debate?

- Legislators
- Businesses
- Technology vendors
- Footballers' wives
- Credit rating agencies
- Tabloid newspapers
- Librarians
- You

Conclusion

Congratulations!

You have reached the end of the **Protecting Your Privacy** training module.