Lecture – Data protection in the online world

What Is Online Privacy?

Online privacy, also known as internet privacy or digital privacy, refers to how much of your personal, financial and browsing information remains private when you're online.

This has become a growing worry, with browsing history and personal data all potentially at risk when online.

Cybersecurity can be confusing sometimes.

Many people underestimate the importance of online privacy, but they should be aware of how much information they're sharing - not just on social networks, but just by browsing itself.

Why online privacy is so important

You should value data privacy online in the same way as the real world. So you have a confidential conversation behind closed doors or only share your financial details with a bank.

It's important to remember that nothing is free: whether it be downloading apps, using a company's "free" email service (such as Gmail) or social networks like Facebook. Even visiting a website means you're sharing data about yourself. And, as some people in your life know you better than others, online privacy exists on a spectrum: some online entities gather and store more information about you than other platforms.

Online privacy is important for numerous reasons. You don't want to share details of your personal life with strangers and it's hard to be sure what personal information is gathered and by whom: information collected by one company might be shared with another.

You might be uncomfortable with bespoke, targeted ads that remember your internet search history.

Even more problematic is information sold from one company to another, or data gathered and shared without your consent. Ultimately, this is identity theft.

Public concern over internet privacy

In a recent poll of American internet users, 81% said they believe they have no control over data collected by private companies. Worse - the number climbs to 84% when asked if they could control the government's collection of their data.

GDPR

In the EU, concerns like these were addressed with GDPR (General Data Protection Regulation). This set of laws, passed in 2016 and implemented in 2018, was intended to protect the privacy and data of every EU citizen.

There are 99 articles in GDPR. These include:

the right to know what data a company holds about you

an opportunity to refuse a company access to browsing history and cookies when you visit their site

clear responsibility for companies to gain consent for customer information

stricter regulations regarding contacting customers and sharing contact details with third parties

The right to be forgotten: data privacy as a human right

“The right to be forgotten” is a relatively new phrase, but it grows in relevance every time someone visits a site. Some tech companies have customer information dating back years, logging every site they visited, their preferences, shopping habits, political views and more.

The right to be forgotten is the right to ask those companies to delete and surrender this information.

This can extend to online chatter and third-party discussions: there have been cases where people have fought to have their names and images removed from “revenge porn” (and search engine results for same). Some have requested past personal stories (involving petty crime or embarrassing viral stories) be taken off the internet.

This is an ongoing debate. On one side, the right to be forgotten arguably protects those who want privacy and not be reminded of previous mistakes. Those opposed (who, incidentally include some tech giants) argue that it amounts to censorship and could lead to the rewriting of history.

What is information privacy?

This is sometimes referred to as data privacy or online privacy.

Information privacy is an element of online security that looks at the following issues:

data acquired

how data is collected or stored

whether or not data is shared with a third party

regulatory restrictions, such as GDPR

Many companies such as Google, Amazon and Facebook have profited handsomely in the “data economy”, - accumulating user data to maximise either product or ad sales. Good practice regarding information privacy means keeping customer information secure, not sharing it with third parties without consent or using data maliciously or negligently.

Personal privacy vs sensitive information

When it comes to internet privacy, there is personal and sensitive information. They are defined the following ways:

Personal information - identifiers, such as name, IP address, address, etc.

Sensitive information - very private data like medical records, but also information that you might not be ready to share publicly, such as your sexual orientation or political views.

How does privacy differ from information security?

Online privacy and security often overlap, as one sometimes affects the other. They can be differentiated this way.

Privacy - you want the company you deal with (say, a bank or a social network) to keep your data and information itself, not share it publicly or with third parties. In this instance, privacy is breached but security is maintained.

Security - this is the next step. If the data shared includes (for instance) financial information or your home address, then both privacy and security is compromised.

The biggest internet privacy issues

As mentioned, internet-related privacy issues exist on a spectrum, from information you don't mind sharing (say, a public social media account), to nuisance privacy compromises (targeted ads, for instance) to public embarrassment or breaches that affect your personal life (financial breaches or professional setbacks).

Here are the online areas currently with the most discussion, risk and controversy...

Search engines user tracking

Search engines not only log what you've been looking for, but often what sites you subsequently visit. Additionally, if the search engine provider also makes the browser (Google Chrome, Firefox, Internet Explorer, etc.), they have your browsing history regardless of whether you searched for the site.

Search engines can (and do) collect:

search history

cookies

IP addresses

click-through history

Collectively, this information can be used for "profiling" - i.e., compositing a customer persona based on browsing, shopping, and social media preferences.

Social media data harvesting

Social media privacy hit the spotlight in recent years thanks to a string of scandals, including the Cambridge Analytica story (in which data was used to manipulate voters), cyber bullying and "doxing" (sharing private information publicly).

Additionally, some major social networks sites have had data breaches, leaving millions of users exposed.

Victims of data and privacy breaches are not to blame, and we will be talking about how best to protect your privacy online later. But there is an adage when it comes to social networking: don't say anything online that you wouldn't like repeated to your parents or employer!

Cookies/online tracking

For the most part, cookies are harmless. They are code that tell a website information on your browsing history, which in turn can help the user by remembering:

logins

identification

preference settings

ad settings

language settings

Cookies can become a concern when third-party ad serving is involved. When you visit a site, your browser has assembled information from various sources that dictates the ads you see. You have, essentially, become a profile/persona, even if it's only seen by bots.

This has been questioned by privacy advocacy groups, as companies like Google amass vast amounts of consumer data to deliver personalised ads based on browser history.

Mobile apps and privacy

We all have apps on our phones. In fact, the average smartphone owner is using 9 apps per day and 30 per month. We know our favourite apps and how they make our lives easier - but they know even more about us.

Many apps request location details (which makes sense if it's, for example, a taxi app), usernames and email addresses.

The next level of information is "risky permission". This means information that would be risky if it fell into the wrong hands including access to a phone's microphone/recorder, camera and contacts.

A good rule of thumb is to consider whether you trust the app provider/company to hold this information. If there's anything you feel uncomfortable with, you can deny access, either instantaneously or in the app's settings.

Identity theft

Identity theft has been a crime since long before the internet, but new technology has opened up fresh avenues for con artists and thieves.

Online identity theft happens when someone accesses your personally identifiable information (PII) to commit fraud. This information might be a driver's license, bank account details, tax numbers, or anything else required to impersonate you online.

In the worst-case scenario, your information might end up for sale on the dark web.

They source this information often by the following means:

phishing: criminals pose as reputable contacts such as financial institutions to trick you into surrendering sensitive information or opening malicious attachments

malware: malicious software that can access your computer's operating system

pharming: hijacking information using a virus without your knowledge, often through a fake site

discarded computers and phones: make sure any device you get rid of is thoroughly scrubbed before you sell it or give it away

Our top tips to help you protect your privacy online

It's easy to feel despondent when you read about online security threats, but there are simple steps you can take to greatly reduce the risk of online fraud.

Here's what we recommend…

1. Use DNT setting

DNT stands for "do not track" and you can change DNT settings on your online browsers. When you enable it in your browsing (be if Chrome, Firefox, or another browser), you are telling websites and third party partners that you do not want to be tracked.

2. Use cookie-blocking browser extensions

There are cookie-blocking browser extensions available which will help keep tracking and especially third-party information gathering, at bay.

3. Opt out of app tracking

As mentioned above, apps have access to a lot of information about you. But you can prevent this by going to your app settings (either within the app or in your phone settings) and opting out of the app tracking information, including location.

4. Review privacy policies carefully

A common mistake when it comes to online browsing is to simply click "agree" to user agreements and privacy policies without reading them. We'd advise you to take a look at any document before clicking "agree" or "accept".

If you don't have time to read it (and some user agreements are hundreds of pages long), research what the app or site asks of its users and whether you're comfortable with what they know about users.

5. Access the internet via VPN

A VPN (virtual private network) routes your online activity through an encrypted virtual tunnel. This keeps your IP address and location secret from sites you visit; it protects you from hackers; and in some cases, it can give you access to some sites and services unavailable in your country.

6. Browse in incognito mode

When browsing online, you have the option of choosing “incognito” mode. Also known as “private browsing”, it means that your online history isn’t stored or remembered.

7. Use a different search engine

If you’re concerned about what a search engine knows, it might be an idea to change engines, even if you only do it occasionally. DuckDuckGo, for instance, markets itself as a more private and secure alternative to Google.

8. Be wary of what you click online

Phishing (sourcing your sensitive data when you go online) depends on you clicking on certain risky sites. So, tread carefully online and do not click on anything remotely suspicious. Don’t forget, some phishing threats pose as ads.

9. Secure your devices and use antivirus software

Finally, you should definitely have up to date, industry-leading antivirus software on your device, whether it’s mobile or a computer. Run it regularly and carry out frequent scans.