

# CSI-COP

## **Citizen Scientists Investigating Cookies and App GDPR Compliance**

CSI-COP MOOC: *Your Right to Privacy Online\_v2*



## Contents

<b>CSI-COP MOOC – informal education course</b>	<b>Page 2</b>
<b>Course Details</b>	<b>Page 3</b>
<b>Step 1: Privacy</b>	<b>Page 4</b>
<b>Step 2: Data</b>	<b>Page 8</b>
<b>Step 3: Online Tracking</b>	<b>Page 13</b>
<b>Step 4: Rights to data protection and privacy</b>	<b>Page 19</b>
<b>Step 5: Tools to protect your data and privacy</b>	<b>Page 23</b>
<b>Your feedback on the course</b>	<b>Page 27</b>
<b>Assessing your learning</b>	<b>Page 28</b>
<b>Becoming a CSI-COP citizen scientist</b>	<b>Page 29</b>
<b>Survey</b>	<b>Page 30</b>



## MOOC

CSI-COP's free informal education short course (massive open, online course -MOOC) can be taken by participating in an online, hybrid or in-person workshop (see the website: <https://csi-cop.eu/> for information), or by working through this document in your own time. Completing the five-step 'Your right to privacy online' course should take between 2 ½ to 3 hours.

The MOOC is about **your data and your right to privacy online**. Data across the Internet is collected through digital technologies in websites, and in apps (software programmes on mobile devices). These technologies include cookies, small text files placed on desktop computers, laptops or smart devices (tablets, mobile phones) when you visit a page on the Internet. Cookies can include digital trackers, such as tracking the precise location of your device. App settings can have permissions to access your contacts, your camera, your messages, microphone and other data on your mobile devices. The location of a device can personally identify a person who uses or owns the device, so its tracking has data protection and privacy implications.

The [CSI-COP EU Horizon2020](#) funded project has as its main objective to informally educate the general public about online tracking technologies and how to reject them. This can lead to the general public becoming "citizen scientists". A citizen scientist (CS) is a member of the general public engaged in the collection and analysis of data, as part of a collaborative project with professional scientists. CSI-COP's aim is to engage citizen scientists to **join the CSI-COP project team** in investigating the extent to which tracking is *by default* all across the Internet. The 2018 general data protection regulation (**GDPR**) offers a checklist against which compliance can be assessed. The CSI-COP team believe that the citizen science approach is necessary to forge collaboration between citizens and scientists and to investigate the extent to which our data is being tracked online through the websites we visit and the apps we use.

### Who is this course for?

This course would suit any individual over the age of 18, or school pupils guided by a teacher, who is interested in understanding how our data is collected across the web and through apps we use. The course would also suit any individual who wants to learn about how to protect their privacy online.

### What you need to complete this course

Use of a smart phone, tablet, laptop or computer with access to the Internet. You may also be able to access free wi-fi if you are in a university, or if you use a local library. But please do be aware that the benefit of free public wi-fi comes with the risk of hackers accessing your data. Please see [Kaspersky](#) information on how to avoid risk on public wi-fi here: <https://bit.ly/3v6thff>

### If you use Twitter

We have suggested a short Tweet at the end of each step that you could send to others letting them know you are taking CSI-COP's informal education course. You can tag CSI-COP by using [@cop\\_csi](#).

### **Please do check the course details on page 3, then try the informal learning steps 1, 2, 3, 4 & 5 from page 4.**

In each step the learning outcomes and the content will be briefly introduced. For background information, names of people will accompany links to further reading in each step. More details will be found at the end of the step in a 'Further Reading' section.

To enhance your learning and understanding, please look out for a **big question** in each step. This asks you to consider a question about a topic before you learn about it. You can discuss the 'big' and other questions with family and friends, or talk with others in a [forum](#) on the CSI-COP website. You will need to register first at this link: <https://csi-cop.eu/citizenscientistlogin/>

You will have a chance to review your learning after each step and there will be activities to help you do this. You will find a look-back after the final step to review the whole course. Information will also be found at the end, after Step 5, on how to join the CSI-COP team to become citizen scientists investigating online privacy, and becoming a **privacy champion**.

Enjoy!



<p><b>CSI-COP MOOC: an Informal Education self-study course</b></p>	<p><i>Your Right to Privacy Online</i></p>
<p><b>Aims of the MOOC</b></p>	<p>CSI-COP's free online course is designed across <b>five steps</b>. Completing each step will provide you with the knowledge to make informed decisions about your right to privacy online. You will also gain skills that will help you to check for, and block tracking technologies across the Internet and in apps on your Android devices (e.g. Samsung mobile, or tablet). Once all five steps are completed, you can request a CSI-COP informal education certificate. You can then progress from an informal learner to becoming a volunteer citizen scientist joining the CSI-COP team to investigate the extent that your data is being tracked across the Internet (please see step 5). CSI-COP EU page: <a href="https://cordis.europa.eu/project/id/873169">https://cordis.europa.eu/project/id/873169</a></p>
<p><b>What you will learn (learning objectives)</b></p>	<ol style="list-style-type: none"> <li>1) Gain knowledge about privacy accorded under human rights charters</li> <li>2) Acquire practical skills (<i>know-how</i>) to uncover online tracking technologies embedded in websites and in Android Apps</li> <li>3) Discover how to become a citizen scientist and join the CSI-COP team to investigate the extent of online tracking through digital tracking technologies</li> </ol>
<p><b>Course duration</b></p>	<p>This course is designed to be completed in these ways:</p> <ul style="list-style-type: none"> <li>• All five steps in one session, including the informal learning and activities, in <b>2 ½ -3 hours</b></li> <li>• At your own pace.</li> </ul>
<p><b><u>Informal Education Details</u></b></p>	
<p><b>Title</b></p>	<p><i>Protecting your Data</i></p>
<p><b>Aims &amp; summary</b></p>	<p>This workshop is designed to be completed in half-a-day at one sitting. However, you can stagger the learning steps to suit your availability.</p> <p>In this online workshop you will gain a comprehensive understanding about the different aspects to privacy, and how this relates to the way your personal data might be used by third-parties in your online interactions on websites and using apps. You will learn about how to make informed decisions about your personal data and how to check for transparency in the way data is collected about you.</p>
<p><b>What you will learn - (learning outcomes)</b></p>	<p><b>Intended course learning outcomes</b></p> <ol style="list-style-type: none"> <li>1. Describe and discuss the different aspects of privacy.</li> <li>2. Identify and evaluate the way personal data is collected whilst navigating the web and using apps on smart devices.</li> <li>3. Understand the rights to privacy arising from charters to protect our data</li> </ol>
<p><b>Course content</b></p>	<ul style="list-style-type: none"> <li>• Privacy and its different aspects</li> <li>• What is personal data?</li> <li>• How is personal data collected through our Internet usage?</li> <li>• Rights to privacy (UN; EU; GDPR)</li> <li>• Protecting your data online.</li> </ul>



## Step 1

Step 1 Title:	<b>Different aspects to privacy</b>
Step learning outcome	1: Describe and discuss the different aspects of privacy.
Topic	Privacy and its different aspects
Big question	<i>Is privacy a privilege or a human right?</i>  Ask your family and friends what they think about <b>privacy</b> . You could post your views on CSI-COP website <a href="https://csi-cop.eu/forum/">forum</a> here: <a href="https://csi-cop.eu/forum/">https://csi-cop.eu/forum/</a> - you will need to register on the website before posting on the forum by creating a log-in here: <a href="https://csi-cop.eu/citizenscientistlogin/">https://csi-cop.eu/citizenscientistlogin/</a>
Short summary	Jan Holvast (2009): "Discussion on privacy issues is as old as mankind".  [Please see further reading section at the end of step 1]
Learning content	<p><b>Brief history of 'privacy'</b></p> <p>According to Jan Holvast (2009) "Discussion on privacy issues is as old as mankind. Starting with the <b>protection of one's body and home</b>, it soon <b>evolved</b> in the <b>direction of controlling one's personal information.</b>"</p>  <p>In 1890, Warren &amp; Brandeis wrote "That the individual shall have full protection in person and in property is a principle as old as the common law", and "in very early times, the law gave a remedy only for physical interference for life and property". They added that "now [in 1890] the right to life has come to mean ... the right to be let alone", and "the term 'property' has grown to comprise every form of possession – intangible, as well as tangible".</p> <p>In 2011 Nissenbaum informed that "The year 2010 was a big one for online privacy. Reports of privacy gaffes, such as those associated with Google Buzz and Facebook's fickle privacy policies, graced front pages of prominent news media. In its series "<b>On What They Know</b>," <i>The Wall Street Journal</i> aimed a spotlight at the rampant tracking of individuals for behavioral advertising and other reasons."</p> <p>In terms of the <i>ethics of privacy</i>, Marijn Sax (2018) "focuses on questions such as '<b>What is the value of privacy?</b>' and '<b>What privacy norms should be respected by individuals (including ourselves), society, and the state?</b>'"</p> <p>On 10 April 2022, British comedian John Oliver in his HBO show '<a href="#">Last Week Tonight</a>' called "attention on the harm by 'data brokers' who capture and put together our online 'digital data crumbs' to deanonymize us and sell our data to third-parties" (in the <a href="#">Guardian</a>, 11 April 2022). Oliver reported that data brokers are "part of a multi-billion dollar industry" that "collect your personal information and then resell or share it with others" with the "main tools are cookies,</p>



which enable websites to remember you and have evolved to include third-party cookies, which track where else you are going on the Internet". ([Guardian](#)). We will be returning to cookies in Step 3.

### Google Chrome

Some of you may use Google's Chrome browser *Incognito* mode to maintain your privacy. However, it appears that Google "secretly scoops up troves of internet data even if users browse in "Incognito" mode to keep their search activity private." (Nayak and Rosenblatt, 2021). A Bloomberg 2021 news item reports that "Consumers have filed a case as a "class action" alleging that "even when they turn off data collection in Chrome, other Google tools used by websites end up amassing their personal information" (Nayak and Rosenblatt, 2021). You can learn more about this case on Bloomberg's new site here: <https://bloom.bg/3gFt4vV>

### Facebook 533million user data breach

You may have heard the recent news that no matter how much we might try to keep our information somewhat private, if we use social media we are at the platform owner's disposal, and competence to secure our privacy. The **personal details of more than 530 million Facebook users were found available on a website for hackers in April 2021** (Holroyd, 2021). Personal information of the 533million include Facebook users in these countries:

- More than 35 million in Italy
- Over 32 million in the US
- Almost 20 million accounts in France
- 11 million users in the UK, and
- 6 million users in India.

Lomas (2021) reports that the data dump, of information that Facebook users have shared on this platform, includes:

- Facebook IDs
- Full names
- Phone numbers
- Locations
- Birthdates
- Bios, and
- Some email addresses

You can read more on [TechCrunch](#).

If you are a Facebook user and want to find out if your information is included in this Facebook data breach you can check either by your email, or using your Facebook ID, or phone number at these websites:

- [Have I been pwned?](#) Here: <https://haveibeenpwned.com/>
- [Have I been Zucked?](#) Here: <https://haveibeenzucked.com/>

You can also follow the tweets of [The Real Facebook Oversight Board](#) "holding Facebook to account" on Twitter here: <https://twitter.com/FBOversight>

You may have heard the name [Frances Haugen](#). She is a data scientist and former employee of Facebook. Haugen gave testimony to the US Senate on 5 October 2021, to the UK



parliament on 25 October 2021, and to the European parliament on 8 November 2021. Haugen exposed Facebook's profit strategy over user welfare. Read more about Frances Haugen's advocacy for "accountability and transparency in social media" on her website: <https://www.franceshaugen.com/>).

The [Irish Data Protection Commission](#) "imposed a fine of 17million Euros on Meta Platforms Ireland Limited over a series of data breaches between 7 June 2018-4 December 2018" (from here: <https://bit.ly/3MmUIKN>).

Christopher Wylie, former data scientist at Cambridge Analytica and author of the 2019 book 'MindF\*ck: Inside Cambridge Analytica's Plot to Break the World' states: "Facebook has too much unchecked power" (page 225).

In 2021, the US District Court Southern District of New York placed a civil action: Google Digital Advertising Antitrust. Paragraph 175 on page 64 of the US court document states: "Google presents a public image of caring about privacy, but behind the scenes Google coordinates closely with the Big Tech companies to lobby the government to delay or destroy measures that would actually protect users' privacy" (from Civil Action No.: 1:21-md-03010-PKC document accessible from [courtlistener.com](https://www.courtlistener.com) ).

Carissa Veliz, author of the 2020 book 'Privacy is Power' warns:

- "The Internet is primarily funded by the collection, analysis and trade of data ... the data economy" (page 1)
- "Much of that data is personal data – data about you" (page 1)
- "... smart phone .... Recording your journey and how long you stayed...." (page 2)
- " The data economy, and the ubiquitous surveillance on which it feeds, took us by surprise" (page 2)

### Rethinking Privacy: Location data?

- Where I am now + activity/context/SSID (WiFi name)
- Where I am not (normally)?
- Where I am heading?
- Where I have been?
- Which route have I travelled?
- Which way I am facing / what is my elevation?
- People and things I am connected to?



privacy   
matters

### What to look forward to in the next steps

In the following step (Step 2) we will start to look *data* and *personal data*.

In Step 3 we will look at *how our data is tracked*.

In Step 4 we will look at what *rights we have to our privacy*

In the final step in this course, Step 5, we will learn about *online tools* we can use to better *secure our privacy and protect our data*.

### Review your learning

Please review what you learnt in step 1 with a question and two activities next.



Review your learning	What is <i>privacy</i> ?
Activities	<p><b>Activity 1</b> Is the statement below true or false?</p> <p>'The discussion on privacy is new, since the invention of Facebook'.</p> <p><b>Activity 2:</b> Discuss the concept of privacy with your family, friends, neighbours, or colleagues.</p> <p>What did you learn about your own understanding of privacy, and other people's perspective on privacy?</p> <p>Reminder: you can post your views on CSI-COP website <a href="https://csi-cop.eu/forum/">forum</a> here: <a href="https://csi-cop.eu/forum/">https://csi-cop.eu/forum/</a> - you will need to register on the website before posting on the forum by creating a log-in here: <a href="https://csi-cop.eu/citizenscientistlogin/">https://csi-cop.eu/citizenscientistlogin/</a></p>
Activity purpose	Gain an understanding on different <i>aspects to privacy</i> .
Short Tweet	Should convenience matter more than privacy in the age of mobile access to the Internet?

<b>Further Reading for Step 1</b>	<p>Links for further reading mentioned in Step 1 can be found by selecting the underlined text below:</p> <p><b>Recommended</b></p> <p>Lomas, N. (2021). <i>Answers being sought from Facebook over latest data breach</i>. Tech Crunch Accessible from here: <a href="https://tcrn.ch/3xfrTsE">https://tcrn.ch/3xfrTsE</a></p> <p>Nayak, M. and Rosenblatt, J. (2021). <i>Google Must Face Suit Over Snooping on 'Incognito' Browsing</i> Bloomberg Technology. Accessible from here: <a href="https://bloom.bg/3gFt4vV">https://bloom.bg/3gFt4vV</a></p> <p>The Real Facebook Oversight Board Twitter account @FBoversight accessible here: <a href="https://twitter.com/FBoversight">https://twitter.com/FBoversight</a></p> <p><b>Additional</b></p> <p>Holroyd, M. (2021). Ireland launches data protection inquiry into Facebook hack. <i>Euronews – Ireland</i>. Accessible from here <a href="https://bit.ly/3mOfIOM">https://bit.ly/3mOfIOM</a></p> <p>Holvast, J. (2009). History of Privacy. In V. Matyáš et al. (Eds.): <i>The Future of Identity</i>, IFIP AICT 298, pp. 13–42, 2009. IFIP International Federation for Information Processing 2009. Available from ResearchGate: <a href="https://www.researchgate.net/publication/225802214_History_of_Privacy">https://www.researchgate.net/publication/225802214_History_of_Privacy</a></p> <p>Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. <i>Dædalus, Journal of the American Academy of Arts &amp; Sciences</i>, Vol 140, No. 4 (Fall 2011), pp. 32-48. Accessible from here: <a href="https://www.amacad.org/publication/contextual-approach-privacy-online">https://www.amacad.org/publication/contextual-approach-privacy-online</a></p> <p>Guardian (2022). <i>John Oliver on Data Brokers: What they can buy is pretty troubling</i>. Guardian Culture. 11 April 2022: <a href="https://bit.ly/3wzX0j3">https://bit.ly/3wzX0j3</a></p> <p>Sax, M. (2018). Privacy from an Ethical Perspective. Chapter in B. Van der Sloot &amp; A. De Groot (Eds.), <i>The Handbook of Privacy Studies: An Interdisciplinary Introduction</i> (pp. 143-173). Amsterdam:</p>
-----------------------------------	--



Amsterdam University Press. Accessible from this link:  
[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3299047](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3299047)

Warren, S.D. & Brandeis, L.D. (1890). The Right to Privacy. *Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220. Accessible from: [The Right to Privacy on JSTOR](#)



## Step 2

Step 2 Title:	<b>Data and personal data</b>
Step learning outcome	1: Describe and discuss the different aspects of privacy.
Topic	What is personal data?
Big question	<p><i>Why should I care who has access to my data, I've nothing to hide?</i></p> <p>Ask your family and friends what they think about their data. You could post your views on CSI-COP website <a href="https://csi-cop.eu/forum/">forum</a> here: <a href="https://csi-cop.eu/forum/">https://csi-cop.eu/forum/</a> - you will need to register on the website before posting on the forum by creating a log-in here: <a href="https://csi-cop.eu/citizenscientistlogin/">https://csi-cop.eu/citizenscientistlogin/</a></p>
Short summary	<p>Andreas Weigend (2017): "Every time we Google something, Facebook someone, Uber somewhere, or even just turning on a light, we create data that businesses collect".</p> <p>[Please see further reading section at the end of step 2]</p>
Learning content	<p><b>What is data?</b></p> <p>Recap: in step1 we were introduced to the concept of 'privacy'</p> <p>In step 2 of CSI-COP's informal education course you will come to understand 'what data is', and 'what data about you' is involved in different aspects of your online life: from shopping online to messaging friends, to searching for information.</p> <p>The singular form of 'data' is datum:</p> <ul style="list-style-type: none"> <li>a single piece of <i>quality</i> or <i>quantity</i> about something</li> </ul> <p>Data is the plural (more than a single item):</p> <ul style="list-style-type: none"> <li>Information points, for example <i>data about you</i> such as</li> </ul> <p>If you are a student, whether you are a 'home' or International student</p> <p>Date of birth</p> <p>Qualifications to achieve a place at university</p> <p>Home address, term-time address</p> <p>Contact number</p> <p>Data is everywhere and is held in many forms:</p> <ul style="list-style-type: none"> <li><i>Unstructured:</i></li> </ul> <p>Consider YouTube videos</p> <p>Examine Instagram images</p> <p>Read emails</p> <p>Satellite images</p>



Weather data

- Structured:

Student/Staff ID number – string of numbers

NHS or Social security number

Airlines reservations

	Structured Data	Unstructured Data
Characteristics	<ul style="list-style-type: none"><li>• Pre-defined data models</li><li>• Usually text only</li><li>• Easy to search</li></ul>	<ul style="list-style-type: none"><li>• No pre-defined data model</li><li>• May be text, images, sound, video or other formats</li><li>• Difficult to search</li></ul>
Resides in	<ul style="list-style-type: none"><li>• Relational databases</li><li>• Data warehouses</li></ul>	<ul style="list-style-type: none"><li>• Applications</li><li>• NoSQL databases</li><li>• Data warehouses</li><li>• Data lakes</li></ul>
Generated by	Humans or machines	Humans or machines
Typical applications	<ul style="list-style-type: none"><li>• Airline reservation systems</li><li>• Inventory control</li><li>• CRM systems</li><li>• ERP systems</li></ul>	<ul style="list-style-type: none"><li>• Word processing</li><li>• Presentation software</li><li>• Email clients</li><li>• Tools for viewing or editing media</li></ul>
Examples	<ul style="list-style-type: none"><li>• Dates</li><li>• Phone numbers</li><li>• Social security numbers</li><li>• Credit card numbers</li><li>• Customer names</li><li>• Addresses</li><li>• Product names and numbers</li><li>• Transaction information</li></ul>	<ul style="list-style-type: none"><li>• Text files</li><li>• Reports</li><li>• Email messages</li><li>• Audio files</li><li>• Video files</li><li>• Images</li><li>• Surveillance imagery</li></ul>

Above image from here: <https://bit.ly/2PhkKHh>

From Irwin (2021): “Under certain circumstances, any of the following can be considered *personal data*.”:

A name and surname

A home address

An email address

An identification card number

Location data

An Internet Protocol (IP) address

The advertising identifier of your phone

**Personal data is data that identifies a “natural” (living) person.**





Pat Walshe of '**Privacy Matters**' says: "We use our smartphones and computers like never before to make calls, send personal texts and pictures, message people via services WhatsApp or Snapchat, shop online for food or medicines, to share personal bits of our lives on social media, search for information on mental or physical health, politics, religion or places to visit, to browse websites, leave feedback and indicate our likes and dislikes. Being digital creates a wealth of data about us often personal and sensitive. Data that may let others know us better than we know ourselves" ([Privacy Matters](#)).

We may **volunteer data** when we place an order online or book a health appointment. Data may be **captured and observed** about us and our devices and our online behaviour (such as the websites we visit, the songs we listen to or movies we watch, the kind of device we use, our locations - whether we realise it or not). Data may be **inferred** from profiling us and analysing information about us (such as which username listened to a song or watched a movie online, the category of the song or movie, at what point a person paused a song or a movie, together with date and time when they paused and restarted or abandoned listening or watching, the location they were in (at least the country) – data that's kind of like a digital shadow of activities online ([Privacy Matters](#)).

In addition to personal data. There is also **sensitive personal data**. Under the general data protection regulation (GDPR) which we will learn more about in step 4, **sensitive personal data** under the GDPR, can include data that reveals your:

- racial or ethnic origin
- religious beliefs
- political opinions
- trade union memberships.

Sensitive personal data also includes data about a person's health (mental or physical for example); data concerning an individual's sex life or sexual orientation; genetic data; biometric data (used to uniquely identify someone) and data relating to criminal convictions and offences ([Privacy Matters](#)).

Brodkin (2021) reported in April 2021 that T-Mobile will:

"... begin a new program that uses some data that we have about you"  
"including information we learn from your web and device usage data (like the apps installed on your device)"  
"and interactions with our products and services for our own and 3<sup>rd</sup> party advertising unless you tell us not to".

How do you feel if your mobile phone provider informed you that they would act like T-Mobile? Or if you use T-Mobile, how does their statement make you feel about their collection and use of your data?



# Digital YOU

## Technical Identifiers

- Cookie IDs
- Mobile Advertising ID
- TV advertising identifier
- IP address
- Device identifiers (Bluetooth, WiFi, mobile serial number, IMEI)

## Technical information

- Device info – Model, OS
- Connection (WiFi, wired, mobile carrier)
- Location (GPS/WiFi/IP)
- User agent – identifies the browser type, phone model and OS version



What you 'browse'

What you search for

What you listen to

What you watch

What you read

Location – precise  
to approximate



## What to look forward to in the next steps

In the following step (Step 3) we will start to *look how our data is tracked*.

In Step 4 we will look at what *rights we have to our privacy*

In the final step in this course, Step 5, we will learn about *online tools* we can use to better *secure our privacy and protect our data*.

## Review your learning

Please review what you learnt in step 2 with a question and two activities next.

Review your learning

What is *personal data*?

Activities

### **Activity 1: short test**

Which of the below names relate to personal data?

- Leonardo da Vinci
- President Joe Biden
- Freddie Mercury
- Queen Elizabeth II
- Alan Turing
- Meghan Markle
- Albert Einstein
- The Pope
- Kim Kardashian

The answer to Step 2 Activity 1 will be provided in Step 3.

### **Activity 2**

Search for and watch TED talks for example, Tech-sociologist, **Zeynep Tufekci's** TED Global NYC talk, September 2017:

**'We're building a dystopia just to make people click on ads'.**



	Reminder: you can post your views your learning on CSI-COP website <a href="https://csi-cop.eu/forum/">forum</a> here: <a href="https://csi-cop.eu/forum/">https://csi-cop.eu/forum/</a> - you will need to register on the website before posting on the forum by creating a log-in here: <a href="https://csi-cop.eu/citizenscientistlogin/">https://csi-cop.eu/citizenscientistlogin/</a>
Activity purpose	Understand <i>what personal data is</i> .
Short Tweet	The statement: "I have nothing to hide so I don't care who has access to my data" is misguided

<b>Further Reading for Step 2</b>	<p>Links for further reading mentioned in Step 2 can be found by selecting the underlined text below:</p> <p><b>Recommended</b>  Brodkin, J. (2021). <i>T-Mobile will sell your web-usage data to advertisers unless you opt out</i>. arsTECHNICA. Accessible from here: <a href="https://bit.ly/3sUdkaQ">https://bit.ly/3sUdkaQ</a></p> <p>Irwin, L. (2021). <i>Personal data vs. sensitive data: what's the difference?</i> IT Governance. Accessible from here: <a href="https://bit.ly/3vhoRIX">https://bit.ly/3vhoRIX</a></p> <p>Privacy Matters on Twitter: @PrivacyMatters: <a href="https://twitter.com/privacymatters?lang=en">https://twitter.com/privacymatters?lang=en</a></p> <p><u>Book that might be held in your local library</u>  Weigend, A. (2017). <i>Data for the people: how to make our post-privacy economy work for you</i>. Basic Books: New York</p>
-----------------------------------	--



### Step 3

Step 3 Title:	<b>Online Tracking Technologies</b>
Step learning outcome	<p>1: Describe and discuss the different aspects of privacy.</p> <p>2. Identify and evaluate the way personal data is collected whilst navigating the web and using apps on smart devices</p>
Topic	How is personal data collected through our Internet usage?
Big question	<p><i>What harm can online tracking technologies do?</i></p> <p>Ask your family and friends what they think about their data. You could post your views on CSI-COP website <a href="https://csi-cop.eu/forum/">forum</a> here: <a href="https://csi-cop.eu/forum/">https://csi-cop.eu/forum/</a> - you will need to register on the website before posting on the forum by creating a log-in here: <a href="https://csi-cop.eu/citizenscientistlogin/">https://csi-cop.eu/citizenscientistlogin/</a></p>
Short summary	<p>Nigel Warburton (2020): “Without your permission ... tech companies are harvesting your data – your location, your likes, your habits, your fears, your diseases, your politics – and sharing it amongst themselves”.</p> <p>[Please see further reading section at the end of step 3]</p>
Learning content	<p><b>How information is collected about you across the Internet</b></p> <p>To recap what we learnt in the previous two steps:</p> <ul style="list-style-type: none"> <li>• In step1 we were introduced to the concept of ‘privacy’</li> <li>• In step2 we learnt that ‘personal data’ refers to a natural (living) person</li> </ul> <p>In this step we will learn about the different online tools that collect data as we use the Internet.</p> <p>Product Manager, Eliza Crawford (2020) informs us that <b>the reason data is collected on you</b> across the Internet is <b>to learn how you behave when you visit a website</b>. This is to <b>“gain insights about how ... customers use” websites “to provide a personalised online experience, and to monetise the user by showing them targeted adverts.”</b></p> <p>Explaining why online tracking occurs, Crawford (2020) says:</p> <ul style="list-style-type: none"> <li>• “When you search for a restaurant on Google and the service provides you with a list of restaurants in your local area, it’s because the search engine knows where you are based.”</li> <li>• “When an e-commerce store shows you a list of recommended products, it knows what you like because it has tracked items you looked at or bought previously.”</li> </ul> <p>Pat Walshe (Privacy Matters) reminds us that <b>behavioural data</b> may include:</p> <ul style="list-style-type: none"> <li>• your <b>web browsing</b> data – the websites you visit, the date and time you visit, the country you visited from (inferred from your IP address - a unique string of characters that identifies each device connecting to the internet and that is automatically sent when you visit a website). Also consider that when you leave a website, they’ll be able to tell which site you are visiting next and the next website you visit may be able to tell which website you came from. All of this would be considered web browsing behavioural data.</li> </ul>



- **'clickstream behaviour'** – data about an individual's interactions on a website, that can include what they click and scroll and tap on a touch screen
- **'search engines'** such as Google that may collect and use information about what you search for, what results you click on, your IP address, and that may use a unique cookie identifier to track you.
- **location** – the location and type of place you visit (supermarket, casino, place of worship, hospital), or where you used an app, the dates and times, route travelled, the frequency of a visit or the routes you travel. Location data can be very [revealing](#) and behavioural in nature.
- **purchase history** – this can include types of subscriptions (trade union membership, gym, newspapers etc), hotel or restaurant reservations that may have been made across [search, maps, smart assistants](#) or directly from retailers or third party services etc.
- **payment or 'transactional' data** – payments that reveal who/what organisation you paid (which can reveal the type of organisation - medical clinic, pharmacy, alcohol provider; food retailer, bookseller etc) and how much and when and how often. Tap and go card payments are a good example – think of that coffee you purchase at the start of a journey, the place, date and time you paid for it, and then payments you make later in the day with the same card.
- **streaming media** – ["you are what you stream"](#) and ["They know what You Watched Last Night"](#). Streaming media generates **a lot** of behavioural data about:
  - the date and time you accessed a streaming music, audio or TV/movie service and non-precise location (country level or region level) you accessed it from
  - which profile accessed and used the service (a name + category e.g. child)
  - the category of music, audio book, TV/movie (e.g. political horror, adult)
  - searches for content
  - whether you paused a song or movie and for how long (including the date(s) and time(s))
  - whether you skipped/abandoned a song or a TV episode movie audio track
  - whether you shared content and who with and your interactions with others within the service
  - whether you rated a song, TV show or movie
  - playlists or 'watch' lists you create
  - the device used to access the service and IP address and device identifiers
- **Activity/Health data** – data about your use of activity apps such as cycling, running, walking or data about your health such as that obtained via dietary or fertility apps. This data can be very revealing and may often be connected with your location for example.
- **Social media graph** – data revealing interconnected social relationships between people and their nature and patterns of communications

A study by Ghostery (2017) "revealed that trackers that collect data on internet users' online behavior are present on at least 79 percent of websites (unique domains) globally. Web tracking has become so pervasive that approximately ten percent of websites send the data they've collected to ten or more different companies (unique tracker domains). In terms of web traffic, 15 percent of all page loads on the internet are monitored by *ten or more* trackers. According to the study, tracking scripts from Google (60.3 percent of page loads) and Facebook (27.1 percent) are the most prevalent".





This tracking is done through digital tools.

We heard about cookies in Step1, from John Oliver's 10 April 2022 HBO show '[Last Week Tonight](#)' exposing Data Brokers.

**Cookies:** Cookies are small pieces of data that websites store on the user's device. Sites often **use cookies to remember user preferences** and **deliver a personalized experience, as well as to gain information for advertising**. Once a website has dropped a cookie on a user's computer, the cookie provider can continue to access it. This is how sites can use cookies to track users from page-to-page or from site-to-site. How long a cookie can track a user depends on the type of cookie. For example, Sessional, Persistent, First-party; Third-party (Crawford, 2020).

**Fingerprinting:** Fingerprinting is a form of website tracking that **uses the attributes of the user's device or browser to build a profile of a user**. Information fingerprinters use include your device, the operating system you have on the device, screen resolution, browser and browser version, language, and time zone. Crawford (2020) states: "On its own, each piece of information isn't that valuable. However, when it is all put together, it provides an incredibly accurate way to identify users. The **Electronic Frontier Foundation (EFF)** runs a site '[cover your tracks](#)' that tests your browser to show how unique your fingerprint is in relation to others the site has tracked."

**Email tracking:** Email tracking **software places an invisible image pixel in your emails that can detect the exact time and date you opened an email**. The reason for email tracking is so that companies/retailers, etc., save time and learn whether a company's first email was interesting enough to you to open. If not, you might be unlikely to open future follow-up emails. By preventing unnecessary follow-up emails, email tracking saves time both for the sales rep and the email recipient. Similarly, if a company notices a contact is clicking on the links sent and viewing a cover letter or a proposal that was attached, the company knows that you're currently at the top of their minds. Reaching out to you at that point, when you're thinking about a company's proposal, say (e.g. purchase an item of clothing) makes the conversation much more relevant, and timely for the company/retailer.

Sivan-Sevilla et al.'s (2020) study found that "companies we may never have heard of are collecting data points on every aspect of our lives – our interests, purchases, health condition, locations, and more". IAB (2019, quoted in Sivan-Sevilla et al., 2020) "These data points are then combined into exceptionally revealing behavioral profiles, exposing intimate parts of our identity and fuel the multi-billion-dollar advertising industry that claims to predict what we are likely to .consume in order to target us with ads".

Sivan-Sevilla et al.'s (2020) further report that when advertisers cross information about users' medical problems, educational interests, and news consumption habits they are in a position to better know when a user can be turned into a consumer and make purchasing decisions that advertisers would not be able to predict otherwise. Studies showed how data from different websites is aggregated and used to infer about the demographics and interests of users, exposing them to manipulative practices that try to make them click on the 'right' (personalized) advertisement at the 'right' (personalized) time ... The advertising industry had



defined these moments as **'prime vulnerability moments of consumers'** ...in which users are 'uniquely receptive' ...".

Srinivasan (2020) enlightens that: "The rise of electronic ad trading, widely known today as "programmatic advertising," paralleled the rise of electronic trading across various sectors of the economy.... early advertising technology company **Right Media** launched the **RMX** "advertising exchange," the **first-ever electronic trading venue for ads**. .... Today, a single company, **Google**, simultaneously operates the leading exchange, as well as the leading middlemen (i.e., intermediaries) that publishers and advertisers must use to trade ... Google not only sells ad space belonging to third-party websites, it sells ad space appearing on its own sites, Google Search and YouTube".

Srinivasan (2020) reports that "The business of advertising has changed drastically over the last two decades. Today, the largest category of advertising, online advertising, is rarely negotiated by people at all. Advances in technology allow ad space to be bought and sold electronically through centralized trading venues at high speeds, without people ever meeting face-to-face. When a user visits a website, the ad space on a page is instantly routed into one or more of these venues. There, the space is auctioned in real-time to the highest bidder. At the conclusion of these auctions, the advertisers' ads return and display to the user in time for the page to load and before the user has noticed anything has occurred. The user just sees ads targeted to them, say one for Barclays bank."

You may now understand that a lot of data is increasingly captured, observed and inferred by those you have a direct relationship with, not just to provide basic services you request, but increasingly to 'personalise experiences' whether you ask for them to or not and/or to target you with advertising on and off their websites, apps and services. But your data isn't just captured, observed and inferred by those you have a direct relationship with, but also with third party entities in the advertising ecosystem who may be embedded in the websites you visit or the apps you use, in order to target you with [behavioural advertising](#) for example. Your data may be used to follow you around the web and apps for behavioural targeting purposes such as [real-time bidding](#) that allows advertisers to automatically bid in real time to target people based on specific criteria – for example, of a specific age range and gender or type of mobile device or location.

So, data about YOU can be very personal indeed revealing intimate aspects of your life. It can impact in ways that you never considered and that breaches your expectations to privacy and that fails to respect and protect your privacy. For example, the Grindr app was [found](#) to share information with a "large number of third parties" involved in profiling and advertising. Data shared "included IP address, Advertising ID, GPS location, age, and gender." This led to an investigation by the Norwegian data protection authority who [fined](#) Grindr the equivalent of £8.6 million (100 million krone).

All of the data types of discussed above are personal data protected by data protection laws such as the GDPR and the EU's electronic privacy law (the [ePrivacy Directive](#) 'ePD') we'll discuss in the next step (step 4) of CSI-COP's informal learning course. These laws place obligations on private and public sector organisations that capture, observe and infer data about you and give rights over that use. Again, this will be discussed in Section 4 of the course.

But take a moment and think about what your data says about YOU and OTHERS that you're connected to.

Do also note, if you use 'free' Wifi, you have to provide information about you to access the Internet. See the image below on what is collected.



# 'Free' Wifi

## Account Information

- Name
- Date of birth
- Gender
- Postal address
- Mobile phone number
- Email address
- Device MAC identifier



## Usage Information

- such as the time and hotspot location where you used the WiFi
- other service-related data including your IP address and information about your device

## Memorable data

- Name of first pet
- Mother's maiden name
- Favourite place

Free WiFi (and our advertising partners) may use your account and usage information to provide you with tailored advertising, including by using cookies. If you'd like more information or to change this please click Free WiFi Advertising Choices below.

- Free WiFi (and its advertising partners) may use my data to provide me with tailored advertising.
- Free WiFi may share my personal data with TV Limited so that the TV Limited adverts I see are more relevant to me.



## What to look forward to in the next steps

In the following step (Step4) we will look at what *rights we have to our privacy*  
 In the final step in this course, Step 5, we will learn about *online tools* we can use to better *secure our privacy and protect our data*.

## Review your learning

Please review what you learnt in step 3. The answer to Step 2-Activity 1 can be found with two activities for this step.

Review your learning

What are the different types of cookies?  
 What is digital fingerprinting?  
 How does email tracking work?

Activities

## **Answer to Step2 Activity 1**

Activity 1 in Step2 asked you to identify personal data from a list of names. As personal data relates to natural (living) people only. For the people in the list who are no longer alive, their names are not personal data. Did you guess right? Check below:

- Leonardo da Vinci – not personal data
- President Joe Biden
- Freddie Mercury – not personal data
- Queen Elizabeth II
- Alan Turing – not personal data
- Meghan Markle
- Albert Einstein – not personal data
- The Pope
- Kim Kardashian

'The Pope' is an interesting one: if you picked this because you felt it relates to the current living pope then you are correct.

## **Step 3 Activity 1**

1. Search on the web to find the different types of cookies that can be embedded in websites
2. What is the difference between fingerprinting and email tracking?



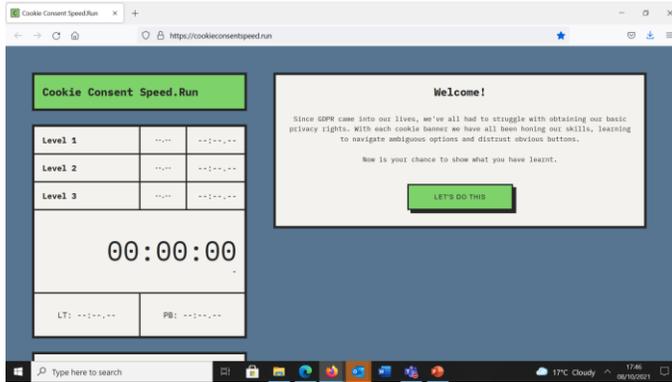
### Step 3 Activity 2

With family, friends, neighbours, or colleagues discuss what you understand by '**online behaviour profiling**' and how it is operated across the web.

### Step 3 Activity 3

Try this free online game to find if you can avoid cookies:

<https://cookieconsentspeed.run/>



Reminder: you can post your views your learning on CSI-COP website [forum](https://csi-cop.eu/forum/) here: <https://csi-cop.eu/forum/> - you will need to register on the website before posting on the forum by creating a log-in here: <https://csi-cop.eu/citizenscientistlogin/>

Activity purpose

Learn about online behaviour profiling.

Short Tweet

Tracking technologies

### Further Reading for Step 3

Links for further reading mentioned in Step 3 can be found by selecting the underlined text below:

#### Recommended

Crawford, E. (2020). Website Tracking: Why and How do Websites Track you? CookiePro Blog: Cookie Compliance. Accessible from here: <https://www.cookiepro.com/blog/website-tracking/>

EFF (no date). The Electronic Frontier Foundation. The leading non-profit defending digital privacy, free speech, and innovation [for 30 years and counting!](https://www.eff.org/) Accessible from here: <https://www.eff.org/>

Ghostery (2017). 79 Percent of Websites Globally Are Secretly Tracking Your Personal Data. Ghostery. Accessible from here: <https://www.ghostery.com/press/ghostery-global-tracking-study/>

Privacy Matters on Twitter: @PrivacyMatters: <https://twitter.com/privacymatters?lang=en>

#### Further reading

Sivan-Sevilla, I., Chu, W., Liang, X. and Nissenbaum, H. (2020). Unaccounted Privacy Violation: A Comparative Analysis of Persistent Identification of Users Across Social Contexts. Federal Trade Commission (FTC) PrivacyCon 2020. Paper available on line via this link: <https://news.cornell.edu/stories/2020/06/study-online-trackers-follow-health-site-visitors>



Srinivasan, D. (2020). Why Google Dominates Advertising Markets Competition Policy Could Lean on the Principles of Financial Market Regulation. 24 STAN. TECH. LAW REV. Accessible from here: <https://law.stanford.edu/publications/why-google-dominates-advertising-markets/>

Warburton, N. (2020) inside cover of book by Véliz, C. (2020). Privacy is Power: Why and how you should take back control of your data. Penguin Hardback.



## Step 4

Step 4 Title:	<b>Your Rights to Privacy</b>
Step learning outcome	<p>1: Describe and discuss the different aspects of privacy.</p> <p>2. Identify and evaluate the way personal data is collected whilst navigating the web and using apps on smart devices.</p> <p>3. Understand the rights to privacy arising from charters to protect our data.</p>
Topic	Rights to privacy: UN Charter on Human Rights; EU Charter on Human Rights; GDPR
Big question	<p><i>What rights do I have to privacy?</i></p> <p>Ask your family and friends what they think about their rights to privacy. You could post your views on CSI-COP website <a href="https://csi-cop.eu/forum/">forum</a> here: <a href="https://csi-cop.eu/forum/">https://csi-cop.eu/forum/</a> - you will need to register on the website before posting on the forum by creating a log-in here: <a href="https://csi-cop.eu/citizenscientistlogin/">https://csi-cop.eu/citizenscientistlogin/</a></p>
Short summary	Charters and regulations that include human right with respect to privacy.
Learning content	<p><b>Human right to privacy</b></p> <p>To recap what we have learnt so far:</p> <ul style="list-style-type: none"> <li>• In step1 we were introduced to the concept of 'privacy'</li> <li>• In step2 we learnt that 'personal data' refers to a living person</li> <li>• In step3 we learnt about some of the ways our data can be captured online (e.g. though cookies)</li> </ul> <p>In this step we will explore 'human rights'.</p> <p>Pat Walshe, of <a href="#">Privacy Matters</a> reminds us that “human rights have long mattered. From as far back as <a href="#">1689</a>, in Britain for example, human rights were considered something essential to being human, to our dignity and to protecting basic rights and freedoms (British Library, 2013). Rights and freedoms that today shape different dimensions of our lives – offline and online. From the right to express opinions, to the right to freely associate with others and to the freedom of assembly, to the freedom of religion, to the right to education, to the right to a fair trial, to the right to marry, and to the <b>right to privacy</b>, for example. Human rights matter. Everyday. Offline and online. They allow us to flourish as human beings.”</p> <p>Human rights in more modern times took on global importance in <b>1948</b>. In response to atrocities committed during the second world war, the United Nations General Assembly adopted the <a href="#">Universal Declaration of Human Rights (UDHR)</a> to protect basic human rights that all people should have. This includes protection against arbitrary interference with an individual's <b>privacy, family, home</b> or <b>correspondence</b> as per Article 12 of the UDHR.</p> <p>In 1949, a number of European countries formed the <a href="#">Council of Europe (CoE)</a> and that currently unifies 47 European member states. In <b>1950</b>, the Council of Europe adopted the <a href="#">European Convention on Human Rights (ECHR)</a>, again to protect us in the future, against atrocities like those committed during the second world war. The ECHR incorporates key rights found in the UDHR and entered into force in <b>1953</b>. The ECHR is the first <b>international</b></p>



**legally binding** instrument protecting human rights. Of note is that all member states of the European Union (EU) have [acceded](#) to the ECHR.

Article 8 of the ECHR provides that everyone has the right to respect for their **private** and **family life** and their **home** and **correspondence**. It's easy to see how such a right is intended to protect intimate aspects of a person's life. Aspects that are easy to observe online.

While Article 8 of the ECHR protects the right privacy it also includes the right to data protection, given that the use of personal information about people not only impacts on their privacy, but also other rights and freedoms, as this course will touch on. To help protect individuals and their rights and freedoms and in particular the right to privacy, in 1981 the **CoE** adopted a set of principles and rules that apply to the processing of personal information about individuals. The principles and rules are known as Convention 108. The Convention was recently modernised to reflect changes in technology and data use that may adversely impact people's rights. It is now known as [Convention 108+](#)

In **2000** the EU established the EU [Charter of Fundamental Rights](#). The charter became legally binding on member states of the EU in 2009. Like the ECHR, the EU Charter of Fundamental Rights (**EU CFR**) provides that everyone has the right to respect for their **private** and **family life, home** and **communications** (Article 7). Additionally, the **EU CFR** also provides that everyone has the right to the protection of their personal data (Article 8).

Article 7 and 8 of the EU CFR respectively provide a right to privacy and data protection as two distinct rights. These rights are given effect by an **ePrivacy instrument** known as the EU [ePrivacy Directive](#) (that applies to things like cookies and other online tracking techniques) and by a data protection instrument, the EU [General Data Protection Regulation \(GDPR\)](#). EU [data protection rules](#) and those of the **CoE** have been implemented in member state law and have been strengthened to reflect changes in technology and changes in data use. Today, when people use their mobile phones or laptops etc, data can be gathered about people in real-time and shared between hundreds of third-party advertisers for example, often in ways without people being genuinely aware or having any meaningful choices. Data that can reveal aspects of a person's private life, such as their locations, their shopping habits, the websites they visit, who their contacts are, and their social connections.

The UK Information Commissioner's Office (ICO): "The 2018 general data protection regulation (GDPR) **provides individuals with the right to be informed about the collection and use of their personal data. This is a key transparency requirement**" – explained on the [ICO's website](#) here: <https://bit.ly/2QxmZH1>

Pat Walshe of Privacy Matters states: "A right to privacy and data protection are more important than ever as our digital data reveals deeply personal and intimate aspects of ourselves and those we are connected to."





What to look forward to in the next step

In the final step in this course, Step 5, we will learn about *online tools* we can use to better *secure our privacy and protect our data*.

Review your learning

Please review what you learnt in step 4 with a mini quiz in the Activities section.

Review your learning

**1948 Universal Declaration of Human Rights (UDHR): Article 12:** “No one shall be subjected to arbitrary interference with his [her] privacy ... [or] correspondence”.

**2000 EU Charter of Fundamental Rights (ECHR): Article 1:** “Human dignity is inviolable. It must be respected and protected”.

**2018 General Data Protection Regulation (GDPR) “sets a high standard for consent”:**  
This *informed* consent entails:

- “offering individuals real choice and control”
- “genuine consent should put individuals in charge, build trust and engagement”.

Activities

**Mini quiz** from the different charters and regulations.

Are the following statements true or false?

- The UNHR is a new regulation granting informed consent.
- The EPrivacy Directive concerns cookies
- The GDPR is not concerned with transparency.

Discuss your answers with family, friends, neighbours, or colleagues.

Reminder: you can post your views on your learning on CSI-COP website [forum](https://csi-cop.eu/forum/) here: <https://csi-cop.eu/forum/> - you will need to register on the website before posting on the forum by creating a log-in here: <https://csi-cop.eu/citizenscientistlogin/>

Activity purpose

Discuss with your friends, family and neighbours, the 1999 statement from Sun Microsystems CEO and co-founder, Scott McNealy:  
**“You have zero privacy anyway .... Get over it!”**  
 Quoted in Wired:  
<https://www.wired.com/1999/01/sun-on-privacy-get-over-it/>

Short Tweet

Online privacy is not a luxury



**Further Reading for Step 4**

Links for further reading mentioned in Step 3 can be found by selecting the underlined text below:

**Recommended reading**

British Library (2013). Taking Liberties: The struggle for Britain's freedoms and rights. Taking Liberties – Star Items Index – Human Rights. Accessible from here: <https://bit.ly/2QU4bSa>

ICO (no date). Guide to the General Data Protection Regulation (GDPR): Right to be informed. UK Information Commissioner's Office (ICO). Accessible from here: <https://bit.ly/3erd79K>

**Further reading**

EHCR (no date ). European Convention on Human Rights. Accessible from here: <https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=>

ePrivacy Directive (2002). 32002L0058 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Accessible in English from here: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN>

GDPR (2016). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Accessible in English from here: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN>

UN (no date). United Nations Declaration of Human Rights. Accessible from here: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>



## Step 5

Step 5 Title:	<b>How to protect your data online</b>
Step learning outcome	<p>1: Describe and discuss the different aspects of privacy.</p> <p>2. Identify and evaluate the way personal data is collected whilst navigating the web and using apps on smart devices.</p> <p>3. Understand the rights to privacy arising from charters to protect our data.</p>
Topic	Tools to protect your data online.
Big question	<p><i>How do I change app and web browsing settings to stop online tracking?</i></p> <p>Once you come to know, do tell your family and friends about the tools that can help them protect their data online . You could post your views on CSI-COP website <a href="#">forum</a> here: <a href="https://csi-cop.eu/forum/">https://csi-cop.eu/forum/</a> - you will need to register on the website before posting on the forum by creating a log-in here: <a href="https://csi-cop.eu/citizenscientistlogin/">https://csi-cop.eu/citizenscientistlogin/</a></p>
Short summary	<p><b>Apps:</b> checking permission in 'Settings' for existing apps on your mobile devices. Before downloading apps, check what permissions the app is requesting – are these necessary to make the app work? For example, a transport app will need access to your location for the app to provide accurate information on when transport is due near you.</p> <p><b>Websites:</b> Use a privacy-by-design browser, or update your browser settings for no tracking and limit third-party advertising and marketing cookies.</p>
Learning content	<p><b>Online tools that can help you protect your data and your privacy</b></p> <p>To recap what we have learnt so far:</p> <ul style="list-style-type: none"> <li>• In step1 we were introduced to the concept of 'privacy'</li> <li>• In step2 we learnt that 'personal data' refers to a living person</li> <li>• In step3 we learnt about some of the ways our data can be captured online (e.g. though tracking cookies)</li> <li>• In step4 we learnt about the different charters and regulations that give you right to privacy</li> </ul> <p>In this step we will find out what free tools are available online to protect our data and our privacy.</p> <p>Thinking about your Internet usage, do you feel you conduct more and more of your life online than ever before?</p> <p>Pat Walshe (<a href="#">Privacy Matters</a>) notes that we go online to: shop, make video calls, message each other, share experiences, thoughts and feelings via social media. We also book health appointments, search for information including about health concerns for example. We also go online to find and follow travel directions – for travel by public transport, car, bicycle or by foot. We also listen to music or audio online and watch movies or TV on the Internet.</p> <p>Much of our lives have become digital. But becoming digital creates and leaves digital footprints, digital data that can be harvested and used to profile us, to learn about us, to influence us in ways we may not be aware of. Every web page you visit; every click and tap you make; every call or message you make or receive; every social media post you make; the places you visit or 'tag'; every 'like' you make; the songs you listen to or the movies you watch (and details of when you did, whether you paused or fast forwarded or skipped a track</p>



or movie) creates data. This is data that reveals aspects of your behaviour, aspects of YOU and often intimate aspects of YOU. For example, fertility apps that know you intimately. See this 2018 Wired magazine article, 'Before using birth control apps, consider your privacy': <https://bit.ly/3ajCyZz>

Additionally, a privacy charity reported in a 2020 Guardian article that 'Menstruation apps store excessive information'. You can read about it here: <https://bit.ly/3aj7IQH>

Then there are apps that share intimate aspects of a person's sexuality, religion or their location for example (and 'location' data can say suggest an awful lot – whether a location is a place of a specific type worship or a health clinic of a specific nature). See this 2020 Consumer report about such apps here: <https://bit.ly/3ggUw2x>

There are also apps targeted at children and teens/young adults that capture data perhaps without the knowledge of the child or teen who downloaded the app, or the knowledge of the parent(s) who might have purchased an app for their child's use on a smart device. **Yubo** is a "social media app" targeted at children to help them find friends. The UK's Sunday Times newspaper reported on the app's safeguarding issues in its 20 February 2022 edition. You can read part of that Sunday Times Report in the image below:



We will learn later in this step 5 about free online tools that go beneath apps like Yubo to find if there are any data-privacy issues in this or other apps targeted at children.

Data reveals not just aspects of YOU but also aspects of OTHERS. Of those you communicate with and share information with, of your relationships and patterns of communications. For example, an app may ask you to upload or give access to the 'contacts' held on your computer or smartphone. But what is in a contact? A contact may include a person's name, picture, mobile number, email address, postal address, social media name, anniversary date. Being digital online may require us to not only think our own privacy but also the privacy of others.



As discussed in Step 4, in the EU and the UK, the right to privacy online is protected by specific **ePrivacy** laws and the General Data Protection Regulation (**GDPR**). But laws and their enforcement can only do so much. There are things you can do to help protect your privacy online.

We learnt about how people are tracked **via the web** in step 3. This includes through advertising technology (ad tech) such as cookies, server side tracking. But what can you do to control it and protect your privacy online? [[privacy self management](#) is hard]. You can learn more about how people are **tracked via mobile apps** (software development kits-SDKs), by reading an article by Binns et al. (2018): 'Third Party Tracking in the Mobile Ecosystem' accessible from here: <https://arxiv.org/pdf/1804.03603.pdf> .

### **Tools to discover tracking and to control it.**

#### **Transparency tools - web:**

There are number of tools available to help you understand the tracking that takes place on the websites you visit. A lot of the tracking is done to target you with advertising or to 'personalise' your experience. This often includes sharing data with third party advertising companies, sometimes hundreds of companies.

#### **Some of the web transparency tools include:**

**Webbkoll** is a tool that simulates what happens when a user visits a web page using a typical browser. It will show what first party and third party cookies may be present on the page visited and also what tracking takes place that doesn't rely on cookies, such as requests made by servers <https://webbkoll.dataskydd.net/en>

**Blacklight** scans a website and reveals key tracking technologies on the site. <https://themarkup.org/blacklight>

**Pagexray** is an analytics tool that shows all the ads and trackers loaded on to a webpage and presents the results in the form of a tree graph. Results can be downloaded as HTTP Archive (.har.json) or detailed results (.json) <https://pagexray.fouanalytics.com/>

**Request Map Generator** helps identify what third-parties are on a website and where data is transmitted. Results can be downloaded into a CSV file. <https://requestmap.webperf.tools>

**Cover Your Tracks** is a tool to test how well your browser protects against tracking and fingerprinting <https://coveryourtracks.eff.org>

#### **Transparency tools – mobile apps:**

Examining mobile apps is not easy. When you use apps on your phone, [O'Flaherty](#), a cybersecurity journalist, states that the apps "may track you across other apps and websites in order to target you with advertising. This is currently done through something called the identifier for advertisers (**IDFA**), which tracks without revealing your personal information".

Some tools exist to help shed light on the existence of 'trackers' embedded in Android apps.

A key tool for Android is **Exodus Privacy**:

<https://exodus-privacy.eu.org/en/>

Android studio <https://developer.android.com/studio>



Pat Walshe (Privacy Matters) advises that there is currently no equivalent tool for Apple's iOS apps. However, Apple has introduced new transparency rules for its store, and developers, that require them to use predefined privacy labels to disclose what data they use and why. Apple's new iOS [14.5](#) also requires developers to "get the user's permission before tracking their data across apps or websites owned by other companies for advertising, or sharing their data with data brokers."

According to Apple, its new privacy function allows owners of Apple phones with this operating system to "tap the Privacy Report button to better understand how websites treat your privacy." ([Apple, 2021](#)). Again according to Apple, its App Tracking Transparency function (ATT) will "require all apps to ask for explicit permission to track" and "Under Settings, users will be able to see which apps have requested permission to track, and make changes as they see fit." ([O'Flaherty, 2021](#)).

On the Mac OS, ('Big Sur') Apple has provides a privacy report tool that appears as an icon in the Safari browser. This lets users see what trackers are on a web page and being blocked. Apple's Safari browser is "giving you more ways to help protect your privacy" ([Apple, 2021](#)). Apple's privacy drive is a "game changer" according to [O'Flaherty, 2021](#).

And with the "third-party cookie dying" ([Cyphers, 2021](#)), citizen scientists could be the groundswell force that prevents any replacement to track us online, such as Google's "new suite of technologies to target ads on the web", moving us closer to privacy browsing.

**Recap: What can you do to protect your privacy?**

Use browsers that protect your privacy

Use Ad blockers

Use privacy settings – operating systems, browsers, apps.

## Citizen Science Library



Review your learning	Please review what you learnt in step 5 by understanding that there are ways to protect your data and your privacy when you are online.
Activities	Experiential learning: learn through exploring websites you visit, and apps you use what digital trackers, if any, are in the websites and in the apps.



	<p><b>Activity 1:</b> Use one of the tools you learnt about in this step, such as <a href="#">webbkoll</a> to explore beneath a website you visit often. Check the website for its a) privacy policy, and b) its cookie notice.</p> <p><u>Questions</u> -How easy was it to understand the privacy policy? -Did the cookie notice inform on any, and the number of cookies? -What embedded <i>third-party cookies</i> were made known to you in the cookie notice?</p> <p><b>Activity 2</b> If you are a parent and allow your children to use a smart phone with apps, check the permissions of an app, especially an app designed for children. For example a game app, or friendship app targeted at young people.. Go to 'Settings' and select any app then check its permissions.</p> <p><u>Questions</u> - What permissions were granted to the app you checked? -Were you aware of these permissions for the app when you downloaded it?</p> <p>Reminder: you can post your views on your learning on CSI-COP website <a href="#">forum</a> here: <a href="https://csi-cop.eu/forum/">https://csi-cop.eu/forum/</a> - you will need to register on the website before posting on the forum by creating a log-in here: <a href="https://csi-cop.eu/citizenscientistlogin/">https://csi-cop.eu/citizenscientistlogin/</a></p>
Activity purpose	<p>Progressing from informal learner to becoming a CSI-COP citizen scientist.</p> <p>Discuss your opinion of this workshop with family and friends:</p> <ul style="list-style-type: none"> <li>• What do you feel you gained from taking CSI-COP's five informal learning steps?</li> <li>• Would you like to join the CSI-COP team and become a citizen scientist to investigate online tracking?</li> <li>• Would you be interested in further education about data protection, privacy, web and app development and related topics?</li> </ul>
Short Tweet	I'm protecting my data with web tools.
Reading for step 5	<p>Recommended Reading</p> <p>Cyphers, B. (2021). Google's FLoC (Federated Learning of Cohorts) is a terrible idea. <b>Electronic Frontier Foundation</b>. Accessible from here: <a href="https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea">https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea</a></p> <p>O'Flaherty, K. (2021). Apple's Stunning iOS14 Privacy Move: a game-changer for all iPhone Users. <b>Forbes</b>. Accessible from here: <a href="https://bit.ly/3vpOq4v/">https://bit.ly/3vpOq4v/</a></p>



## Your feedback

<p>Your feedback on CSI-COP's informal education course 'Your Right to Privacy Online'</p>	<p>It would help the CSI-COP team to know how useful you found this course, please select one from the list below:</p> <ul style="list-style-type: none"><li>5. Very useful</li><li>4. Useful</li><li>3. No thoughts</li><li>2. Not useful</li><li>1. Definitely not useful</li></ul> <p>Please feel free to add any other comments or suggestions you might have about this course:</p>
--	--



## Assess your learning

To assess your learning and to gain a CSI-COP certificate, please answer the questions and return to either Huma or Jaimz at the emails below. If you gain 8/10 then you will receive a CSI-COP informal education certificate. You can try the questions as many times and send your answers to the CSI-COP team at Coventry University:

Huma on [ab7778@coventry.ac.uk](mailto:ab7778@coventry.ac.uk) or

Jaimz on [ad5956@coventry.ac.uk](mailto:ad5956@coventry.ac.uk)

### Questions

- a. Is this statement true or false: Privacy has become an issue since Facebook?
- b. Is this statement true or false: Google Chrome's Incognito browser allows you to search in complete privacy?
- c. Is this statement true or false: Using public wi-fi can share your location data?
- d. Is this statement true or false: Sensitive personal data relates to your name?
- e. Is this statement true or false: Fingerprinting is a form of website tracking that uses the attributes of your device or browser to build a profile of you?
- f. What classes as behavioural data – please choose all that apply from below:
  - i. Your interactions on a website
  - ii. Your web browsing data
  - iii. Online purchase history
  - iv. When you use an online map
  - v. Using an app, for example to monitor your health
- g. Is this statement true or false: Human rights were considered something essential to our dignity and to protecting basic rights and freedoms?
- h. Is this statement true or false: Your rights under the Universal Declaration of Human Rights (UDHR) include “protection against arbitrary interference with an individual’s privacy, family, home or correspondence”?
- i. Is this statement true or false: Under the European convention on human rights (ECHR): in the modern age we have no right to expect a private and family life in our home and our correspondence?
- j. Under the general data protection regulation (GDPR), please select all that apply:
  - i. Right to be informed
  - ii. Right to transparency
  - iii. Right to data protection
  - iv. Right not to be filmed by other people’s camera equipment



## Becoming a citizen scientist

<b>Becoming a CSI-COP citizen scientist</b>	<p>After completing the five steps in CSI-COP's informal education course and receiving your certificate, we would welcome you to join the CSI-COP team and help us investigate the extent of online tracking.</p> <p>You can join the CSI-COP team and volunteer as a citizen scientist in the project.</p> <p>Full information will be provided to you on request including:</p> <ul style="list-style-type: none"><li>• Participants Information Sheet: on the purpose of the citizen scientist's role</li><li>• Informed Consent Sheet complying with the general data protection regulation (GDPR)</li><li>• Information on how to get started on investigating websites and apps for cookies.</li></ul> <p>You can learn more now by going to the CSI-COP website '<a href="https://csi-cop.eu/about/">About</a>' page here: <a href="https://csi-cop.eu/about/">https://csi-cop.eu/about/</a> - You can also check the 'frequently asked questions' (FAQ) page on the website here: <a href="https://csi-cop.eu/faq/">https://csi-cop.eu/faq/</a></p> <p>If you have not yet, you can <a href="https://csi-cop.eu/citizenscientistlogin/">register</a> your interest by creating an account on the CSI-COP website here: <a href="https://csi-cop.eu/citizenscientistlogin/">https://csi-cop.eu/citizenscientistlogin/</a></p> <p>CSI-COP website forum to discuss with other citizen scientists in this project can be found here: <a href="https://csi-cop.eu/forum/">https://csi-cop.eu/forum/</a></p> <p>Thank you so much for reaching this far. We have one more task we would like you to help us with: learn <i>who are</i> citizen scientists. Overleaf you will find a survey, you will note we do not ask questions that can identify you as a person. We really appreciate your time assisting us with this. We look forward to your joining CSI-COP as a citizen scientist and a future privacy champion.</p> <p>Huma and Jaimz</p>
---	---



<p><b>Age range: please circle one from the range</b></p>	<p>18-39;      40-65;      66+;      Prefer not to say</p>
<p><b>Gender: please select one</b></p>	<p>Female; Male; Intersex; Trans Umbrella; Other; Prefer not to say</p>
<p><b>Location: please select one</b></p>	<p>Urban – towns and cities -e.g. Patras, Coventry, London</p> <p>Rural – villages (below 2000 population)</p> <p>Prefer not to say</p>
<p><b>Languages:</b></p> <p>1. What is your dominant, or mother tongue?</p> <p>2. Do you speak more than one language fluently?</p> <p><b>You can prefer not to say.</b></p>	<p>1.</p> <p>2.</p> <p>Prefer not to say</p>
<p><b>Accessibility:</b></p> <p>Do you regard yourself as having some accessibility issues; for example, use text-to-speech software due to a visual impairment?</p>	<p>YES</p> <p>NO</p> <p>Prefer not to say</p>
<p><b>Work:</b></p>	<p>Student level: please select</p> <p>Undergraduate</p> <p>Postgraduate</p> <p>Doctoral</p> <p>Non-student: please select the category that best describes your employment status:</p> <p>Employed, working 36.5 or more hours per week</p> <p>Employed, working 1-36 hours per week</p> <p>Not employed, looking for work</p> <p>Not employed, not looking for work</p>



	<p>Refugee seeking asylum</p> <p>Retired</p> <p>Having accessibility issues, not able to work</p> <p>Prefer not to say</p>
<b>Internet access:</b>	<p>Have access to own Internet connection (home or work broadband/mobile)</p> <p>Use public access when using the Internet</p> <p>Prefer not to say</p>
<p><b>Internet usage:</b></p> <p>How often do you use the Internet? Please select:</p>	<p>Daily</p> <p>2-3 times a week</p> <p>Once a week</p> <p>Less than once a week</p> <p>Never</p> <p>Prefer not to say</p>
<b>Purpose of Internet use:</b>	<p>Use the Internet as part of daily work</p> <p>Use the Internet for leisure, not part of work</p> <p>Use the Internet for work and leisure</p> <p>Use the Internet in a limited way, for example, using a computer in a public library.</p> <p>Prefer not to say</p>
<b>Apps usage: Desktops and laptops</b>	<p>Use apps regularly, for example to authenticate access to work tools (e.g. Zoom, MS Teams). If so please provide names of some apps you use and their purpose:</p> <p>Work tools (e.g. Microsoft Office, etc.)</p> <p>Playing Games (e.g. STEAM).</p> <p>Educational apps</p> <p>Lifestyle (sport, fitness, health)</p>



	<p>News</p> <p>Entertainment (e.g. streaming apps, such as Netflix)</p> <p>Other</p> <p>Prefer not to say</p> <p>Rarely use apps on desktops and laptops</p> <p>Do not use apps on desktops and laptops</p> <p>Prefer not to say</p>
<p><b>Apps usage: Mobile devices</b></p>	<p>Use apps regularly, for example, transport apps to inform on timing of next train, bus, etc. If so please provide names of some apps you use and their purpose:</p> <p>Playing Games</p> <p>Educational apps</p> <p>Lifestyle (sport, fitness, health):</p> <p>News</p> <p>Entertainment (e.g. streaming apps – Amazon Prime):</p> <p>Other</p> <p>Prefer not to say</p> <p>Rarely use apps on mobile phone or tablet</p> <p>Do not use apps</p> <p>Prefer not to say</p>
<p><b>How did you hear about the CSI-COP project?</b></p>	<p>From CSI-COP website</p> <p>From a university</p> <p>From membership to an association (e.g. Women in tech)</p> <p>From a citizen science platform, for example</p> <ul style="list-style-type: none"> <li>• SciStarter</li> <li>• Zooniverse</li> <li>• EU-Citizen.Science</li> <li>• Other citizen science platform</li> <li>•</li> </ul>



	<p>Surfing the web</p> <p>Previous voluntary work</p> <p>From Social media, <u>please say which platform</u></p> <p>Word-of-mouth</p> <p>Other</p>
<b>Did you complete CSI-COP's free online informal education workshop?</b>	<p>Yes</p> <p>Not yet but intend to</p> <p>No, prefer to wait for future face-to-face workshops if held near to where I live</p>
<b>If you did complete the workshop, do you intend to join the CSI-COP team as a volunteer citizen scientist?</b>	<p>Yes</p> <p>Maybe</p> <p>I need more information</p> <p>No</p>
<b>To send your completed 'Assess your learning' questions, your survey and for any other queries please contact Coventry University's CSI-COP team:</b>	<p>Please send return this completed document to Coventry University CSI-COP team members:</p> <p>Huma on <a href="mailto:ab7778@coventry.ac.uk">ab7778@coventry.ac.uk</a> or Jaimz on <a href="mailto:ad5956@coventry.ac.uk">ad5956@coventry.ac.uk</a></p>
<p><b>Thank you for your time completing CSI-COP's informal education course and the survey</b></p> <p><b>This document will be available in other languages soon.</b></p> <p><b>Please check CSI-COP website here: <a href="https://csi-cop.eu/">https://csi-cop.eu/</a></b></p>	

