European Commission

JRC TECHNICAL REPORTS

Privacy safeguards and online anonymity

Pizzirani A., Di Gioia R., Chaudron S., Draper Gil G., Sanchez I.

2018

EUR 28991 EN

This publication is a technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

Contact information
Name: Alberto Pizzirani
Address: Via Enrico Fermi 2749, I-21027 Ispra (VA), Italy
Email: alberto.pizzirani@ec.europa.eu
Tel. +39 0332783663

JRC Science Hub
https://ec.europa.eu/jrc

JRC109792

EUR 28991 EN

PDF ISBN 978-92-79-77231-3 ISSN 1831-9424 doi:10.2760/30934

Ispra: European Commission, 2018

How to cite this report: Author(s), *Title*, EUR, doi

Contents

Abstract

In a world that is increasingly more connected, digital citizens actively or passively accept to transmit information, part of which is 'personal data'. This information is often collected and elaborated by third parties to infer further knowledge about users. The act of gathering the data is commonly called 'tracking' and can be performed through several means. The act of analysing and processing those data and relating them to the individual is called 'profiling'.

The aim of this JRC technical report is to be an instrument of support for digital citizens to help them to protect and to manage their privacy during online activities.

After a brief introduction in Chapter 1, the following chapter is dedicated to the description of two legitimate use cases to track and profile users online, namely target advertising and personalisation of the user experience. Chapters 3 and 4 identify and analyse the set of techniques currently used by online digital providers to track citizens and profile them based on their online behaviour. Chapter 5 deals with some of the available tools that could be helpful to protect privacy while browsing online; these are cited in Chapter 6. Chapter 6 also aims to raise awareness among users and provide some guidelines to address specific issues related to privacy through a multidisciplinary approach. The report concludes by highlighting the importance of raising awareness among digital users and empowering them through educational, technical and legal tools, including the general data protection regulation (GDPR), to overcome possible privacy issues.

This page is intentionally left blank

1. Introduction

In a world that is increasingly more connected, digital citizens actively or passively accept to transmit information. Some of these data are 'personal data' and can be used to uniquely identify an individual, while others, even if they are not strictly 'personal', are still related to the individual. There is a growing interest in using those data, both personal and not, and gathering further information from them.

In this scenario, the recent GDPR helps citizens to better control their personal data. However, for those data that do not fall in the category of 'personal data', additional efforts have to be made to improve the degree of control that citizens have over them.

The act of collecting data is commonly called 'tracking' and can be performed through several means. Sometimes those data are directly submitted by citizens, whereas in some other cases third parties gather them through different mechanisms, such as observing the actions of the individuals.

Once these data have been collected, even if they are not personal data, they can still be processed to infer additional information of the individual. The act of analysing and processing those data and then relating them to the individual is called profiling.

While tracking and profiling have some legitimate use cases (for example to offer a more personalised experience to a specific visitor of a website), this is not always the case. Moreover, additional privacy issues could appear in the data flow where data are transferred, processed and used by third parties.

Chapter 2 presents two of the typical use cases for user tracking and profiling. Chapter 3 describes possible technical means to track users online and Chapter 4 is dedicated to profiling.

Chapter 5 deals with some of the available tools that we have identified to be helpful to the data subject to protect their privacy while browsing online.

Chapter 6 is dedicated to user awareness and education. In this chapter, we started from the taxonomy of the privacy-related harms described by Solove (Solove, 2006) and used a multidisciplinary approach to analyse each one. In this way, we created tables to regroup, in a schematic way and for each specific harm highlighted by Solove, the possible legal means offered by the GDPR, the possible technical means and the digital competences involved both in the prevention and in the resolution of each privacy harm.

This page is intentionally left blank

2. Motivations

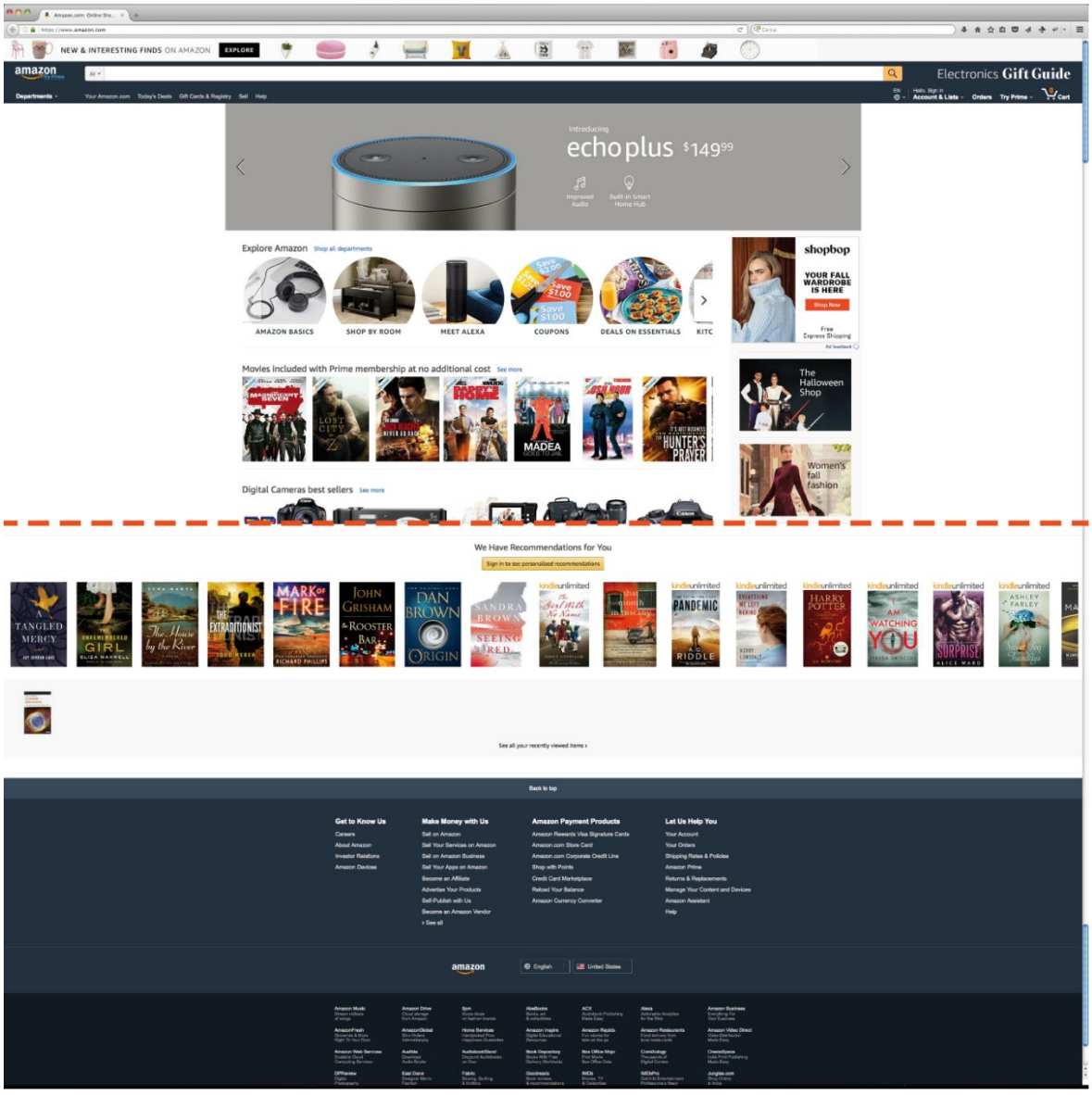
Collecting data is not harmful in itself; the problem could arise when the data are used in an unhallowed way or when a specific limit of the privacy of an individual is violated.

In this section, we give an overview of the possible scopes to process the data collected.

2.1. Targeted advertising

The term 'targeted advertising' commonly refers to a special form of advertising that is specifically aimed at a group of people or at a single person.

Figure 1: An example of target advertising, where the recommended products are suggested through the analysis of the previous browsing history of the user



This form of advertising takes into account specific traits of the audience. The considered traits can be demographic (like race, economic status, sex, age, level of education, income

level and employment) or they can be psychographic (like attitudes, lifestyle interests and personality).

While this form of advertising can also be performed on traditional media, considering the typical audience of a specific transmission or journal, it is the one performed online that is the most refined, displaying specific advertisements related to the website where the advertisement is going to appear as well as the content of the web page and the detailed information of the specific user.

Targeted advertising can be seen either as a good thing or as a malicious thing.

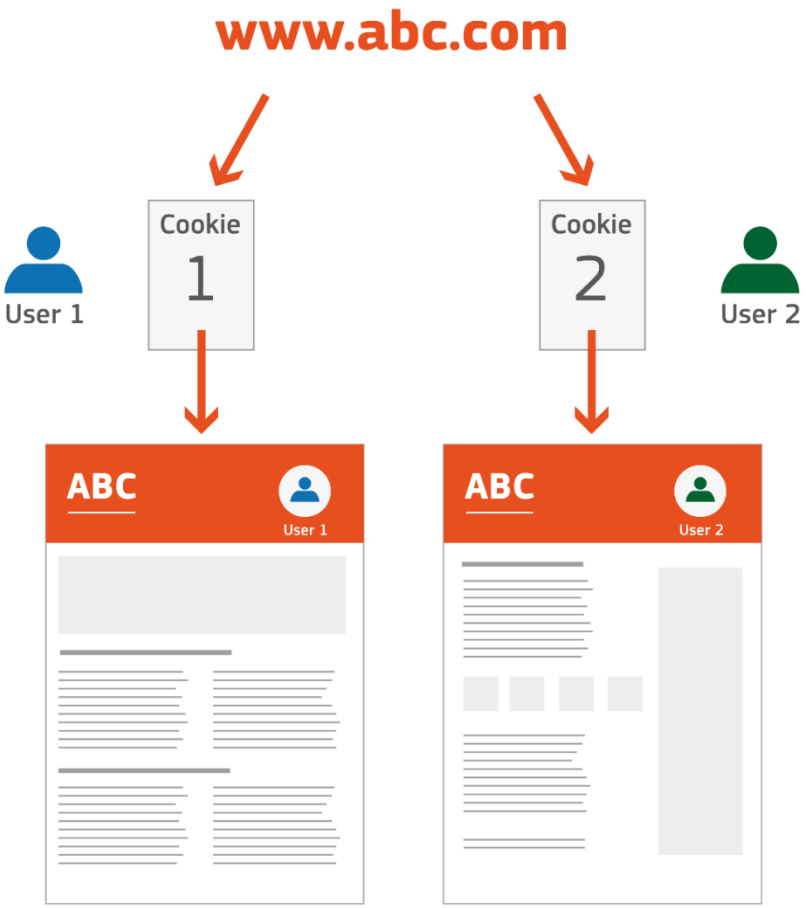
On the one hand it is helpful since it saves the users from specific advertisements in which they will (probably) never be interested, but on the other hand it presses the right buttons to push the user into buying items, and this, in some circumstances, could be dangerous when the audience of the advertisement is an easily influenced subject, such as a minor.

This form of advertising has evolved so much, to the point of becoming a subdiscipline whose main challenge is to find the best advertisement to show to a user when he/she is in a specific context.

2.2. Personalising the user experience

Customising a user's experience is a highly requested feature by the users of several websites.

Figure 2: Tracking users makes it possible for a website to offer personalised content



To personalise the experience, the simplest usage of cookies is just to keep the users logged on to the website in such a way that they do not need to login again every time they access the website from a trusted platform (their own personal computer, smartphone, laptop, etc.).

Another simple usage of cookies is to store specific settings of the user, for example the layout of the page, the colour scheme, the fonts, and so on.

On blogs portals, for example, the personalisation of the page of a blog is a feature that is not only requested but in some cases mandatory.

The change of appearance of a website, at higher levels, can show users a completely different website, taking into account the geographical data of the users themselves. For example, a website could show a homepage in English, Italian, Japanese or Chinese according the location obtained from the device of users.

In some ways, the targeted advertisements could also be considered a personalisation of users' experience, since they just show advertisements that are aimed at them and are very specific.

2.3. Malicious — Fraudulent — Illicit

While tracking and profiling users can be used to sell specific products, they can also be used to generate clicks for advertisements that follow the 'pay per click' policy.

Of course there is no specific threat for the user by clicking on these advertisements, but their scope is not specifically to sell the product.

Furthermore, an entity that gathers information related to a subject can place itself in a position of advantage with respect to the subject.

This could lead to threats related to privacy, not only online, but also in the real world (e.g. distortion, blackmail).

For example, the information could be gathered through a malicious code executed on the machine of the data subject, or it could be gathered through deceptive forms or questions, where the user might answer by disclosing information that they would otherwise not do.

Even if several tools are already available to protect the privacy of users, the most powerful tool is always through educating users.

This page is intentionally left blank

3. Behavioural tracking

The phase where data related to a user that will be used to profile them are collected is often referred to as behavioural tracking.

With this term we refer to the collection of actions of the users in order to perform further analyses on the data collected.

Nowadays technology offers several means to facilitate tracking. In this chapter we offer an overview of the technical means that can be used online to perform behavioural tracking of users.

3.1. Web tracking

When we talk about 'web tracking' we refer to the collection of data relative to a user, across different visits of a specific website or across different websites.

This form of tracking is the main source of information used for profiling.

The tracking is mainly performed by monitoring IP addresses and using well-known techniques, such as cookies or JavaScript, and other less well-known techniques, like so-called supercookies.

3.1.1. Cookies

An HTTP cookie, web cookie or simply 'cookie' is a piece of data that is used from web pages as a token to identify users.

The main reason to use cookies is because the HTTP protocol is stateless, so cookies are useful to mantain stateful information.

The use of cookies has been disciplinated both in European legislation (European Commission, 2016) and in several national legislations.

Even if a cookie can be stored inside a text file, it is not mandatory that the container is a text file.

Usually the main fields inside a cookie are:

- Name/Value: it is a variable and it is a mandatory field;

  Expiration date: this field is optional and defines the date after which the cookies can be considered as expired — this value can be expressed as a date, a number of days, 'Now' (meaning that the cookies must be deleted immediately) or 'Never';
- HttpOnly: it defines that the access to the cookie must be strictly restricted to HTTP;
- Secure: it defines if the cookie must be sent through a secure connection (HTTPS).

'Domain' and 'path' fields indicate that the cookie can be sent to the server only for the specific domain and path defined. If they are not specified, the value taken by default is the domain and path that originally requested it.

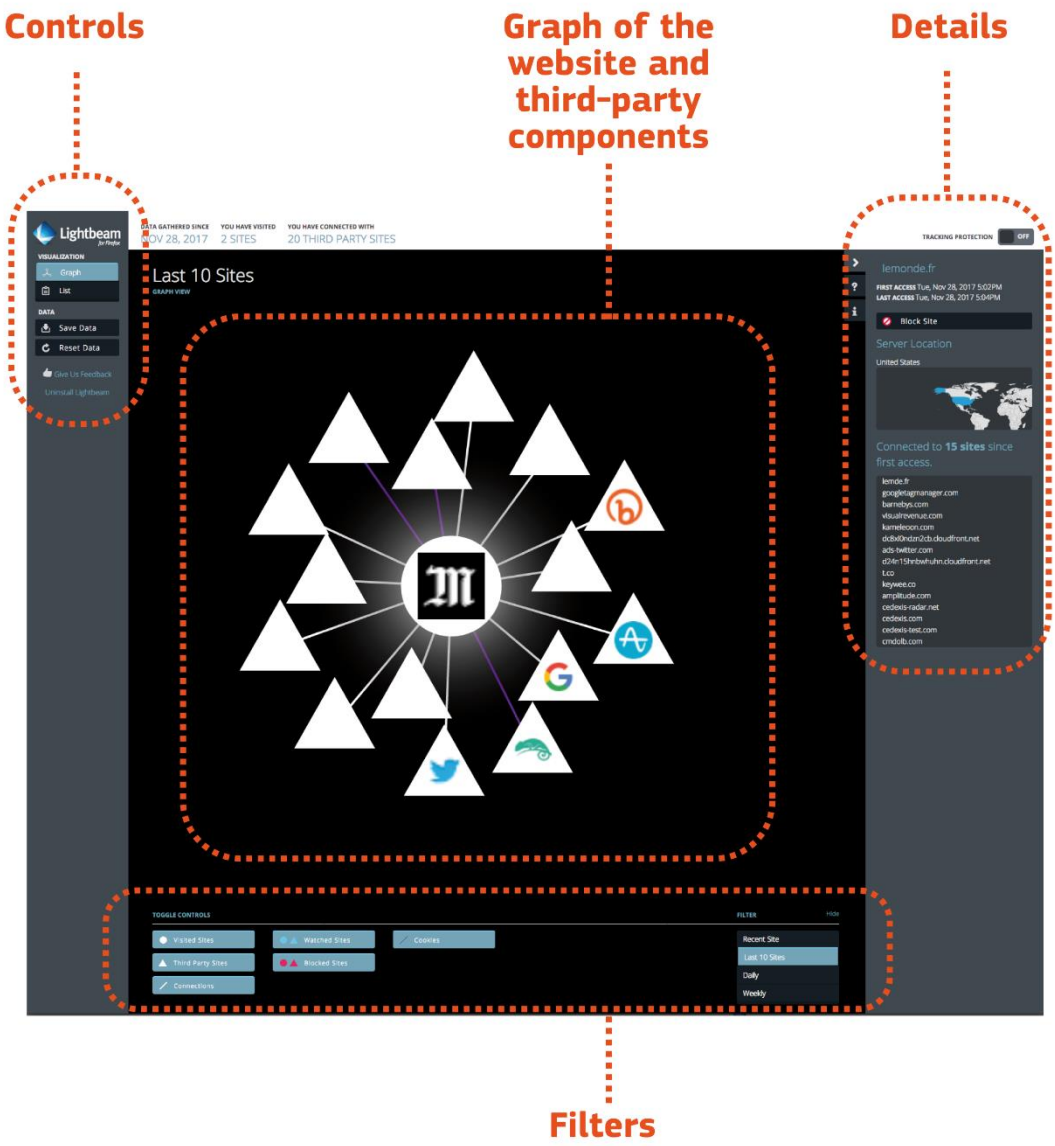
Cookies can be classified according the expiration date:

- session cookie: these cookies will be deleted when the browser is closed and they do not have an expiration date so that the browser can identify them;
- persistent cookie: these cookies have an expiry date, which means that the cookie will be saved on the user's platform until then (unless it is deleted earlier) — they are useful to maintain information between separate visits to the same website (e.g. the 'keep me logged on' or 'remember me' function on several websites).

A further classification can be done according to the domain that creates them:

- first-party cookies: usually the domain attribute will be the same as that of the website that the user is exploring;
- third-party cookies: these are usually saved when the web page on the website has embedded contents (like banners, web bugs, Iframe, JavaScript) coming from other domains.

Figure 3: Lightbeam is a plugin for several browsers, making it possible for users to know the third-party components that are loaded while browsing a specific website, including more detailed information about each of them



The use of cookies has been regulated in the European Union by the so-called e-privacy directive, Directive 2002/58/EC (European Parliament, 2002), and later amended by Directive 2009/136/EC (European).

The directive itself recognises the importance and usefulness of cookies in its recital 25, below.

> However, such devices, for instance so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

However, it regulates their usage with Article 5, paragraph 3, below:

> Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, *inter alia* about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

The amendment by Directive 2009/136/EC slightly changes Article 5, paragraph 3, whereby instead of requiring an option for users to opt out of cookie storage, it states that consent must be requested to the users for cookie storage.

Further recommendations and clarifications related to cookies are given by the "Article 29 Working Party" in the 'Working Document 02/2013 providing guidance on obtaining consent for cookies (Party, 2013)'.

The paper of the Article 29 explains in detail what the informed consent is and how it should be requested for it to be valid under the European legislation. While concerning the recommendations given, the opinion is that there are some cases where the user's explicit consent for the storage of cookies, which are not used for additional purposes, or for the storage of analytic cookies, which are used by the originating website itself, is not needed.

Super cookies

Supercookies are a special kind of cookie that, contrary to those that originate from a specific domain, come from a first-level domain (e.g. '.com') or a public suffix.

This kind of cookies are often blocked on browsers by default, because otherwise they could be a potential security problem since they can interfere with the requests from users or from legitimate websites with the same extension as the domain.

A special case of super cookies are those saved through the Adobe Flash Player application, which is an add-on for almost all browsers. It is usually used to allow the reproduction of multimedia content or to implement simple and portable applications (like games) inside a web page.

Flash cookies are downloaded or created when a flash code is executed by the flash plugin of the browser. However, unlike conventional cookies, they are not under the control of the browser itself and users have no direct control over them.

Furthermore, there is no notification to users when these cookies are set and they also never expire.

Zombie cookies

In a similar way to the fictional characters, 'zombie cookies' refers to a special kind of cookie that 'comes back' after being eliminated.

This is possible because the information stored in the cookie is duplicated in multiple locations (e.g. a flash cookie), and when the website detects that a cookie is missing it can replicate the information from the secondary repository.

3.1.2. JavaScript

Often websites use small JavaScript files to perform several activities.

These small files are downloaded by the user, but have limited access to the user's data.

They perform computations and sometimes, since they are allowed to access the information stored in browsers, they update first-party cookies.

3.1.3. ETags

With an increasing will to protect privacy and a better understanding of the problem by non-technical people, a greater number of persons block or delete cookies more frequently. However, in this race, websites with a will to track users move towards alternative ways to do so. One of the newest methods used for user tracking is through ETags.

ETags are a unique identifier assigned to resources (e.g. images inside a website) and are used to avoid repeatedly downloading the resources if they are already cached. If a website detects that the current version of a resource is the same inside the cache of the user's browser, it informs the browser to use the cached one, otherwise the new resource, together with a new ETag, is sent back to the browser.

The purpose of ETags is to reduce the bandwidth consumption using resources already cached (if they are still valid) on the device of the user.

3.2. Social network tracking

Outside the trivial aspects related to the information derived by 'social' actions performed while users are logged on to the network, like posting pictures (potentially of items like food or beverages that a user likes), joining groups of interests or simply liking other posts of friends, the relation between social networks and user tracking runs a little deeper.

Some social networks offer an additional service for so-called premium users: the possibility to track other users.

This option is available, for example, on:

- job search portals, to know the identity of other candidates for a position and to compare curricula, or to see the profile of recruiters who visited a candidate's own profile;
- academic social networks, to know who downloaded an academic's papers;
- online dating websites, to know further (personal) details about other users.

The possibility to know more about other users is usually, not only, accepted by the community, but often it is a feature requested by the users themselves who implicitly accept to be tracked.

There is another hidden aspect of the social networks related to tracking.

Sometimes things that are apparently harmless have some hidden implications.

A typical example is the 'like' button (typical of a large social network, displaying a blue hand showing a thumbs up), which has been added by several websites to give their users a means to show their appreciation.

The plugin that implements the button is a success from a marketing point of view, with an increase in traffic that has been shown to exceed 200 % on average. According to a study performed by Roosendaal (Roosendaal, 2012), however, the button has revealed to also be an amazing tool to track users.

The button is a piece of HTML code that requests the 'like' image to the main server of the social network when the hosting website is loaded. In this way, the button can be used to set third-party cookies or to recognise them.

Third-party cookies always have knowledge of the website hosting the plugin, since data related to the referrer are included in every HTTP request associated with the cookie.

Due to the great number of websites implementing this feature as well as to the fact that the data related to multiple websites can be combined, the cookie associated to the button can be used to build the browsing history of a web user.

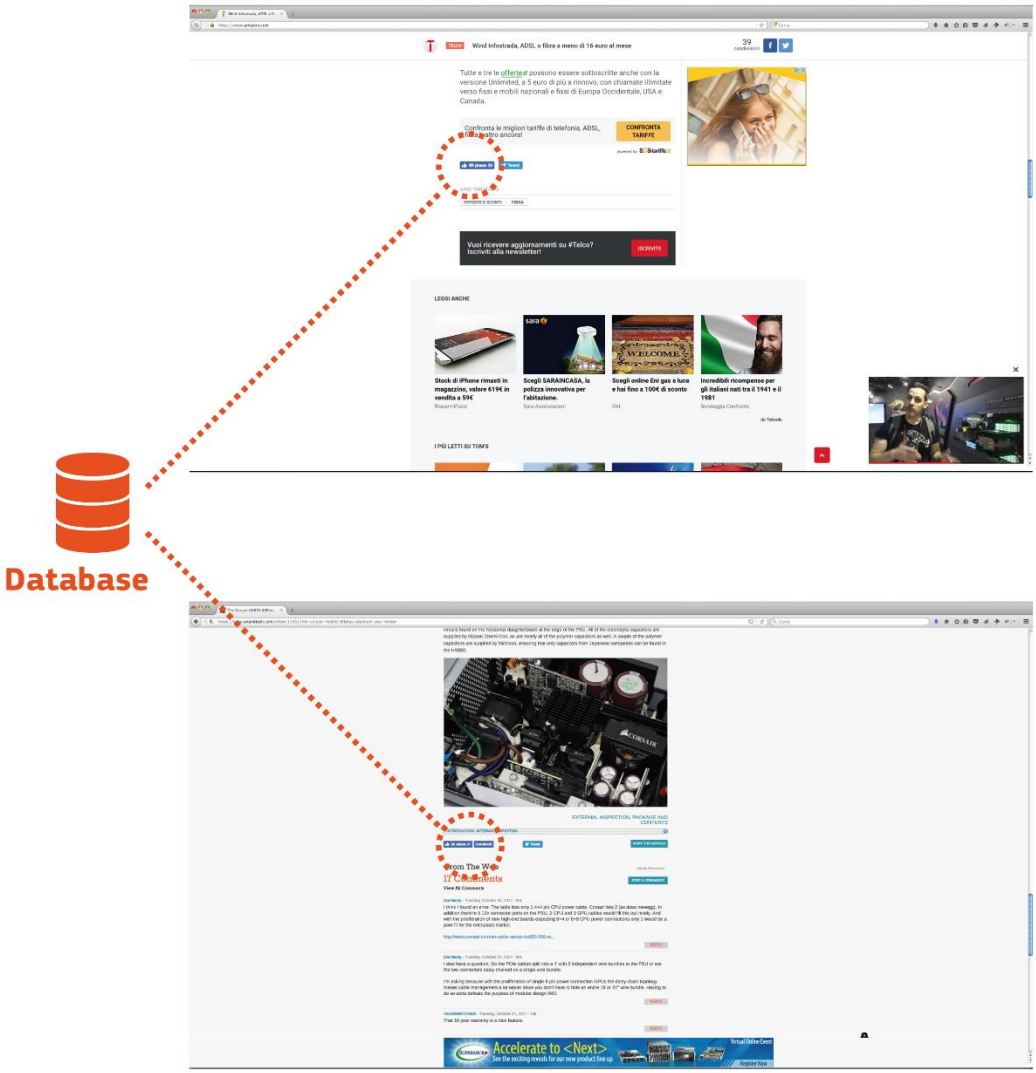
Roosendaal underlines that the user does not need to click on the button; the cookie that identifies the user is sent to the server of the social network the moment the web page is loaded.

Roosendaal's paper gives a detailed analysis of several scenarios, taking into account the differences of the cookie according to the existence, or not, of an account on the user's social network and whether they are logged on to the network itself or not.

The results can be summarised in the following way:

- If a user has an account, the cookie is created by the server of the social network when the account is created, and is created again every time the user logs in from a new device. This cookie will be the one used by the 'like' button component in the following visits to the websites implementing this feature.
- If a user does not have an account, a cookie will be created anyway during the first visit to a website implementing a specific component of the social network. If the user later decides to create an account on the social network, the information stored in the cookie can be moved to the new cookie that identifies the user.
- If a user deletes their account, they can still be tracked (through a previously stored cookie) and the browsing data can be connected to an individual data set. After deleting an account, the user will be considered as not having an account, whereby every service connected to the social network, every cookie related to them and the social network itself must be deleted.

Figure 4: When browsing different websites, the same resource may be loaded from the same repository, making it possible for third parties to perform cross-site tracking



3.3. Location tracking

In recent years the availability of new technologies that can be moved easily in the physical world has created a new kind of 'location-based service'.

Like the name suggests, these services offer, or allow the user to perform, specific actions based on their location.

Among the technologies on which these services are based, we can cite, for example, RFID, which makes it possible for users to use wireless payment of the highway toll, or the Global Positioning System, better known as GPS, which is now integrated into any smartphone that can be used as a navigation system.

While these services are undeniably useful and are now considered essential, the market is evolving towards a different kind of location services with an increasing 'social' aspect.

In the past years we have observed the arrival and an increased interest in apps like:

- navigation systems with integrated social networks to signal traffic jams or car accidents;

- apps that can tell users the possible points of interests (restaurants, museums, attractions, etc.) in the surrounding area based on the reviews of other users;
- apps to signal to 'friends' one's presence in a place or one's will to go there to meet them.

As time goes on, the line between location-based services and online social networks becomes fuzzier, and 'traditional' online social networks have added options for users to obtain and make use of a user's location.

While all of them are downloaded and installed by the user, there is an exchange of information related to the location that could be a privacy issue if not properly handled.

The possibility to be geolocalised is not only linked to the usage of specific apps or location-based services.

The use of GSM itself is already enough to be geolocalised.

A few years ago (Biermann, 2011) the case of a German politician became famous when he requested his telecom operator to provide 6 months of his phone data, which he later made available to an online newspaper.

The data was then combined with his public feeds, blog entries and interviews, all of them freely available online.

Figure 5: Zeit Online newspaper showing the power of crossing information gathered from different sources

Then everything was put into a small application that like a movie reproduces his movements and actions on a map.

The result has a great visual impact and can give a good idea about what can be achieved when data coming from several sources, all related to a single individual, are crossed together.

Another good example that illustrates the power of location tracking is the website Pleaserobme (http://pleaserobme.com/).

While the name perhaps sounds a little scary, it is built with the specific scope of 'raising awareness about over-sharing'. The site automatically scans Twitter feeds to find location check-ins that are being twitted out. Then it posts a message on Twitter, like the following:

Hi @NAME, did you know the whole world can see your location through Twitter? #pleaserobme.com

---

Where 'NAME' is the name of the account that revealed the information and '@NAME' is the way to alert the account owner who has been cited (tagged) into another post.

Similar work is performed by the website WeKnowYourHouse.com (linked to the homonymous Twitter account https://twitter.com/weknowyourhouse), which scans Twitter feeds for posts containing the word 'Home' and messages the owners of the feed to point out that they have revealed the location of where they live.

Even more worrisome is the fact that a lot of people distribute information related to their exact position with anyone else (not only with their own telecom operator), without even knowing it.

This happens because people often distribute pictures they take, not knowing that they contain data of the location where the picture was taken.

The data related to the location are saved among the metadata of the Exif (Exchangeable image file format) and are taken from a GPS connected to a normal camera or from the GPS sensor of a smartphone.

While some social networks strip the images of the Exif data to protect the privacy of their users, not all of them do.

This is because, for some specific social networks like the ones for photo enthusiasts, the data relative to the location where the picture was taken are especially important, so the possibility to show them is a welcome feature.

3.4. Browser fingerprinting

It is also possible to identify users with a high level of accuracy even if no information has been saved onto their machine. This is the so called stateless tracking.

A study performed by Echersley (Eckersley, 2010) shows that online tracking tools are able to identify the user's browser among a set of 286777 other browsers.

This is performed by analysing the information provided by the browser itself (user agent, fonts, screen resolution, plugins or other flags that have been set or not in the browser's settings …) on the website when the user performs a connection.

4. Profiling

4.1. Definition

Profiling is a process that transforms raw data into information that can be later used in a decision process. It applies to different fields, from psychology to law enforcement to computer science. To understand what profiling is, and to put it into context in this report, we refer to the *Oxford English Dictionary*'s definition:

> *'The recording and analysis of a person's psychological and behavioural characteristics so as to assess or predict their capabilities in a certain sphere or to assist in identifying categories of people.'*

This is a very general definition, but it introduces the basics of profiling as a process executed on data referring to an individual, with the objective of using the results in later decisions. In 2008, Hildebrandt et al. (Hildebrandt, 2008) elaborated a definition of profiling that extends its application to a generic subject, e.g. it can be applied to a person or a business. It also defines profiling as a process of discovery or a process of applying a profile. Profiles are defined as sets of correlated data.

> *'The process of "discovering" correlations between data in databases that can be used to identify and represent a human or non-human subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category.'*

In 2014, the Profiling project dedicated an entire report (V. Ferraris, 2014) to define the meaning of profiling, using as its source the definition of Hildebrandt et al. (Hildebrandt, 2008), among others. This definition introduces the objective of making decisions as part of the profiling process, classifies the data into personal and non-personal categories and explicitly mentions that profiling is an automatic process. In their conclusions, Ferraris et al. (V. Ferraris, 2014) define profiling as the following:

> *'Profiling is a technique to automatically process personal and non-personal data, aimed at developing predictive knowledge from the data in the form of constructing profiles that can subsequently be applied as a basis for decision-making. A profile is a set of correlated data that represents a (human or non-human, individual or group) subject. Constructing profiles is the process of discovering unexpected patterns between data in large data sets that can be used to create profiles. Applying profiles is the process of identifying and representing a specific subject or to identify a subject as a member of a specific group or category and taking some form of decision based on this identification and representation.'*

In this chapter we will focus on the profiling definition of the GDPR, which constrains its previous definitions to an automated process of personal data. This definition is more precise and fits better in the context of online anonymity, which is the scope of this work. According to Article 4 (4) of the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016):

> *'profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.*

A typical classification of profiling describes it according to what profiles represent, how they are built or on the relation of the members of a certain profile.

Individual versus group profiling

Individual profiling is used to describe the behaviour, preferences, interests, etc. of a particular person, to the point of even being able to identify this person within a group. Group profiling describes the same traits of a group/category of individuals.

Explicit versus predictive profiling

In explicit profiling the profiles are built on data that are explicitly given by the user, e.g. when a list of interests or an online survey is filled in, whereas predictive profiling builds profiles on data obtained from observing the activity and behaviour of the user, e.g. browsing activity (types of websites visited, queries, etc.). In practice, the best results are obtained using a hybrid approach, where the profiling process uses data from both sources.

Distributive versus non-distributive profiling

In distributive profiling all the members of a profile share the same aspects, whereas in non-distributive profiling the members of a profile share only some aspects. As an example, a group of parents with children in a particular school would be distributive, as everyone in the group has a child in the same school. An example of a non-distributive group could be a list of clients with high risk in an insurance company. In this case, it is possible to end up classified in that category without being a high-risk driver, as there are many variables involved.

4.2. Use cases

As use cases we resort to the two scenarios presented in Chapter 2: targeted advertising and personalisation of user experience. These two activities are strongly related to our daily online activity and are two clear examples of how tracking and profiling work.

4.2.1. Targeted advertising

In the online advertising industry (G. Chen, 2016), user profiling is used to maximise the probability of an advertisement being clicked. To do so, content providers rely on user profiling to decide which advertisement to show to a user. The set of data composed of our browsing activity, search queries, etc. allows content providers to create a profile that describes the habits, interests, etc. of an individual or group. Based on this profile, content providers can decide which advertisement is more likely to attract a user's interest.

In a typical architecture, we have the user, the publisher, the advertisement network and the advertiser. The user is the final user, i.e. the target of the advertisement. The publisher is the website (or application) where the user is browsing. The advertisement network is the entity that connects publishers and advertisers. In a real scenario, the architecture is more complex, and we may have advertisement exchangers, demand and supply platforms (Tuzhilin, 2005), etc.

Publishers sell space on their sites or applications to advertisement networks that then use this space to send advertisements provided by their clients, the advertisers. When a user enters a website, they will receive one or more advertisements within the content of the site, but these will not be provided by the publisher, but by the advertisement network. This network is again responsible for deciding which advertisement to send, depending on the profile of the user who requested the advertisement.

A clear example that users are being profiled is when they start seeing advertisements related to their last internet searches or their last visits to online shops. Moreover, the advertisements can also be related to an interest that they may have, like sports or cooking, something that may not be related to a specific website but to a group of websites.

4.2.2. Personalising the user experience

Many online services offer the possibility of enhancing the user experience they provide by processing personal data. These data are usually acquired through one of the many existing tracking technologies, like those presented in Chapter 3, or directly from the user by answering surveys, rating items/services, etc.

Behind this personalisation, which suggests articles to read, books to buy, music to listen to, etc., there is usually a so-called recommender system. These work by creating a profile (model) of the user and using this profile to offer suggestions. They are typically grouped in three categories (Tuzhilin, 2005):

- content-based: recommendations are based on items/services that the user has previously liked, e.g. movies previously watched and/or positively reviewed;
- collaborative: recommendations are based on items that similar users liked, e.g. music that other users with similar preferences rated positively;
- hybrid: a recommender system that mixes both approaches using data from the user itself and data from similar users.

As an example, music stream services can generate music lists based on the music a user listened to and/or based on the music other users listened to, like the people who liked the user's music lists. Other examples could be services that suggest buying items that are similar to the ones a user previously bought or to the ones that other people bought.

4.2.3. Negative aspects of profiling

There is no doubt that the use of profiling can benefit both users and advertisers in online advertising. On the one hand, the users can receive online advertisements on topics they are interested in, and on the other hand, advertisers can communicate with their potential clients in a more effective way and their advertisements will only be sent to users who may be interested.

In the case of online services, profiling also has a positive impact on both sides. Users of online services can receive content tailored to their needs or even discover new services or content related to their interests. Providers of online services can use profiling as a tool to improve the experience of users, which can help them to obtain new users and/or keep the ones they already have.

Even though profiling has a clear positive impact, its application is not exempt of risks. In Gutwirth and Hildebrant (Gutwirth S., 2010), the authors describe some of the concerns that the application of profiling presents. These concerns are related to privacy and data protection (the data protection law applies only to personal data) and dependency on decisions based on profiling, discrimination, auditability, knowledge asymmetries and transparency.

In a more practical approach, the limitations of profiling can also affect the user in the long term (e.g. if only content related to things that have been liked by a user is visible, users will not be able to discover new topics of interest). These technical limitations have been addressed in different papers (Požrl, 2017; Verbert, 2016; and Veijalainen, 2016), where authors present a survey of previous work carried out on recommender systems and propose research directions to improve the quality of the choices offered by recommender systems.

5. Tools to prevent tracking and profiling

5.1. Technical means

Some of the suggestions that can be given to reduce the risk of being tracked and to avoid (or at least reduce) privacy-related issues are common good sense:

- operating systems and programmes must be kept up to date to fix known security vulnerabilities;
- antivirus software must be kept up to date with the latest virus signature definition;
- programmes or applications for installation and sources where they are downloaded from must be trustworthy;
- personal sensitive information must not be disclosed to untrusted third parties.

5.1.1. Privacy-Enhancing Technologies

Privacy-Enhancing Technologies (PETs) are tools, methods or best practices to protect privacy and to improve the control of the data subject over their personal data, in accordance with the laws of data protection, or to minimise the amount of the data handled by data controllers.

PETs are usually designed to address a single, specific concern about privacy even if there are some that solve (or try to solve) more than one at the same time.

There are already examples of existing and commonly used PETs:

- Communication anonymisers: they aim to implement one of the most promising methods to protect privacy, which is anonymity. There are already several services that offer methods to preserve privacy through complete anonymity or pseudonymity (i.e. anonymity that is reversible if needed). These tools operate at different levels, and some examples that we can cite are disposable/one–time email addresses, pseudonyms for online payment and anonymisers for web browsing. These services have mainly been proposed as 'countermeasures to surveillance'.
- Shared bogus online accounts: the main purpose of these accounts is to have an account for a service that is not related to the real identity of the user. This kind of account is created with bogus data and then the user identifier and the associated password are shared online. In this way, every user who needs an account for that service and does not want to register with their data can use the service anyway.
- Access to personal data: this kind of PET is usually provided by Data Controllers in order to grant the users the right to handle their personal data easily and to fulfil the requirements of the GDPR.
- Enhanced privacy ID (EPID): this is an algorithm for the attestation of a trusted system while preserving privacy. The algorithm is compliant with the international standards ISO 20008 (ISO/IEC JTC 1/SC 27, 2013), ISO 20009 (ISO/IEC JTC 1/SC 27, 2013) and the Trusted Platform Module 2.0 (ISO/IEC JTC 1, 2015) of the Trusted Computing Group. It has been heavily supported by Intel and has been incorporated into Intel chipsets since 2008 and in processors since 2011. The idea is that each entity has a unique public verification key associated with multiple private signature keys. In this way, a device supporting the algorithm could prove to an external party the kind of device it is without revealing all the information.

The list of PETs is by no means exhaustive and is growing as time passes.

In the following sections we will give some examples of PETs and will describe some applications or technologies that can be helpful for citizens to preserve privacy while performing their online experiences.

5.1.2. Private browsing

Several browsers are now implementing the feature of 'Private Browsing' (some browsers call them 'Incognito Mode' or 'InPrivate Browsing' instead of Private Browsing).

While this mode is enabled, data like browsing history, search history, cookies and temporary files are only saved until the end of the private session, while downloaded files and bookmarks are saved and if needed, they must be deleted manually.

Some browsers perform a further step towards privacy and offer the option to login to a virtual private network (VPN) (see paragraph 5.1.5) while performing private browsing.

While private browsing is not the perfect solution to privacy problems, since it works only locally, it could be helpful for tracking problems even if with some drawbacks: if all cookies of a session are deleted, the ones saving your settings or keeping the user logged in will be lost and the user will have to login manually every time.

5.1.3. Do Not Track

Do Not Track (DNT) is a proposed HTTP header field that is used to request websites and applications to disable tracking or cross-site user tracking.

The field was proposed in 2009 by researchers Christopher Soghoian, Sid Stamm and Dan Kaminsky (Soghoian, 2011) and has been added as an extension to the HTTP protocol in a document by the World Wide Web Consortium (W3C) (W3C, 2015).

The main purpose of the DNT header is to express the preference of a user related to the tracking behaviour of websites.

The header field can assume three different values: 1, if the user does not want to be tracked (opt out); 0, if the user consents to being tracked; or 'null', if the user has not yet expressed a preference.

The extension to the HTTP protocol to include the DNT header not only defines a way for users to express their preferences regarding the tracking, but it also enables servers to communicate their own settings regarding the tracking behaviour in a machine-readable form.

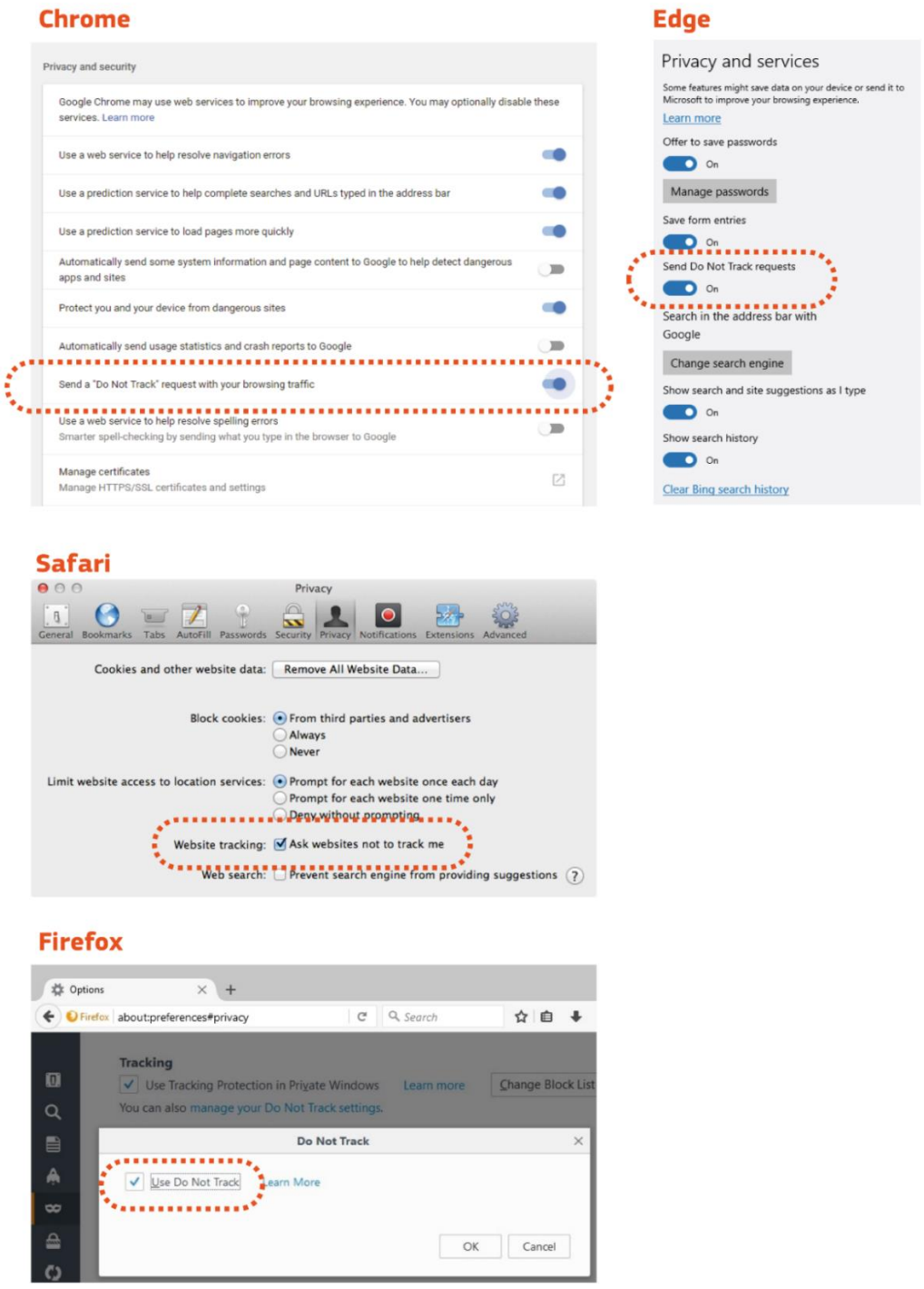
It offers means to declare:

- the identity of the site's owner (also known as the Data Controller);
- its tracking policy (purposes for which the collected personal data are used);
- the compliance regimes it operates under;
- the other host domains it controls;
- how consent can be given or revoked;
- how its tracking behaviour has been modified in the light of a specific tracking preference.

The W3C has developed several guides for the correct application of the DNT as well guides for the formal verification of its correct implementation. This is useful to meet the requirements of the GDPR and e-privacy directive, in particular the right to object to processing personal data or the requirement for prior consent.

The guide to the formal check of the compliance to the DNT was proposed on 7.3.2016 by W3C but, while it could help in the practical implementation of a useful tool for users, there is no legal obligation for web servers to consider the DNT header field. As such, servers can either honour a user's request not to be tracked (DNT field = 1) or can just discard the field while processing the HTTP request.

Figure 6: How to enable DNT in Chrome, Edge, Safari and Firefox



To grant users the ability to give their consent, even if they have the DNT field set to '1', several JavaScript Consent API (application programming interfaces) plugins, also known as tracking exception APIs, have been developed. This allows websites to register users'

consent. At the time of writing this report, not all browsers support the Consent API plugin and some have implemented it in a proprietary way.

To help users, some browsers have their own means to handle a white list of websites for which users want the DNT flag set to '0', for example to keep them logged on to a website or to maintain the so-called user experience with the customisation of a website.

5.1.4. Anti-tracking browser plugins

To better protect the privacy of users, several tools have been developed as plugins of web browsers.

In the following sections we give a description of some plugins that act from different perspectives.

Electronic Frontier Foundation plugins

Electronic Frontier Foundation (https://www.eff.org) is a non-profit organisation whose aim is to defend civil liberties in the digital world.

The organisation offers a collection of stand-alone programmes and plugins for several browsers to protect the privacy of users.

The projects are released under free or open-source licenses (e.g. the operating system GNU or the organisation Creative Commons) and are made publicly available.

The tools are the following:

- **Privacy Badger**: puts you back in control by spotting and then blocking third-party domains that seem to be tracking your browsing habits. This tool, on the other hand, allows contents from domains that respect the 'DNT' policy. In this way, they promote respect for users who want to maintain their anonymity.
- **Panopticlick**: is a tool that performs a detailed analysis of your browser fingerprint and attributes a 'uniqueness score', which should give users of the tool an idea of how easily identifiable they are through their browser.
- **HTTPS://Everywhere**: offered as an extension to several browsers, this tool has been developed together with the TOR Project (https://www.torproject.org/). The purpose is to encrypt the communication, whenever possible, while browsing. Some websites, though they may support HTTPS, do not use it in a consistent way or use HTTP as a default instead; there are even links from HTTPS pages to HTTP pages. By default, HTTPS://Everywhere rewrites all requests to websites to HTTPS, activating encryption to improve protection.
- **Certbot**: while the previous tool offers users a means to use HTTPS on websites, this tool offers website administrators a simple and effective way to set up HTTPS. Certbot is a client for the Let's Encrypt (https://letsencrypt.org/) certification authority, operated by the Internet Security Research Group (https://letsencrypt.org/isrg/). The tool will help website administrators to deploy Let's Encrypt certificates with easy-to-follow, interactive instructions based on webservers and operating systems.
- **Surveillance Self-Defence**: is a guide to introduce users to specific topics related to privacy and security, like threat modelling, the importance of strong passwords and protecting metadata. Together with this 'educational' side, this guide helps users to install and set up security-friendly software.

AdBlock

AdBlock is a free plugin available for all the most important web browsers on the market.

The purpose of the tool is to prevent the display of annoying pop-ups that could open while browsing and to block the tracking cookies.

The programme has a good impact concerning the protection of privacy of users, but since a lot of personal blogs and news websites earn money showing advertisements, web administrators are implementing countermeasures for people using AdBlock (e.g. showing only a small part of the contents of the page or not showing them at all).

Its usage is simple, with a 'deny by default' policy; but, if needed, every website can be added to a white list.

Figure 7: Example of a website before and after the activation of AdBlock with the removed advertisements highlighted

Anti-browser fingerprint

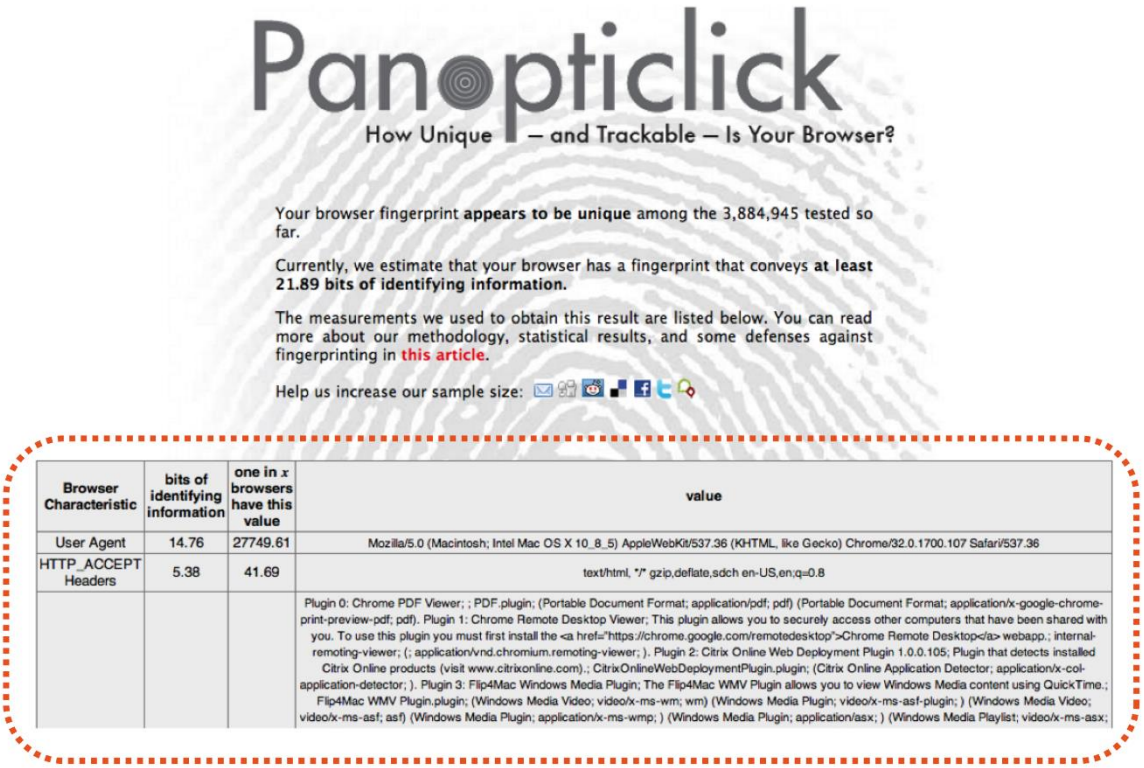
As said earlier (see paragraph 3.4), there are means to track users that are not based on data stored on their personal computer or smartphone.

To have a simple idea of how easily identifiable users are through their own browsers, it is enough to use the Panopticlick tool provided by the Electronic Frontier Foundation, which gives an idea of how easily it can be done through browser fingerprints.

Unless users do not want to constantly keep changing the parameters of their operating system and their browser itself to generate a different fingerprint, there are plugins for several browsers or those that are built ad hoc that prevent the fingerprint or confuse the methods that create the fingerprint.

The idea behind these plugins is to send false data related, for example, to the browser, the operating system or the language settings of users.

Figure 8: Analysis of the browser performed by Panopticlick with the specific settings of the browser taken into account for browser fingerprinting highlighted



5.1.5.'The onion router' and virtual private networks

There are some cases where avoiding fingerprinting or just deleting cookies is not enough to protect the privacy of the individual.

Some users need a further layer of protection in cases where the network traffic that they use is under surveillance or there are serious threats to their freedom or to their life.

In recent years, for example, some government institutions or regimes have performed mass surveillance and data collection. Without much effort, though, users should be able to simply protect their own confidential business activities and relationships, or even just their privacy, when connected to a public Wi-Fi hotspot. The use of a Virtual Private Network (VPN) could help in developing such protection.

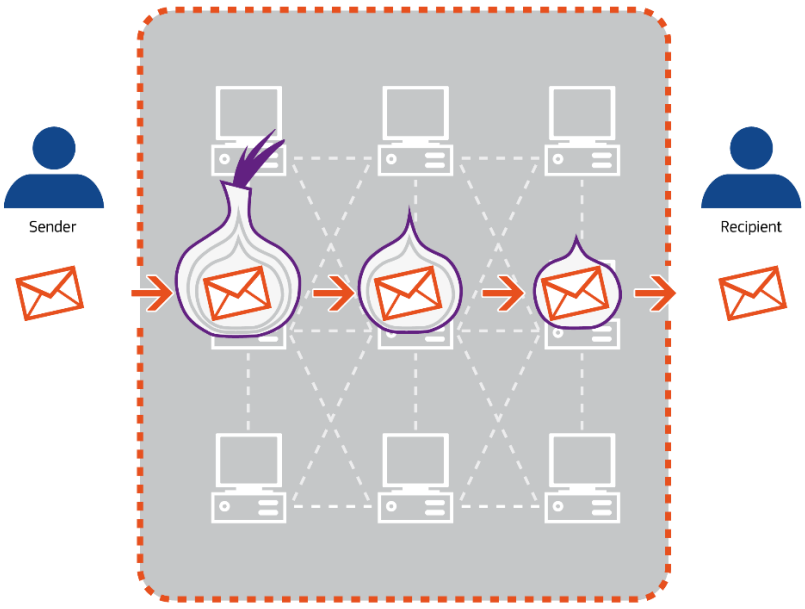
A VPN extends to the concept of a private network across a public network. This is achieved creating a (virtual) point-to-point connection through wide area networks.

Typically, VPNs only allow authenticated remote access using tunnelling protocols and encryption of data, thereby assuring:

- confidentiality: if the traffic is intercepted at the packet level, the eavesdropper will only collect encrypted data;
- sender authentication: because the access to the VPN is prevented to unauthorised users;
- message integrity: if the VPN also supports IPsec, a hash of the message will be used to verify the message itself upon reception.

A step ahead towards privacy protection is the use of 'The Onion Router' (TOR). The idea behind this project is to route the traffic coming from a user through an overlay network. The term 'onion' comes from the fact that the messages through the network are encapsulated into several layers of encryption, just like the layers of an onion. When the packets pass through the mesh of the network, at every hop a layer of encryption is removed, with the last layer removed when the message is received by the recipient.

Figure 9: The flow of a message inside the TOR network from a sender to a recipient



This kind of onion encryption assures that, at every hop, the current node knows only the preceding hop and the subsequent hop, but not the full virtual circuit or the content of the message. While a potential eavesdropper will only collect encrypted data. Furthermore, the

virtual circuit through the nodes that messages follow is recreated periodically by the TOR network.

6. User awareness and education

Nowadays, more and more users share huge amounts of data and personal information, sometimes without being fully aware of what and with whom they are sharing them.

Even the term 'privacy' does not have a globally recognised definition; and it is open to discussion and cultural influences. As a general attitude, privacy concerns are addressed by using the construct of perceived risk and trust.

As proposed by the first privacy theorists (Warren & Brandeis, 1890), the 'right to privacy' is acknowledged by the European Union as promoting a rights-based capacity-building model in line with the GDPR and the Commission's 'Digital4Development' approach.

6.1. Privacy concerns

Some initiatives have been put in place to assess EU citizens' perception on privacy and data protection. In the EU, according to the Eurobarometer survey on data protection, the protection of personal data is seen as an important concern for citizens. The central finding of the survey shows that trust in digital environments remains low. Two thirds of respondents (67 %) said that they are worried about not having any control over the information they provide online, while only 15 % feel they have complete control. This outcome confirms the need to finalise the data protection reform.

Within the scope of the 7th framework programme's funding, the PACT project, which stands for 'Public perception of security and privacy: assessing knowledge, collecting evidence, translating research into action' (European Commission, 2016), (PACT project, 2014)), ran from 2012 to 2015 with the aim of assessing existing knowledge about the relationship between security, privacy, trust and concern.

The PACT project has contributed to the further understanding of the sensitivity of privacy–security relations. The PACT provided insight into the tensions and arrangements raised by individuals in different fields; however, further research is needed when it comes to aspects of everyday life in technology-dense societies.

Finally, a practical lesson learned concerns the importance of dissemination and popularisation.

6.2. Digital competences

Education and user awareness are fundamental dimensions of an effective privacy safeguards strategy that also relies on the skills of those concerned.

As set out in the last Joint Communication to the European Parliament and the Council (European Commission, 2017) to render the EU better placed to face cybersecurity and privacy threats, the EU needs to affirm a resilient and complete strategy to boost citizens' skills in terms of technology, awareness and education.

To respond to this need, the Institute for Prospective Technological Studies of the Directorate General JRC, on behalf of DG Education, Youth, Sport and Culture and later on behalf of DG Employment, Social Affairs and Inclusion, already in 2013 developed and published a detailed **Digital Competence Framework** (Brecko Barbara, 2017). This framework, developed with intensive consultation of stakeholders, is tied to needs that every citizen faces when interacting with digital devices and environments, and it has become a general reference model for all EU Member States for many digital competence initiatives with the aim to create a common language on the development of digital competences.

This first paragraph aims to illustrate the possible tools conceived at European level to boost citizens' digital competences. Dedicated frameworks are available for enterprises, teachers, consumers and organisations.

The framework foresees 21 competences (with three proficiency levels), divided into five areas, which can be summarised as below:

(1) **Information and data literacy**: to articulate information needs and to locate and retrieve digital data, information and content; to judge the relevance of the source and its content; and to store, manage and organise digital data, information and content.

(2) **Communication and collaboration**: to interact, communicate and collaborate through digital technologies while being aware of cultural and generational diversity; to participate in society through public and private digital services and participatory citizenship; and to manage one's digital identity and reputation.

(3) **Digital content creation**: to create and edit digital content to improve and integrate information and content into an existing body of knowledge while understanding how copyright and licences are to be applied; and to know how to give understandable instructions for a computer system.

(4) **Safety**: to protect devices, content and personal data and privacy in digital environments; to protect physical and psychological health and to be aware of digital technologies for social well-being and social inclusion; and to be aware of the environmental impact of digital technologies and their use.

(5) **Problem solving**: to identify needs and problems and to resolve conceptual issues and complicated situations in digital environments; to use digital tools to innovate processes and products; and to keep up to date with the digital evolution.

In a prospective of a lifelong learning approach, DigComp is experiencing different phases. The result of the first phase is an update of the framework, named **DigComp 2.0** (Carretero Stephanie, 2017), with a focus on the conceptual reference model, new vocabulary and streamlined descriptors. In comparison with the first version, for example, new focuses are on **mobile devices**, **new environments, data literacy, privacy legislation** and **social inclusion** (Vourikari Riina, 2017).

Today, a new version is available. The current version is labelled **DigComp 2.1** (Carretero Gomez Stephanie, 2017) and focuses on expanding the initial three proficiency levels to a more fine-grained eight-level description as well as on providing examples of use for these eight levels. Its aim is to support stakeholders with the further implementation of DigComp.

Other related JRC works enhancing the development of digital competence have as results the following frameworks:

- **DigCompConsumers** (Brečko, 2017),
- **DigCompOrg** (Kampylis Panagiotis, European Framework for Digitally Competent Educational Organisations, 2016),
- **DigCompEdu** (Punie Yves, 2017).

A framework for opening up higher education institutions, called OpenEDU (Inamorato dos Santos Andreia, 2016), was also published in 2016, along with a competence framework for entrepreneurship called EntreComp (Bacigalupo Margherita, 2017). Some of these frameworks are accompanied by (self-)assessment instruments. Additional research has been undertaken on computational thinking, also known as CompuThink (Kampylis Panagiotis, The Computational Thinking Study, 2016), learning analytics, massive open online courses (MOOC) learners (MOOCKnowledge) (FERGUSON Rebecca, 2017) and MOOCs and free digital learning opportunities for migrants and refugees (MOOCs4inclusion) (Charalambos Vrasidas).

Table 1: DigComp 2.1

DigComp 2.0 (year 2016)		DigComp 2.1 (year 2017)	
Competence areas (dimension 1)	**Competences (dimension 2)**	**Proficiency levels (dimension 3)**	**Examples of use (dimension 5)**
1. Information and data literacy	1.1. Browsing, searching and filtering data, information and digital content 1.2. Evaluating data, information and digital content 1.3. Managing data, information and digital content	Eight proficiency levels for each of the 21 competences	Examples of use of the eight proficiency levels applied to learning and employment scenarios in the 21 competences
2. Communication and collaboration	2.1. Interacting through digital technologies 2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies 2.5. Netiquette 2.6. Managing digital identity		
3. Digital content creation	3.1. Developing digital content 3.2. Integrating and re-elaborating digital content 3.3. Copyright and licences 3.4. Programming		
4. Safety	4.1. Protecting devices 4.2. Protecting personal data and privacy 4.3. Protecting health and well-being 4.4. Protecting the environment		
5. Problem solving	5.1. Solving technical problems 5.2. Identifying needs and technological responses 5.3. Creatively using digital technologies 5.4. Identifying digital competence gaps		

6.3. Privacy safeguards and online anonymity in the DigComp

Digital transformation enhances new requirements and new vocabulary updates for digital competences. Already in its update of 2016 and now in its current version, the first area of DigComp has been updated from 'Information' to 'Information and data literacy'. This is to emphasise both the importance of data per se and the skills needed to critically evaluate and manage data in a safe and awareness-based way.

In competence area No 4, entitled 'Safety', Section 4.2 has also been renamed from 'Protection personal data' to 'Protection personal data and privacy'. This update aims at raising awareness about data privacy as a concept, meaning that data and technology are related to public and legal expectations of privacy (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016). According to DigComp, by acquiring digital skills on safety, users are able:

- to protect personal data and privacy in digital environments;
- to understand how to use and share personally identifiable information while being able to protect oneself and others from damages;
- to understand that digital services use a 'privacy policy' to inform how personal data are used.

Privacy and data protection, profiling and targeting and behavioural tracking are extensively analysed in the digital competence framework for consumers.

The most detailed taxonomy of possible problems related to privacy has been published by Solove (Solove, 2006), who groups the possible harms related to privacy into four categories:

- **Information Collection:**
    - Harms: *Surveillance*, *Interrogation*
- **Information Processing:**
    - Harms: *Aggregation, Identification, Insecurity, Secondary Use, Exclusion*
- **Information Dissemination:**
    - Harms: *Breach of Confidentiality, Disclosure, Exposure, Increased Accessibility, Blackmail, Appropriation, Distortion*
- **Invasion:**
    - Harms: *Intrusion, Decisional Interference*.

While some of the harms are recognised crimes (e.g. blackmail, appropriation and distortion) that already had (before the 'digital world') specific laws to prevent and punish them, others instead become 'problems' only after a threshold (e.g. surveillance, interrogation), otherwise they are perfectly legitimate if performed by law enforcement agencies following the law and respecting human rights.

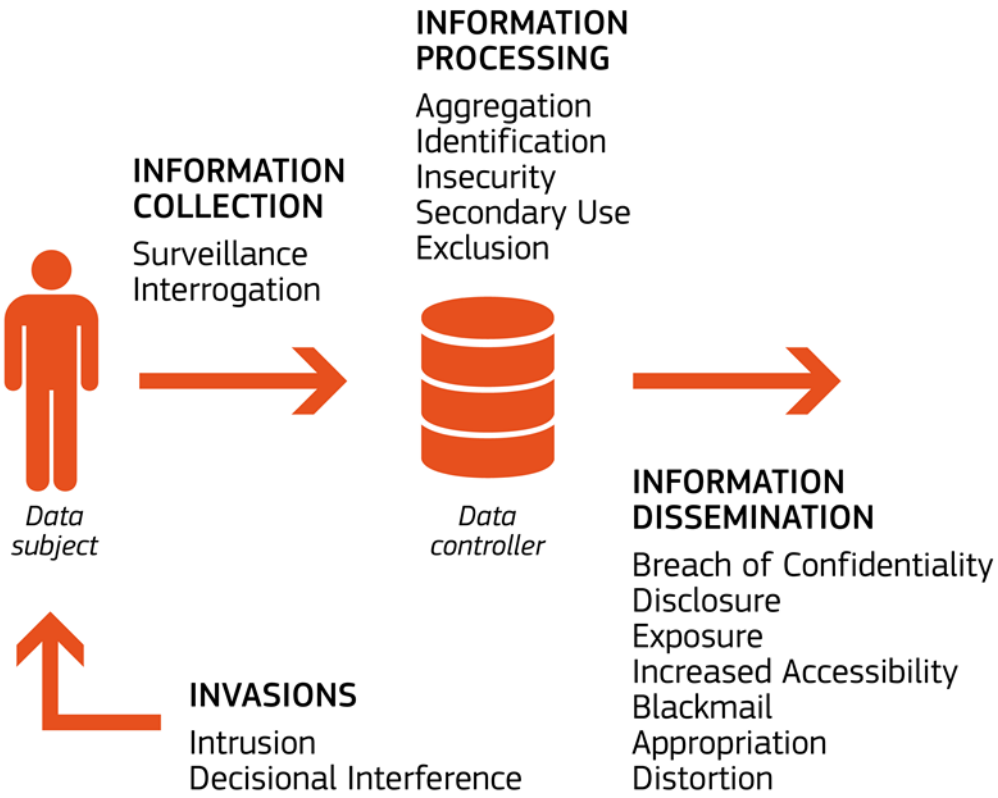
Table 2: Solove's taxonomy

A Taxonomy of Privacy Harms (compiled from (Solove, 2006))		
Domain	**Privacy breach**	**Description**
Information Collection	Surveillance	Watching, listening to, or recording of an individual's activities
	Interrogation	Various forms of questioning or probing for information
Information Processing	Aggregation	The combination of various pieces of data about a person
	Identification	Linking information to particular individuals
	Insecurity	Carelessness in protecting stored information from leaks and improper access
	Secondary Use	Use of information collected for one purpose for a different purpose without the data subject's consent
	Exclusion	Failure to allow the data subject to know about the data that others have about her and participate in its handling and use, including being barred from being able to access and correct errors
Information Dissemination	Breach of Confidentiality	Breaking a promise to keep a person's information confidential
	Disclosure	Revelation of information about a person that impacts the way others judge her character
	Exposure	Revealing another's nudity, grief, or bodily functions
	Increased Accessibility	Amplifying the accessibility of information
	Blackmail	Threat to disclose personal information
	Appropriation	The use of the data subject's identity to serve the aims and interests of another
	Distortion	Dissemination of false or misleading information about individuals
Invasion	Intrusion	Invasive acts that disturb one's tranquillity or solitude
	Decisional Interference	Incursion into the data sunject's decisions regarding her private affairs

In this report, with reference to Solove's taxonomy in the digital domain, we deemed it worthy to provide possible practical scenarios where digital competences are identified to complement technical and legal resources seen as strategies to deal with privacy harms.

In the following, we analyse the privacy harms in four different sections (one for each category identified by Solove). At the end of each section corresponding to a specific domain, there is a table that summarises the findings.

Figure 10: Privacy harms as grouped by Solove



In the table, the first two columns refer to Solove's taxonomy:

1. the privacy harm itself;
2. the description of the specific privacy harm (Robin Mansell, 2015).

The second group of columns refers to the tools that could be helpful to prevent or resolve the specific harm:

3. legal resources ([1]);
4. technical resources.

The third group of columns refers to the Digital Competence Framework (DigComp 2.1):

5. Competence Area (dimension 1);
6. Competences (dimension 2).

While DigComp 2.1, together with the previously named dimensions, foresees the proficiency levels, we have decided not to include them. Our indications should therefore not be considered a difficulty for users who do not have a minimum level of proficiency.

([1]) The content of this column does not at all intend to be an exhaustive list of tools offered by the legislation. With regards the articles suggested, they could only apply in specific circumstances. Furthermore, some of the problems related to privacy, as identified by Solove, were already addressed by the legislation before the existence of the 'digital world'.

Privacy is a hot topic of discussion, in particular for the online life of individuals. All privacy problems involve personal data or sensitive information. In the digital competence framework, we identified some competences that apply in the prevention and/or solution of almost all privacy harms identified by Solove:

1.3. Managing data, information and digital content: all harms related to privacy involve data management, thus careful handling of data and information by users is needed;

2.2. Sharing through digital technologies: users should pay attention to what and with whom they are going to share information online;

2.3. Engaging in citizenship through digital technologies: users should participate in society through the use of public and private digital services and should seek opportunities for self-empowerment. Furthermore, users should actively participate as citizens of the digital world through appropriate technologies;

2.4. Collaborating through digital technologies: thanks to digital tools, users should collaborate with other persons and law enforcement agencies to build knowledge related to privacy harms (e.g. report privacy harms in which they were involved) and to raise awareness;

2.6. Managing digital identity: users should be able to manage and protect their own online data, information and reputation that build their own digital identity (or multiple identities);

4.2. Protecting personal data and privacy: users should protect personal data and privacy in digital environments. They should understand how to use and share personally identifiable information in a safe and responsible way. They should also be able to protect themselves and others from damages. Furthermore, users should understand that digital services use a 'privacy policy' to inform how personal data are used;

4.3. Protecting health and well-being: users should be aware of possible risks or threats, both physical and psychological, arising from privacy harms. In addition, users should be able to protect themselves and others from those dangers and should use, if possible, digital technologies for social well-being and inclusion in order to fight those harms;

5.4. Identifying digital competence gaps: users who operate in the digital world should improve their digital competences to be able to identify possible risks and try to solve them, either alone or by asking for help from a proficient user. Likewise, proficient users should provide support to those who do not have a sufficient proficiency level.

In the following section, we are going to analyse each privacy harm identified by Solove by placing it in a digital context. We will provide a description of the specific harm and an example to allow readers to better understand the harm itself. **The examples provided are inspired by real and recent cases, but not necessarily ones that happened in the European Union**.

6.4. Information Collection

6.4.1. Surveillance

Description: 'The watching, listening to or recording of an individual's activities' (Robin Mansell, 2015).

'What is the harm if people or the government watch or listen to us? Certainly, we all watch or listen, even when others may not want us to, and we often do not view this as problematic. However, when done in a certain manner — such as continuous monitoring — surveillance has problematic effects. For example, people expect to be looked at when they ride the bus or subway, but persistent gawking can create feelings of anxiety and discomfort.

Not only can direct awareness of surveillance make a person feel extremely uncomfortable, but it can also cause that person to alter her behaviour. Surveillance can lead to self-censorship and inhibition. Because of its inhibitory effects, surveillance is a tool of social control, enhancing the power of social norms, which work more effectively when people are being observed by others in the community. […] This aspect of surveillance does not automatically make it harmful, though, since social control can be beneficial and every society must exercise a sizeable degree of social control. […] Too much social control, however, can adversely impact freedom, creativity, and self-development.' (Solove, 2006)

As a general rule, surveillance has for a long time been considered as troubling, in particular if it is set up with the purpose of spying on or invading the privacy of the persons being spied upon. Video surveillance and audio surveillance enable the same perceptions and can create feelings of anxiety and discomfort. Another point is that surveillance can have a chilling effect on behaviour, when one is aware of the possibility of surveillance. This conformity to the rules effect is known as panoptic, based on Jeremy Bentham's architectural design for a prison building he called the Panopticon. Nevertheless, surveillance is applied as a deterrent to crime and some people desire the discipline and control that surveillance can bring. In this sense, surveillance can be perceived as a guardian with a 'friendly eye on their lives'.

Example: Let us assume that a European citizen travels to a country where the regime reduces the freedom of expression, analysing the internet traffic passing through the national gateways and performing censorship.

Possible means for prevention and/or resolution:

In such cases, there are several solutions like using anonymisers to perform the most common activities online (disposable email accounts, pseudo-anonymisers for electronic payments, etc.). Furthermore, by passing through VPNs or the TOR network, the traffic generated by the user is encrypted, so the traffic is harder to be analysed by an eavesdropper.

Digital competences involved:

The use of such tools requires that users have a sufficient level of skills to set them up. The digital competences involved in the management of this problem include 1.3, 2.2, 2.3, 2.4, 2.6, 4.2, 4.3 and 5.4 (see paragraph 6.2). Furthermore, alongside the abovementioned, the following ones are also needed:

- '4.1. Protecting devices' *(*unprotected devices can be easily kept under surveillance by malicious intent);
- '5.1. Solving technical problems';
- '5.2. Identifying needs and technological responses'.

6.4.2. Interrogation

Description: 'Various forms of questioning or probing for information' (Robin Mansell, 2015).

'Interrogation is the pressuring of individuals to divulge information. Interrogation has many benefits; it is useful for ferreting out information that others want to know.

However, interrogation can create harm. Part of this harm arises from the degree of coerciveness involved. […] However, for interrogation generally, the compulsion need not be direct; nor must it rise to the level of outright coercion. Compulsion can consist of the fear of not getting a job or of social opprobrium. People take offense when others ask an unduly probing question — even if there is no compulsion to answer. One explanation may be that people still feel some degree of compulsion because not answering might create the impression that they have something to hide. This is why, I believe, there are social norms against asking excessively probing or prying questions: they make the person being questioned feel uncomfortable. Interrogation forces people to be concerned about how they will explain themselves or how their refusal to answer will appear to others.

Interrogation resembles intrusion in its invasiveness, for interrogation is a probing, a form of searching. Like disclosure, interrogation often involves the divulging of concealed information; unlike disclosure, interrogation can create discomfort even if the information is barely disseminated. To some degree, surveillance resembles interrogation, for both involve the involuntary gathering of information. Interrogation, however, occurs with the conscious awareness of the subject; surveillance can be clandestine.' (Solove, 2006)

Interrogation can have some benefits and it can be useful during some activities, as for example the interrogation of suspects in criminal investigations. However, depending on the grade of coerciveness involved, interrogation can create uncomfortable feelings. Moreover, a skilled interrogator can orchestrate a dialogue to elicit specific responses. Communication and persuasion methods are also applied in information and communications technology in order to create individuals' disclosure.

Example: Although the interrogation issue can be put in place outside the digital context, we may assume that third parties can deliberately try to extort information from internet users. The issue could take place through digital technologies (e.g. Skype, WhatsApp, text chat or VoIP, through which users might share any kind of information). A user registered on a social network could receive a request of 'friendship' by another user that they do not know. The second user could start asking the first user for personal information.

Possible means for prevention and/or resolution:

Users should be able to understand the possible risks of answering detailed questions and evaluate if the other party can be trusted.

The only countermeasure against interrogation, if there is no coercion, is good sense:

- if you receive a message from somebody pretending to be a data controller that asks for your user name or password, it is probably (almost certainly) a scam email;
- if somebody that you do not know (or you know very little about them) starts to question you about personal data, it is not a good idea to reveal too much.

Since the hardest part related to the prevention of interrogation performed online is the evaluation of trust, interrogation is a problem for minors in particular. For this reason, it is important to perform awareness-raising campaigns.

Digital competences involved:

The digital competences involved in the management of this problem include 1.3, 2.2, 2.3, 2.4, 2.6, 4.2, 4.3 and 5.4 (see paragraph 6.2).

To manage this issue, the following digital competence is desirable:

- '1.2. Evaluating data, information and digital content' (user should be able to critically evaluate to whom they are answering and if they can be trusted).

Table 3: Information Collection

Information Collection					
Privacy harm	**Description**	**Possible means for prevention and/or resolution**		**Digital competencies involved**	
		Legal resources	**Technical resources**	**Area (dimension 1)**	**Competence (dimension 2)**
Surveillance	*'The watching, listening to, or recording of an individual's activities'*	GDPR (e.g. Articles 5, 6, 7, 9, 10, 12, 13, 14 and 23). —	Communication anonymiser (e.g. TOR, VPNs, disposable email addresses, pseudonyms for online payment)	1. Information and data literacy	1.3. Managing data, information and digital content
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies 2.6. Managing digital identity
				3. Digital content creation	—
				4. Safety	4.1. Protecting devices 4.2. Protecting personal data and privacy 4.3 Protecting health and well-being
				5. Problem solving	5.1. Solving technical problems 5.2. Identifying needs and technological responses 5.4. Identifying digital competence gaps
Interrogation	*'Various forms of questioning or probing for information' (possibly also with coercion)*	See end of p. 32		1. Information and data literacy	1.2. Evaluating data, information and digital content 1.3. Managing data, information and digital content
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies 2.6. Managing digital identity
				3. Digital content creation	—
				4. Safety	4.2. Protecting personal data and privacy 4.3. Protecting health and well-being
				5. Problem solving	5.4. Identifying digital competence gaps

6.5. Information Processing

6.5.1. Aggregation

Description: 'The combination of various pieces of data about a person' (Robin Mansell, 2015).

'Aggregation is the gathering together of information about a person. A piece of information here or there is not very telling. But when combined together, bits and pieces of data begin to form a portrait of a person. The whole becomes greater than the parts. This occurs because combining information creates synergies. When analyzed, aggregated information can reveal new facts about a person that she did not expect would be known about her when the original, isolated data was collected.

Aggregating information is certainly not a new activity. It was always possible to combine various pieces of personal information, to put two and two together to learn something new about a person. But aggregation's power and scope are different in the Information Age; the data gathered about people is significantly more extensive, the process of combining it is much easier, and the computer technologies to analyze it are more sophisticated and powerful.

Combining data and analyzing it certainly can be put to beneficial uses. Amazon.com, for example, uses aggregated data about a person's book-buying history to recommend other books that the person might find of interest. […] These developments make sense in a world where there are billions of people and word-of-mouth is insufficient to assess reputation.

Alongside these benefits, however, aggregation can cause dignitary harms because of how it unsettles expectations. People expect certain limits on what is known about them and on what others will find out. Aggregation upsets these expectations, because it involves the combination of data in new, potentially unanticipated ways to reveal facts about a person that are not readily known.' (Solove, 2006)

Everyone selectively spreads pieces of information in their daily activities, offline and online, and the boundaries of such disclosure is decided by the data subject, who probably reveals very little about themselves. The perception of this disclosure can indeed change in case of aggregation of data, as it can reveal much more than what one expected when one provided data separately.

Example: Several online market places make use of the information provided by users both directly and/or by their browsing history to create a profile of them. These websites might identify users because they are not logged into the service according to public records. Nevertheless, by aggregating and merging data they can get an idea about users' preferences and make some inferences. Those inferences are then used to propose products to users that they could be interested in and to increase the chances of a purchase.

Possible means for prevention and/or resolution:

The aggregated data could be useful for the data subject in some circumstances like online shopping. By analysing a data subject's behaviour and browsing activity, a web shop proposes specific products that users with a similar history found interesting.

Sometimes data collection and aggregation go too far, like when it is not strictly needed or when users do not want it.

As a first measure to prevent aggregation, users should be aware of the possible risks of their actions online and how they can be tracked and profiled.

Users could reduce the risk of providing too much data while performing their online activities using:

- private browsing sessions;
- DNT;
- anti-tracking plugins (available for the most widespread browsers);
- anonymisers for payments and disposable email addresses.

Users could further reduce the information provided by disabling the GPS on their mobile device when it is not needed and when taking pictures (or disabling the function to geotag them).

Moreover, in the GDPR, the following articles are related to aggregation:

- Article 13: information to be provided where personal data are collected from the data subject;
- Article 21: right to object;
- Article 22: automated individual decision-making, including profiling.

Digital competences involved:

The digital competences involved in the management of this problem include 1.3, 2.2, 2.3, 2.4, 2.6, 4.2, 4.3 and 5.4 (see paragraph 6.2).

Furthermore:

- '1.2. Evaluating data, information and digital content' (users should be able to critically evaluate if the third party processing their personal data can be trusted);
- '5.2. Identifying needs and technological responses' (users should be able to evaluate whether they need further protection while browsing online and apply countermeasures if need be).

6.5.2. Identification

Description: 'The linking of information to a particular individual' (Robin Mansell, 2015) (this can be with high or low aggregation).

''Identification' is connecting information to individuals. […] Identification is related to disclosure in that both involve the revelation of true information. Identification involves a particular form of true information (one's identity), which enables databases of information to be linked to people. Identification is similar to aggregation as both involve the combination of different pieces of information, one being the identity of a person. However, identification differs from aggregation in that it entails a link to the person in the flesh. For example, there can be extensive aggregations of data about a person in many databases, but these aggregations might be rarely connected to that person as she goes through her day-to-day activities. This is a situation involving high aggregation and low identification. On the flip side, one can have high identification and low aggregation, such as in a world of checkpoints, where people constantly have to show identification but where there are few linkages to larger repositories of data about people.

Identification has many benefits. In order to access various accounts, people's identity must be verified, a step that can reduce fraud and enhance accountability.[…] Although identification of people or sources of particular messages can be beneficial, it also creates problems.[…] Identification goes a step further—it links the digital person directly to a person in real space.[..] Identification can inhibit one's ability to be anonymous or pseudonymous.

Anonymity and pseudonymity protect people from bias based on their identities and enable people to vote, speak, and associate more freely by protecting them from the danger of reprisal.' (Solove, 2006)

Identification can be perceived as demeaning to dignity, as some argue that it reduces people to a number of bodily characteristics or data. According to Solove '[…] identification is a means to link people to data, not necessarily an indication that people are the equivalent of their identifying characteristics.' Identification markers like scarlet letters, tattoos or branding have been used in different social contexts to recognise people belonging to specific social categories, and often they bear particular stigmas. This can bring to people's inhibition ability to change and disclosure. On the contrary, non-expressive means of identification such as fingerprints identify people without signalling anything to the public. Anonymity can enhance prejudice reduction and increase online safety.

Example: Services like Pleaserobme or WeKnowYourHouse are good examples to illustrate how information shared online can be used (or misused) when it is linked to persons outside the digital world.

While the names of those Twitter accounts are a little bit alarmist, as explained also in Chapter 3.3, they are used only to raise awareness among users, with the aim to teach them not to overshare.

Possible means for prevention and/or resolution:

The first tool to prevent problems that derive from identification is education. Users should be able to discriminate trusted persons and/or sources and be able to understand which information they should disclose or not.

The technical tools that users should use are the same that were suggested for aggregation, keeping in mind that those tools are not helpful at all if users are inclined to share information with non-trusted parties.

Digital competences involved:

The digital competences involved in the management of this problem include 1.3, 2.2, 2.3, 2.4, 2.6, 4.2, 4.3 and 5.4 (see paragraph 6.2).

Furthermore:

- '1.2. Evaluating data, information and digital content' (users should be able to critically evaluate if the third party processing their personal data can be trusted);
- '5.2. Identifying needs and technological responses' (users should be able to evaluate whether they need further protection while browsing online and apply countermeasures if need be).

6.5.3. Insecurity

Description: 'Carelessness in protecting stored information from leaks and improper access' (Robin Mansell, 2015).

'Insecurity, in short, is a problem caused by the way our information is handled and protected. […] Insecurity exposes people to potential future harm. […] Many privacy statutes require that information be kept secure.' (Solove, 2006)

In this issue, two entities might be responsible for the insecurity risks: the data subject and the data controller.

Example: Insecurity in itself is not a problem for privacy, but it can be the cause of several other problems related to privacy. Let us suppose that an online shop does not use the minimum cryptographic standard to protect the data (in particular credit card numbers) of their customers. In the case of data breach, those data can easily be read by whomever.

Insecurity can be the cause of several other harms identified by Solove:

- surveillance and intrusion: insecurity in a domestic network could allow the unauthorised access by other users;
- breach of confidentiality, disclosure, exposure, identification, secondary use, blackmail and appropriation: insecurity in the network of a data controller can cause data breaches that could lead to a loss of trust in the data controller from the data subject as well as various harms, according to the kind of information that has been leaked.

Possible means for prevention and/or resolution:

Users should be able to understand their level of proficiency to evaluate if they need help to fix security holes. A common best practice is to update the operating system, the applications used and the antivirus as soon as a new patch is available to avoid malicious users from taking advantage of possible vulnerabilities left unresolved.

Users should also be able to evaluate which information everybody can see and which can only be seen by friends or trusted persons/websites, and consequently act to restrict the access to the most sensitive pieces of information.

As for the data controller, the GDPR establishes some specific articles (and heavy fines) that should be sufficient to put pressure on the data controller to invest in the security of their infrastructure.

Digital competences involved:

The digital competences involved in the management of this problem include 1.3, 2.2, 2.3, 2.4, 2.6, 4.2, 4.3 and 5.4 (see paragraph 6.2).

Furthermore:

- '1.2. Evaluating data, information and digital content' (users should be able to critically evaluate if the third party processing their personal data can be trusted);
- '4.1. Protecting personal data and privacy';
- '5.1. Solving technical problems' (if users detect a problem related to their devices, they should be able to solve it or ask somebody (trusted) with a sufficient proficiency level to solve it);
- '5.2. Identifying needs and technological responses' (users should be able to evaluate whether they need further protection while browsing online and apply countermeasures if need be).

6.5.4. Secondary use

Description: 'Secondary use of information collected for one purpose without the data subject's consent' (Robin Mansell, 2015).

''Secondary use' is the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject's consent. There are certainly many desirable instances of secondary use. Information might be used to stop a crime or to save a life. The variety of possible secondary uses of data is virtually infinite, and they range from

benign to malignant.[…] Secondary use can cause problems.[…] Secondary uses thwart people's expectations about how the data they give out will be used. People might not give out data if they know about a potential secondary use, such as for telemarketing, spam, or other forms of intrusive advertising.[…] The potential for secondary use generates fear and uncertainty over how one's information will be used in the future, creating a sense of powerlessness and vulnerability. In this respect, secondary use resembles the harm created by insecurity. […] Secondary use also creates architectural problems. The secondary use of information can create problems because the information may not fit as well with the new use. When removed from the original context in which it was collected, data can more readily be misunderstood.' (Solove, 2006)

Even though there are benign secondary uses of data (e.g. saving a life, stopping crime), this harm can be perceived as a breach of confidentiality (see paragraph 6.6.1), as it involves using information in ways that a person does not consent to and might not find desirable. Even for those privacy policies stating that information might be used in secondary ways, people do not always read and/or do not (completely) understand these policies and have little idea about the range of potential secondary uses.

Example: Let us assume that an online platform that hosts online petitions asks for the consent of voters for the petition to treat their data only for the petitions subscribed. If the online platform starts to sell those data for marketing purposes, some of the specific interests of users can be inferred from the subscribed petitions.

Of course this is a secondary use for which subscribers of the petitions did not provide their consent.

Possible means for prevention and/or resolution:

The first tool to be protected from secondary use is to carefully read the terms and conditions of a service upon registration. When users are going to give consent for specific services, they should also be aware that (unless special conditions hold) the data controller is not allowed to perform actions for which it does not have consent.

The GDPR is clear concerning the meaning of 'consent', how it should be requested and the conditions that make it valid. Several articles give details about the special processing of personal data for which explicit consent from the data subject is not needed and, at the same time, they restrict the unauthorised processing of those data.

Digital competences involved:

The digital competences involved in the management of this problem include 1.3, 2.2, 2.3, 2.4, 2.6, 4.2, 4.3 and 5.4 (see paragraph 6.2).

Furthermore:

- '1.2. Evaluating data, information and digital content' (users should be able to critically evaluate if the third party processing their personal data can be trusted);
- '4.1. Protecting personal data and privacy';
- '5.1. Solving technical problems' (if users detect a problem related to their devices, they should be able to solve it or ask somebody (trusted) with a sufficient proficiency level to solve it);
- '5.2. Identifying needs and technological responses' (users should be able to evaluate whether they need further protection while browsing online and apply countermeasures if need be).

6.5.5. Exclusion

Description: '*The failure to allow the data subject to know about the data that others have about his/her and participate in its handling and use'* (Robin Mansell, 2015).

'I refer to the failure to provide individuals with notice and input about their records as exclusion. […] it is a harm created by being shut out from participating in the use of one's personal data, by not being informed about how that data is used, and by not being able to do anything to affect how it is used. […] As with secondary use and insecurity, exclusion creates a sense of vulnerability and uncertainty in individuals. An inability to participate in the maintenance and use of one's information can lead to feelings of powerlessness and frustration.' (Solove, 2006)

The inability to participate in the managing and use of one's personal information can lead to feelings of powerlessness and frustration, especially when one party stands in a special position of power over another person.

Example: Let us assume that a user registers on an online shop and gives their consent to the shop to manage the data provided. Now the online shop is the data controller of the information related to the user (the data subject). Let us suppose that the same user, after a while, no longer uses the services provided by the website and wants to delete his/her personal information stored by the data controller. Of course, if there is no special reason for the data controller to preserve the data related to the user, the user must be able to modify and/or delete them.

Possible means for prevention and/or resolution:

Users should be aware that they have the right to access their own personal data collected by the data controller, which is explicitly stated in Article 15 of the GDPR (Right of access). Furthermore, the GDPR grants users other rights to manage their own personal data, like:

- The right to rectification,
- The right to data portability,
- The right of erasure.

Digital competences involved

The digital competences involved in the management of this problem include 1.3, 2.2, 2.3, 2.4, 2.6, 4.2, 4.3 and 5.4 (see paragraph 6.2).

Furthermore:

- '1.2. Evaluating data, information and digital content' (users should be able to critically evaluate if the third party processing their personal data can be trusted).

Table 4: Information Processing

Information Processing					
Privacy harm	**Description**	**Possible means for prevention and/or resolution**		**Digital competencies involved**	
		Legal resources	**Technical resources**	**Area (dimension 1)**	**Competence (dimension 2)**
Aggregation	*'The combination of various pieces of data about a person'*	GDPR (e.g. Articles 13, 21 and 22)	Countermeasures to tracking	1. Information and data literacy	1.2. Evaluating data, information and digital content 1.3. Managing data, information and digital content
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies 2.6. Managing digital identity
				3. Digital content creation	—
				4. Safety	4.2. Protecting personal data and privacy 4.3. Protecting health and well-being
				5. Problem solving	5.2. Identifying needs and technological responses 5.4. Identifying digital competence gaps
Identification	*'The linking of information to a particular individuals'* (this can be with high or low aggregation)	GDPR (e.g. Articles 13, 21 and 22).	Countermeasures to profiling	1. Information and data literacy	1.2. Evaluating data, information and digital content 1.3. Managing data, information and digital content
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies 2.6. Managing digital identity
				3. Digital content creation	—
				4. Safety	4.2. Protecting personal data and privacy 4.3. Protecting health and well-being
				5. Problem solving	5.2. Identifying needs and technological responses 5.4. Identifying digital competence gaps
Insecurity	*'Carelessness in protecting stored information from leaks and improper access'*	GDPR (e.g. Articles 24, 25, 32, 33 and 34)	User awareness and education to privacy management	1. Information and data literacy	1.2. Evaluating data, information and digital content 1.3. Managing data, information and digital content
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies

					2.6. Managing digital identity
				3. Digital content creation	—
				4. Safety	4.2. Protecting personal data and privacy 4.3. Protecting health and well-being
				5. Problem solving	5.1. Solving technical problems 5.2. Identifying needs and technological responses 5.4. Identifying digital competence gaps
Secondary Use	*'Secondary use of information collected for one purpose without the data subject's consent'*	GDPR (e.g. Articles 5, 6 and 13(3))		1. Information and data literacy	1.2. Evaluating data, information and digital content 1.3. Managing data, information and digital content
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies 2.6. Managing digital identity
				3. Digital content creation	—
				4. Safety	4.2. Protecting personal data and privacy 4.3. Protecting health and well-being
				5. Problem solving	5.1. Solving technical problems 5.2. Identifying needs and technological responses 5.4. Identifying digital competence gaps
Exclusion	*'The failure to allow the data subject to know about the data that others have about his/her and participate in its handling and use'*	GDPR (e.g. Article 15)		1. Information and data literacy	1.2. Evaluating data, information and digital content 1.3. Managing data, information and digital content
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies 2.6. Managing digital identity
				3. Digital content creation	—
				4. Safety	4.2. Protecting personal data and privacy 4.3. Protecting health and well-being
				5. Problem solving	5.4. Identifying digital competence gaps

6.6. Information Dissemination

6.6.1. Breach of confidentiality

Description: '*The breaking of a promise to keep a person's information confidential'* (Robin Mansell, 2015).

'The harm from a breach of confidence, then, is not simply that information has been disclosed, but that the victim has been betrayed. […] Breach of confidentiality requires only a betrayal of trust, regardless of the nature of the data revealed. […] When people establish a relationship with banks, Internet service providers, phone companies, and other businesses, they are not disclosing their information to the world. They are giving it to a party with implicit (and often explicit) promises that the information will not be disseminated.' (Solove, 2006)

Breach of confidentiality violates the trust in a specific relationship and can create a feeling of disillusion and frustration.

6.6.2. Disclosure

Description: '*The revelation of truthful information about a person that impacts the way others judge his/her character'* (Robin Mansell, 2015).

''Disclosure' occurs when certain true information about a person is revealed to others. Disclosure differs from breach of confidentiality because the harm in disclosure involves the damage to reputation caused by the dissemination; the harm with breach of confidentiality is the violation of trust in the relationship. […] Although protecting against disclosure does limit freedom of speech, disclosure can inhibit the very interests free speech protects. Protection from disclosure, like free speech, promotes individual autonomy. The risk of disclosure can prevent people from engaging in activities that further their own self-development. Second, as with free speech, disclosure protections further democratic self-governance. […] Disclosure can inhibit people from associating with others, impinging upon freedom of association, and can also destroy anonymity, which is sometimes critical for the promotion of free expression. Disclosure can also threaten people's security. […] People want to protect information that makes them vulnerable or that can be used by others to harm them physically, emotionally, financially, and reputationally.' (Solove, 2006)

Disclosing a private matter can be perceived as highly offensive when it is not a legitimate concern to the public.

6.6.3. Exposure

Description: '*revealing another's sensitive or personal activities such as nudity, grief, or bodily functions'* (Robin Mansell, 2015).

'These are all illustrations of a disruption I call 'exposure.' Exposure involves the exposing to others of certain physical and emotional attributes about a person. These are attributes that people view as deeply primordial, and their exposure often creates embarrassment and humiliation. Grief, suffering, trauma, injury, nudity, sex, urination, and defecation all involve primal aspects of our lives—ones that are physical, instinctual, and necessary. We have been socialized into concealing these activities.

Although exposure is similar to disclosure—both involve the dissemination of true information—they diverge in an important respect. Exposure is related to disclosure in that

concealed information is revealed to others, but the information is not revealing of anything we typically use to judge people's character. Unlike disclosure, exposure rarely reveals any significant new information that can be used in the assessment of a person's character or personality.

Exposure creates injury because we have developed social practices to conceal aspects of life that we find animal-like or disgusting. Further, in certain activities, we are vulnerable and weak, such as when we are nude or going to the bathroom. […] The need for privacy, and therefore the prevention of exposure, is created by the fact that we have social relationships and concomitant norms of dignity and decorum. […] When these practices are disrupted by exposure, people can experience a severe and sometimes debilitating humiliation and loss of self-esteem. Exposure thus impedes a person's ability to participate in society.' (Solove, 2006)

Examples: Let us consider the case of a data breach involving the passwords used for one's email server and let us assume that the same password(s) are used for both a user's email and their mobile device (as is the case for iPhone and Android). In case of data breach, the user should react as fast as possible to change the password(s) to avoid any risk related to the devices' content as well as to future email traffic. Indeed, the user should be aware of the meaning beyond the concept of *data breach*.

While a data breach is a big problem for the spread of personal information, there are several other ways this could happen: for example, secrets told to a friend that are then not maintained so secretly, or pictures posted or phrases written online thinking that they are anonymous only to find out that they are associated back to the posting individual.

Possible means for prevention and/or resolution:

Again, concerning prevention, most of the work is left to be done for the data controller.

Concerning users, they should carefully evaluate the party with whom they are going to share information.

Should users realise that data and information have already been made available to the public, therefore circulated, they could refer and apply the Right of erasure foreseen by Article 17 of the GDPR. Users could also undertake legal measures at national level to limit damages resulting from the *data breach*.

Digital competences involved:

We consider these three problems together, since the digital competencies involved, both in the management and in the prevention, are the same.

The digital competences involved in the management of this problem include 1.3, 2.2, 2.3, 2.4, 2.6, 4.2, 4.3 and 5.4 (see paragraph 6.2).

Furthermore:

- '1.2. Evaluating data, information and digital content' (users should be able to critically evaluate if the third party processing their personal data can be trusted);
- '4.1. Protecting personal data and privacy';
- '5.1. Solving technical problems' (if users detect a problem related to their devices, they should be able to solve it or ask somebody (trusted) with a sufficient proficiency level to solve it);
- '5.2. Identifying needs and technological responses' (users should be able to evaluate whether they need further protection while browsing online and apply countermeasures if need be).

6.6.4. Increased accessibility

Description: *'The amplification of the accessibility of information'* (Robin Mansell, 2015).

'Increased accessibility does not involve a direct disclosure. Secret information is not disclosed. Rather, information that is already available to the public is made easier to access. Unlike disclosure, the harm is not a direct revealing of information to another. Confidentiality is not breached; the cat is already out of the bag. With increased accessibility, a difference in quantity becomes a difference in quality—it enhances the risk of the harms of disclosure. Increased accessibility to personal information has many benefits. It enhances openness, allowing people to locate information that they are seeking more easily. […] Increased accessibility, however, creates problems such as the increased possibility of disclosure. Information can readily be exploited for purposes other than those for which it was originally made publicly accessible.' (Solove, 2006)

Example: The problem seems to be similar to that of *aggregation*, even though in this case we are considering specific data stored in specific records. It can happen that those records are made too easily accessible.

For example, let us assume that bankruptcy was recorded for an individual, who in the meantime has repaid the outstanding debt and now has a stable financial situation. The recorded bankruptcy and the increased accessibility by a financial institution, which might have access to that judgment, could invalidate the accessibility to a loan by the said individual.

Possible means for prevention and/or resolution:

…

Digital Competences involved:

In this specific case, users' digital competences do not contribute significantly in the solution of the problem; however, we think that the digital competencies 2.2, 2.3 and 2.4 could be helpful to raise awareness about the issue.

6.6.5. Blackmail

Description: '*The threat to disclose personal information'* (Robin Mansell, 2015).

'Blackmail allows a person to be dominated and controlled by another. With blackmail, the harm is not in the actual disclosure of the information, but in the control exercised by the one who makes the threat over the data subject. In some cases, blackmail can also involve information more akin to exposure than disclosure. Breach of confidentiality is also related to blackmail, as a confidant can threaten to disclose a secret in return for money. Blackmail differs from disclosure, exposure, and breach of confidentiality in that it involves a threat of disclosure rather than an actual disclosure.' (Solove, 2006)

Example: Let us suppose that following a data breach, somebody received some sensitive information related to some users that they do not want spread. The person holding this information could try to obtain some profit from them through blackmail.

Possible means for prevention and/or resolution:

Blackmailing is a crime, regardless of whether it happens online or outside the digital world.

In case of blackmail, the best way to react is to seek help from a legal point of view; nevertheless, we believe that users can protect themselves from threating to reveal personal data by way of prevention.

Digital competences involved:

Since blackmail could be performed through the threat to disclose stolen information, most of the digital competencies involved are related to the protection of data. The digital competences involved in the management of this problem include 1.3, 2.2, 2.3, 2.4, 2.6, 4.2, 4.3 and 5.4 (see paragraph 6.2).

Furthermore:

- '1.2. Evaluating data, information and digital content' (users should be able to critically evaluate if the third party processing their personal data can be trusted);
- '4.1. Protecting personal data and privacy';
- '5.1. Solving technical problems' (if users detect a problem related to their devices, they should be able to solve it or ask somebody (trusted) with a sufficient proficiency level to solve it);
- '5.2. Identifying needs and technological responses' (users should be able to evaluate whether they need further protection while browsing online and apply countermeasures if need be).

6.6.6. Appropriation

Description: '*The use of the data subject's identity to serve the aims and interests of another'* (Robin Mansell, 2015).

'Appropriation' is the use of one's identity or personality for the purposes and goals of another. Appropriation, like the privacy disruptions of disclosure and distortion, involves the way an individual desires to present herself to society. […] The interest safeguarded by protections against appropriation is control of the way one presents oneself to society. The products and causes people publicly endorse shape their public image. When people are associated with products, they become known in terms of these products. […] Thus, appropriation can be harmful even if it is not humiliating, degrading, or disrespectful. Being unwillingly used to endorse a product resembles, in certain respects, being compelled to speak and to represent certain viewpoints.

Protection against appropriation establishes what society considers appropriate for others to do in shaping a person's identity. The harm, then, is an impingement on the victim's freedom in the authorship of her self-narrative, not merely her loss of profits.' (Solove, 2006)

Example: A malicious individual who obtains personal information (through a data breach or social engineering) related to another person could use it for their own benefits. Personal information gathered could be of any kind:

- login credentials (user name and password) on a social network/email/instant messenger/shop online;
- credit card number/online payment service account;
- personal information related to a person's real life and that could be used to pretend to be that person when online.

Possible means for prevention and/or resolution:

Victims of a crime of appropriation should first seek help from a legal point of view as well as try to understand how the criminal was able to obtain the information. Once users understand what the source of the data is, they should take countermeasures depending on whether it is related to their own devices being insecure or whether it is a problem of insecurity related to a data controller that was hosting their personal data.

Digital competences involved

The digital competences involved in the management of this problem include 1.3, 2.2, 2.3, 2.4, 2.6, 4.2, 4.3 and 5.4 (see paragraph 6.2).

Furthermore:

- '1.2. Evaluating data, information and digital content' (users should be able to critically evaluate if the third party processing their personal data can be trusted);
- '4.1. Protecting personal data and privacy';
- '5.1. Solving technical problems' (if users detect a problem related to their devices, they should be able to solve it or ask somebody (trusted) with a sufficient proficiency level to solve it);
- '5.2. Identifying needs and technological responses' (users should be able to evaluate whether they need further protection while browsing online and apply countermeasures if need be).

6.6.7. Distortion

Description: '*The dissemination of false or misleading information about individuals'* (Robin Mansell, 2015).

'I refer to these harms as 'distortion.' Distortion is the manipulation of the way a person is perceived and judged by others, and involves the victim being inaccurately exposed to the public. I include distortion in the taxonomy of privacy because of its significant similarity to other privacy disruptions. Distortion, like disclosure, involves the spreading of information that affects the way society views a person. Both distortion and disclosure can result in embarrassment, humiliation, stigma, and reputational harm. They both involve the ability to control information about oneself and to have some limited dominion over the way one is viewed by society. Distortion differs from disclosure, however, because with distortion, the information revealed is false and misleading. […] Reputation is not merely an individual creation. Although it is true that people work very hard to build their reputations, one's reputation is the product of the judgment of other people in society. Reputation is a currency through which we interact with each other. Protection against distortion structures our interactions because it protects this currency. Distortion not only affects the aggrieved individual; it also affects the society that judges that individual: it interferes with our relationships to that individual, and it inhibits our ability to assess the character of those that we deal with.' (Solove, 2006)

This harm refers to one's reputation as an indispensable element to self-identity and the ability to engage in public life. Nowadays, in the digital society, we assist to the transposition of this concept to the web reputation and digital identity that both deserve acknowledged social regard, acceptance and respect.

Example: This problem is extremely hard to prevent and resolve.

There is a twofold origin for this problem: an individual spreads false information either because, in good faith, they have not verified sources, or intentionally to cause a bad reputation to somebody else.

Possible means for prevention and/or resolution:

Concerning distortion, there is no real countermeasure that users can take to prevent the problem, but users themselves can signal to authorities or to the victim if they recognise any false or misleading information. In this way, users behave as good digital citizens, reducing the spread of false information.

Digital Competences involved:

While digital competencies like 2.2, 2.3 and 2.4 could be helpful to raise awareness about the issue, dissemination of distorted information might take place regardless of users' digital competences. Legal measures can be the solution and the application of the GDPR's 'right to rectify' (Article 16) or 'right to erasure' (Article 17) where the 'distortion' are online.

Table 5: Information Dissemination

Information dissemination					
Privacy harm	**Description**	**Possible means for prevention and/or resolution**		**Digital competencies involved**	
		Legal resources	**Technical resources**	**Area (dimension 1)**	**Competence (dimension 2)**
Breach of Confidentiality	*'The breaking of a promise to keep a person's information confidential'*	GDPR (e.g. Articles 32, 33 and 34)		1. Information and data literacy	1.2. Evaluating data, information and digital content 1.3. Managing data, information and digital content
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies 2.6. Managing digital identity
				3. Digital content creation	—
				4. Safety	4.1. Protecting devices 4.2. Protecting personal data and privacy 4.3. Protecting health and well-being
				5. Problem solving	5.1. Solving technical problems 5.2. Identifying needs and technological responses 5.4. Identifying digital competence gaps
Disclosure	*'The revelation of truthful information about a person that impacts the way others judge his/her character'*	GDPR (e.g. Articles 32, 33 and 34)		1. Information and data literacy	1.2. Evaluating data, information and digital content 1.3. Managing data, information and digital content
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies 2.6. Managing digital identity
				3. Digital content creation	—
				4. Safety	4.1. Protecting devices 4.2. Protecting personal data and privacy 4.3. Protecting health and well-being
				5. Problem solving	5.1. Solving technical problems 5.2. Identifying needs and technological responses 5.4. Identifying digital competence gaps

Exposure	*'revealing another's sensitive or personal activities such as nudity, grief, or bodily functions'*	GDPR (e.g. Articles 32, 33 and 34)		1. Information and data literacy	1.2. Evaluating data, information and digital content 1.3. Managing data, information and digital content
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies 2.6. Managing digital identity
				3. Digital content creation	—
				4. Safety	4.1. Protecting devices 4.2. Protecting personal data and privacy 4.3. Protecting health and well-being
				5. Problem solving	5.1. Solving technical problems 5.2. Identifying needs and technological responses 5.4. Identifying digital competence gaps
Increased Accessibility	*'The amplification of the accessibility of information'*	GDPR (e.g. Article 10)		1. Information and data literacy	—
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies
				3. Digital content creation	—
				4. Safety	—
				5. Problem solving	—
Blackmail	*'The threat to disclose personal information'*	See end of p. 32		1. Information and data literacy	1.2. Evaluating data, information and digital content 1.3. Managing data, information and digital content
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies 2.6. Managing digital identity
				3. Digital content creation	—
				4. Safety	4.1. Protecting devices 4.2. Protecting personal data and privacy 4.3. Protecting health and well-being

				5. Problem solving	5.1. Solving technical problems 5.2. Identifying needs and technological responses 5.4. Identifying digital competence gaps
Appropriation	*'The use of the data subject's identity to serve the aims and interests of another'*	See end of p. 32		1. Information and data literacy	1.2. Evaluating data, information and digital content 1.3. Managing data, information and digital content
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies 2.6. Managing digital identity
				3. Digital content creation	—
				4. Safety	4.1. Protecting devices 4.2. Protecting personal data and privacy 4.3. Protecting health and well-being
				5. Problem solving	5.1. Solving technical problems 5.2. Identifying needs and technological responses 5.4. Identifying digital competence gaps
Distortion	*'The dissemination of false or misleading information about individuals'*	GDPR (e.g. Articles 16 and 17)		1. Information and data literacy	—
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies
				3. Digital content creation	—
				4. Safety	—
				5. Problem solving	—

6.7. Invasion

6.7.1. Intrusion

Description: '*Invasive acts that disturb one's tranquillity or solitude'* (Robin Mansell, 2015).

'Intrusion involves invasions or incursions into one's life. It disturbs the victim's daily activities, alters her routines, destroys her solitude, and often makes her feel uncomfortable and uneasy. Protection against intrusion involves protecting the individual from unwanted social invasions, affording people what Warren and Brandeis called 'the right to be let alone.' […] While many forms of intrusion are motivated by a desire to gather information or result in the revelation of information, intrusion can cause harm even if no information is involved. In particular, intrusion often interferes with solitude, the state of being alone or able to retreat from the presence of others.' (Solove, 2006)

Example: Let us assume that the wireless domestic network of an individual's house is not secured enough and that a malicious user in range of the individual's network connection has access to it. If the user starts to download large amounts of data, the individual could experience a reduction of bandwidth and the experience online could be unpleasant. Intrusion on private accounts of an individual (following a data breach) or on the personal device itself (because it was not properly secured) can be also more annoying and cause additional problems.

Possible means for prevention and/or resolution:

The victim of an intrusion should try to understand what has been done by the intruder and evaluate the seriousness of the actions performed. In the best case scenario it should be enough that the user fixes (if they are able to, or otherwise ask for support) the 'entry point' of the intruder, while in the worst case scenario the intervention of law enforcement agencies could be needed.

Digital competences involved:

The digital competences involved in the management of this problem include 1.3, 2.2, 2.3, 2.4, 2.6, 4.2, 4.3 and 5.4 (see paragraph 6.2). Furthermore, the following digital competencies are useful to prevent intrusion caused by insecurity:

- '4.1. Protecting personal data and privacy';
- '5.1. Solving technical problems' (if users detect a problem related to their devices, they should be able to solve it or ask somebody (trusted) with a sufficient proficiency level to solve it);
- '5.2. Identifying needs and technological responses' (users should be able to evaluate whether they need further protection while browsing online and apply countermeasures if need be).

6.7.2. Decisional interference

Description: '*The government's incursion into the data subject's decisions regarding his/her private affairs'* (Robin Mansell, 2015).

'[…] what I call 'decisional interference'—that is, governmental interference with people's decisions regarding certain matters of their lives. […] Many commentators have argued that

the language of privacy is inappropriate for decisional interference cases, since they primarily concern a harm to autonomy and liberty, not to privacy. […] What relationship does decisional interference have with the other forms of privacy in the taxon-omy?

The decisional interference cases are deeply connected to information privacy. In particular, […] the constitutionally protected 'zone of privacy' extends not only to the 'interest in independence in making certain kinds of important decisions' but also to the 'individual interest in avoiding disclosure of personal matters.' (Solove, 2006)

Example: The restriction or incursion by the government into a data subject's decisions regarding fundamental rights is considered decisional interference. An example in the online world could be the surveillance where 'a government' (or better yet 'a regime') regulates the freedom of expression and opinion of individuals. In that case, citizens will probably change their behaviour online to be compliant with the regime.

Possible means for prevention and/or resolution:

Digital competencies involved:

For decisional interference (as for increased accessibility), users' digital competences do not contribute significantly to finding a solution to the problem. However, we think that the digital competencies 2.2, 2.3 and 2.4 could be helpful to raise awareness about the issue.

Table 6: Invasion

Invasion					
Privacy harm	**Description**	**Possible means for prevention and/or resolution**		**Digital competencies involved**	
		Legal resources	**Technical resources**	**Area (dimension 1)**	**Competence (dimension 2)**
Intrusion	*'Invasive acts that disturb one's tranquillity or solitude'*	See end of p. 32		1. Information and data literacy	1.3. Managing data, information and digital content
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies 2.6. Managing digital identity
				3. Digital content creation	—
				4. Safety	4.1. Protecting devices 4.2. Protecting personal data and privacy 4.3. Protecting health and well-being
				5. Problem solving	5.1. Solving technical problems 5.2. Identifying needs and technological responses 5.4. Identifying digital competence gaps
Decisional Interference	*'The government's incursion into the data subject's decisions regarding his/her private affairs'*			1. Information and data literacy	—
				2. Communication and collaboration	2.2. Sharing through digital technologies 2.3. Engaging in citizenship through digital technologies 2.4. Collaborating through digital technologies
				3. Digital content creation	—
				4. Safety	—
				5. Problem solving	—

This page is intentionally left blank

7. Conclusions

Nowadays, digital citizens, either actively or passively, accept to provide personal information in their everyday online activities. Some of the information shared is personal data as defined by Article 4(1) of the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016). Some of the data can be used to uniquely identify an individual, whereas others, even if they are not strictly 'personal data', are still related to the individual and can still lead to their identification. Some issues on the privacy of data subjects can appear in specific areas of the data flow, as identified by Solove (Solove, 2006) in his paper 'A Taxonomy of Privacy'. We have used it as the basis of our study.

To perform an analysis of those privacy issues, we chose a multidisciplinary approach as the methodology, looking at technical tools, legal tools and educational aspects needed to prevent and/or resolve them.

In this report we have presented a survey of the techniques to perform the tracking (browser fingerprinting, ETags, location tracking, etc.) and profiling of data subjects. We complemented the survey by analysing some of the Privacy-Enhancing Technologies (PETs) (see paragraph 5.1) available that could be helpful for digital citizens to better manage and safeguard their privacy online.

We also considered the recent GDPR in our analysis, as it represents a big step forward in 'the protection of natural persons with regard to the processing of personal data'. Indeed, the regulation helps European citizens to better manage their personal data, with specific articles addressing some issues related to privacy such as, for example, the '*Right of Access by the data subject*' (art.15), to avoid '*Exclusion*' and '*Right of Rectification*' (art.16), '*Right of Erasure*' (art.17), to fight '*Secondary Use*' of personal data (art.5) or '*Distortion*'.

We concluded our analysis by summarising our findings related to technical and legal tools to address (prevent and resolve) privacy harms following the categorisation of Solove (Solove, 2006). The analysis was done under the point of view of data subjects (digital citizens) who could be facing those harms. This perspective allowed us to identify the digital competences needed by data subjects in order to enact the suggested measures of prevention or resolutions of privacy issues.

Our research has led to the main conclusion that, whilst there exist legal and technical tools to protect privacy online, they cannot be effective unless they are complemented by the proper education of individuals. Therefore, it is our recommendation to increase user awareness in this topic and put forward initiatives to promote existing tools and education campaigns to improve the well-being of digital citizens.

This page is intentionally left blank

References

Bacigalupo Margherita, K. P. (2017, 05 10). *Entrepreneurship Competence.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/entrecomp

Biermann, K. (2011, MArch 10). Data Protection: Betrayed by our own data. *Betrayed by our own data*. (Z. ONLINE, Ed.) Retrieved from http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz

Brecko Barbara, F. A. (2017, 04 08). *The Digital Competence Framework for Consumers.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digital-competence-framework-consumers

Brečko, B. F. (2017, 03 20). *The Digital Competence Framework for Consumers.* doi:10.2791/838886

Carretero Gomez Stephanie, V. R. (2017). *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-21-digital-competence-framework-citizens-eight-proficiency-levels-and-examples-use

Carretero Stephanie, P. Y. (2017, 04 20). *The Digital Competence Framework 2.0.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework

Charalambos Vrasidas, E. C. (n.d.). *MOOCS4inclusion.* Retrieved from MOOCS4inclusion: http://moocs4inclusion.org/

Control, T. I. (A cura di). (2002). *IEC TC 65/290/DC* (Vol. Device Profile Guideline).

DG Justice and Consumers. (2015, 06 24). *Data protection Eurobarometer out today.* Retrieved from European Commission: http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm

Eckersley, P. (2010). How Unique Is Your Web Browser? In M. J. Atallah, & N. J. Hopper (Ed.), *Privacy Enhancing Technologies: 10th International Symposium, PETS 2010, Berlin, Germany, July 21-23, 2010. Proceedings* (pp. 1-18). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-14527-8_1

European Commission. (2016, 09 21). *European Commission*. Retrieved from INFORMATION PROVIDERS GUIDE: The EU Internet Handbook - Cookies: http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm

European Commission. (2016, 07 01). *PACT — Result In Brief.* Retrieved from Eurpean Commission: http://cordis.europa.eu/result/rcn/155988_en.html

European Commission. (2017). Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. *European Commission - High Representative of the Union for Foreign Aggairs and Security Policy, Final*.

European Parliament, E. C. (2002, July 12). Data protection in the electronic communications sector. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24120

European, E. P. (n.d.). DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF

FERGUSON Rebecca, B. A. (2017, 01 13). *Research Evidence on the Use of Learning Analytics: Implications for Education Policy.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-

research-reports/research-evidence-use-learning-analytics-implications-education-policy

G. Chen, J. H. (2016, January). In-Depth Survey of Digital Advertising Technologies. *IEEE Communications Surveys & Tutorials, 18*(3), 2124-2148. doi:10.1109/COMST.2016.2519912

Gutwirth S., H. M. (2010). Some Caveats on Profiling. In P. Y. Gutwirth S., *Data Protection in a Profiled World.* Springer, Dordrecht. doi:https://doi.org/10.1007/978-90-481-8865-9_2

Hildebrandt, M. (2008). Defining Profiling: A New Type of Knowledge? In M. G. Hildebrandt (Ed.), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (pp. 17-45). Springer Netherlands. doi:10.1007/978-1-4020-6914-7

Inamorato dos Santos Andreia, P. Y. (2016, 07 27). *Policy Recommendations for Opening Up Education.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/open-education

ISO/IEC JTC 1. (2015). *ISO/IEC 11889-1:2015: Information technology -- Trusted platform module library -- Part 1: Architecture.* International Organization for Standardization.

ISO/IEC JTC 1/SC 27. (2013). *ISO/IEC 20008: Information technology — Security techniques — Anonymous digital signatures.* International Organization for Standardization.

ISO/IEC JTC 1/SC 27. (2013). *ISO/IEC 20009-1:2013: Information technology -- Security techniques -- Anonymous entity authentication -- Part 1: General.* International Organization for Standardization.

Kampylis Panagiotis, P. Y. (2016, 07 27). *European Framework for Digitally Competent Educational Organisations.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/digcomporg

Kampylis Panagiotis, P. Y. (2016, 07 27). *The Computational Thinking Study.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/computational-thinking

PACT project. (2014, 11 14). *PACT Final Conference - Vienna [13-14 November 2014].* Retrieved from PACT Final Conference: http://www.projectpact.eu/

Party, A. 2. (2013, October 2). Working Document 02/2013 providing guidance on obtaining consent for cookies. Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

Požrl, M. K. (2017). Diversity in recommender systems – A survey. *Knowledge-Based Systems, 123*(Supplement C), 154 - 162. doi:https://doi.org/10.1016/j.knosys.2017.02.009

Punie Yves, R. C. (2017, 12 01). *Digital Competence Framework for Educators (DigCompEdu).* Retrieved from European Commission: https://ec.europa.eu/jrc/en/digcompedu

Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016, may). *Official Journal of the European Union*, 1-88. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

Robin Mansell, P. H. (2015). *The International Ecnyclopedia of Digital Commuinication and Society.* Wiley Publishing.

Roosendaal, A. (2012). We Are All Connected to Facebook … by Facebook! In A. Roosendaal, *European Data Protection: In Good Health?* (pp. 3-19). Dordrecht: Springer Netherlands. doi:10.1007/978-94-007-2903-2_1

Soghoian, C. (2011, January 21). *The History of the Do Not Track Header*. Retrieved from slight paranoia - Analysis and opinion by Christopher Soghoian, security and privacy researcher.: http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html

Solove, D. J. (2006, January). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154*, 477-560.

Tuzhilin, G. A. (2005). Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions. *IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, 17*(6), 734-749.

V. Ferraris, F. B. (2014). *Working Paper Defining Profiling.*

Veijalainen, D. K. (2016). A survey of serendipity in recommender systems. *Knowledge-Based Systems, 111*(Supplement C), 180-192. doi:https://doi.org/10.1016/j.knosys.2016.08.014

Verbert, C. H. (2016). Interactive recommender systems: A survey of the state of the art and future research challenges and opportunities. *Expert Systems with Applications, 56*(Supplement C), 9-27. doi:https://doi.org/10.1016/j.eswa.2016.02.013

Vourikari Riina, P. Y. (2017, 07 15). *DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-20-digital-competence-framework-citizens-update-phase-1-conceptual-reference-model

W3C. (2015, August 20). *Tracking Preference Expression (DNT)*. Retrieved from www.w3.org: https://www.w3.org/TR/tracking-dnt/

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, 193-220.

This page is intentionally left blank

List of figures

This page is intentionally left blank

List of tables

This page is intentionally left blank

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*)**:**

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

More information on the European Union is available on the internet (http://europa.eu).

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);
- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or
  calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

KJ-NA-28991-EN-N

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/30934

ISBN 978-92-79-77231-3