~~PRIVACY~~
~~INTERNATIONAL~~

Privacy International's contribution to the EU Commission consultation on the review of the e-Privacy Directive (2002/58/EC)

July 2016

1. Introduction

Increasingly devices, networks and services generate data that is used to identify and distinguish individuals from each other and map their behaviour, predict their future behaviour and affect (or even direct) such behaviour.

Modern devices collect data (e.g. temperature, acceleration, images, sound, and location) through the use of sensors that generate data based on events. These can be processed into information about the user. Increasingly, sensors contained in a range of devices (including the so-called "Internet of Things"), record, store and transfer various types of data unobtrusively and seamlessly (or, more ominously, secretly and constantly.) Such data is generated and transmitted by technology in the possession of individuals (smartphones, etc.) but increasingly they are generated and transmitted by sensors surrounding individuals. These sensors vary widely in purpose and design and may be placed in public and semi-public spaces – they include traditional CCTV (to capture video or events like through Automated Number Plate Recognition and Facial Recognition), microphones (to capture specific sounds), environmental sensors (e.g. may detect variations in heat and humidity), movement sensors (e.g. to track number and variety of people or vehicles), beacons (e.g. to detect Bluetooth devices), wifi networks (to detect wifi capabilities on devices), and IMSI catchers (to detect mobile phones). Further, in transmitting or delivering communications or other services, networks add data, such as timestamps, position, signal quality and other metadata. Much of this data generation and transmission is done without the knowledge or involvement of the individual, and it is increasingly the case that the individual can do little to prevent it. This data is also highly structured, unlike content, so large volumes of it can be easily processed and mined for identification and behavioural patterns.

Data generated and transmitted is then aggregated, analysed, and compared with other sets of data. Algorithms may be applied to the data sets which in turn generate further data ("data augmentation") and the algorithms themselves become a representation of the data as they adapt and learn. Intelligence is gleaned from the data, to "identify" and "predict" an individual's behaviour and ultimately, used to make decisions that affect the individual concerned. In this sense, algorithms that learn are not static; they evolve over time based on the data they are presented with.

The following two scenarios are illustrative of the kind of issues we currently face.

Scenario One: As individuals browse the internet, data is generated on their browsers, but also by the websites and other internet services with which they interact – some of which the individual does not even know they are interacting with. Individuals' devices are fingerprinted based on their profile information (version of browser, operating system, clock skew, plugins installed in the browser, music library) and/or through the use of cookies and identifiers that are generated to track individuals across services. Individuals may be tracked across devices through probabilistic (sometimes using non-personally identifiable information aggregated to create a fingerprint), authenticated, or even sensor-shared information (e.g. using audio signals to link devices). All of this may be done with the claim that no 'personal data' was processed to conduct these activities. All this data is brought together to create a profile of the individual and his or her devices, to understand daily habits, interests, ambitions, and likely activities, and encounters with audio-visual content (e.g. what he or she is watching on television). These profiles can be used to target advertisements, provide services and tailor them, or in the future to discern candidacy for benefits and services.

Scenario Two: A family is in a car that drives down a city street on the daily run to schools and work. The car contains a mobile phone chipset that generates data on its location. The individuals in the car have mobile devices that generate mobile signals and wifi signals. External sensors collect: street-level car data, citywide wifi data of all devices in the car, store-level wifi data of all devices in the car as the car drives by a cafe. Automated Number Plate Recognition (ANPR) cameras capture the car registration. Any irregularity in the pattern of travel and number of devices in the car can be discerned through deviations in collected data. Security and police services already collect ANPR, and covertly collect IMSI data; we have tracked the collection of wifi data by city-level networks. While the possible uses are bountiful, we have not yet been able to find how this data is being processed in a transparent manner, if at all. It may be possible to identify when a family member is not present, or additional individuals are in the automobile, or unexpected individuals are in an automobile, or if the family has purchased a new type of automobile, or any new devices. This can then be used to discern financial, marital, health status as well as the pattern of human relationships.

In this new world, with a myriad of new data sources, it will become even more important for individuals to be able to know what data is collected about them, how it is generated, and how to control it. For these reasons, we suggest in the following discussion ways in which the successor to the EU e-Privacy Directive may be updated to address these new challenges.

2. The scope of application

Since the EU e-Privacy Directive was adopted in July 2002, the landscape of generation, collection and other processing of data in the digital sphere has changed significantly. First, there has been a massive increase in the capacity of devices to generate, transmit and collect data, including personal data, combined with an expansion of the type of devices generating and processing such data. Second, there is now increased interest in the development of techniques, including through the use of algorithms, to process such data with the view to generate inferences or predictions of an individual's behaviour based on such data. Finally, a more fundamental shift has occurred in our relationship with technology. At the start of the last decade, virtually the only devices collecting data on us were the ones we purchased ourselves. However, now there is a myriad of ways that technology deployed by other private parties and state agencies is collecting personal data and this demands a fresh look at the principles that underpin an ever more digitized society.

As noted by the European Data Protection Supervisor (EDPS), "the internet has evolved such that the tracking of people's behaviour has become routine for many intelligence agencies, not to mention an essential revenue stream for some of the most successful companies. I've said it before but it's worth emphasising: we are each more than the sum of our data and yet we are more defined by our quantified selves than ever".[1]

How will this impact individual's behaviour? For example, would they be able to generate false data and if so, how would that affect a way a decision is made? How would the system view it?

The successor to the EU e-Privacy Directive (the new instrument) should aim to address some of the challenges to data protection posed by:

- The growing use of technology to generate, collect, process data at vast scale and speed (including the growing number of devices generating data);

- The ever increasing complexity of our devices, networks and services;

- The use of techniques to "identify" individuals or to distinguish them from others or from a significant portion of others;

- The use of techniques to "infer" information based on such data and to use such inferences as the basis for automated decisions affecting individuals; and

- The use of techniques to generate intelligence based on such data about groups of individuals, affecting group privacy, and also creating new and likely closed pools of knowledge about human activity without any ability of the individuals and groups to be aware or object to these entities having the benefit of this knowledge.

As such the scope of application of the new instrument should aim to cover communications and data transmitted "over the Internet", including instant messaging and webmail; data transferred within private networks accessible by the general public (e.g. wifi networks in airports, parts of cities, etc.); and to data collection and identification devices such as those referred to as belonging to the "Internet of Things", and otherwise sensor networks, whether or not they are integrated into other systems.

[1] Buttarelli, Big Brother, Big Data and Ethics, 31 May 2016, https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Big_Brother

3. Defining personal data in light of the challenges of anonymisation

The definition of personal data contained in the EU GDPR should be the starting point of the new instrument.[2]

The recital to the EU GDPR states that "to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments." (italics added.)[3]

The new instrument should provide some guidance on what "all the means reasonably likely to be used" may consist of in the context of online data and technologies that process it. Considering the level of investment and innovation, combined with the low costs of data collection and retention, unless there are strict retention periods we do not believe the test of available technology at the time is as meaningful as it once was as a constraint.

In doing that, the new instrument should also take into account the challenges to anonymisation of data posed by new technologies, particularly in light of the increased possibility of cross-referencing data. It should also consider the intelligence value of even de-identified data that is not used to identify a natural person but instead is used to understand groups, organisations, and societies as a whole.

Data controllers should demonstrate what methods they use to attempt re-identification based on the data they hold or are likely to come into the possession of.

As noted by the Advocate General of the CJEU, dynamic 'IP' addresses qualify as personal data, even if the website operator in question cannot identify the user behind the IP address, since the users' internet access providers have data which, in connection with the IP address, can identify the users in question.[4]

This conclusion can be applied to a range of other contexts, for example in relation to MAC addresses and cookies. When data is combined from various sources, it can also be used to identify users and their attributes. This may include the combination of browser type (of which there are relatively few for all users but version), combined with rendering time (which makes some reference to the device and the setup of software on the device), and means of connection to the service. All of this non-unique data that, when combined, renders an

[2] Article 4(1): "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

[3] EU GDPR, recital 26.

[4] See Opinion in Case C-582/14 Patrick Breyer v Germany, (12 May 2016), http://curia.europa.eu/juris/fiche.jsf?id=C;582;14;RP;1;P;1;C2014/0582/P

individual relatively unique to the service. An individual can still be treated unfairly on the basis of any of these types of information, or the combination, e.g. price discrimination based on the type of device used.

The mere fact of data being processed must be considered as part of the identifiability question. For example, many devices will limit the amount of activity they perform due to power and bandwidth constraints. However, in some cases, these limitations may change if circumstances require. For example, a heart rate monitor may transmit data at a normal rate if the measured heartbeats are within normal ranges. However, if these drop or increase then it may increase the sampling and transmission rates. Accordingly, a change in transmission rate can indicate abnormally high or low heart rates for the circumstances the user is in.

In the context of the proliferation of devices, generating vast amounts of data and the ever-increasing processing capabilities of new technologies, data is increasingly at risk of re-identification. The Working Party 29 noted that "even data relating to individuals that is intended to be processed only after the implementation of pseudonymisation, or even of anonymisation techniques may have to be considered as personal data. In fact, the large amount of data processed automatically in the context of IoT entails risks of re-identification".[5]

The European Data Protection Supervisor, in his Opinion 7/2015 argues that it "will be ever easier to infer a person's identity by combining allegedly 'anonymous' data with publicly available information such as on social media".[6]

The above considerations point to the need of a significant shift in the way data perceived as "anonymous data" is considered and treated. Apparently anonymous data can be used to "identify" an individual user and to "infer" an individual's habit or property. For example, the accelerometer and the gyroscope of a smartphone can be used to identify an individual's driving habits. Or the two most commonly recurrent location data in someone's smartphone can be used to "infer" the individual's respective home and office addresses. The registration and de-registration of devices on a wifi network, even when personal identifiers are hashed, can be used to identify when two individuals both arrived and departed from a restaurant with the wifi network in place. It is vital that any claims around the anonymity of data are tested thoroughly.

Consideration should be given, for example, to the purpose of the processing.

As noted by the Working Party 29 "where the purpose of the processing implies the identification of individuals, it can be assumed that the controller or any other person involved have or will have the means 'likely reasonably to be used' to identify the data subject. In fact, to argue that individuals are not identifiable, where the purpose of the processing is precisely to identify them, would be a sheer contradiction in terms. Therefore, the information should be considered as relating to identifiable individuals and the processing should be subject to data protection rules."[7]

[5] Opinion 8/2014 on the on Recent Developments on the Internet of Things, available here: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[6] Opinion 7/2015, Meeting the Challenges of Big Data, available here: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf

[7] The Working Party 29 opinion on the definition of personal data http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

It is key that the new instrument adequately takes into account this reality and addresses the limits of anonymisation, including by stipulating that processing anonymous data should not exclude the application of relevant data protection principles (minimization, fair processing, etc.).

4. Some of the grounds for processing personal data

4.1 Consent

Consent is one of the legitimate grounds for processing of personal data.[8]

In many cases users may not be aware of data processing (including data generation) of the applications or sensors in their devices (e.g. by many devices or by the same applications operating across different platforms.) Again, the increase in the number of available devices generating, collecting and transmitting data raises significant questions on whether consent can be freely given and freely revoked/withdrawn. This applies not only to data processing of devices possessed by individual users, but also to the growing deployment of devices generating and transmitting data in public and semi-public spaces.

For example, “smart bins” were introduced in the financial district of London. These bins collected mobile phone metadata to provide tailored ads on the bins themselves, while tracking people’s devices across town – essentially becoming a sensor network. Once it became publicly known that this was occurring, adverse media and public reaction led to their withdrawal.

Nonetheless city-level wifi systems and beacons also generate and collect this kind of data – sometimes without the user’s knowledge and more often without the user being aware of the potential of this technology to do things other than what the individual believes is being done, e.g. a user may not understand that there is tracking and monitoring of wifi connections even though he or she may wish to use the wifi network for the purpose of connecting to a service.

Therefore, there may be situation where the individual may effectively not have the capacity to give free and informed consent. This may be particularly so where there is an imbalance of power between the data controller or data processor and the individual (e.g. dominant position of certain companies offering certain services), or when the processing of data is “embedded” in the device.

Finally, even though an individual may take significant care in trying to control the release and use of his or her personal data through traditional means, the devices may undermine these efforts. An individual who expresses concerns about a grocery store tracking his or her purchases may yet be tracked through payment, movement in the store, and the uniqueness of his or her purchases. Where consent was sometimes sought, in the future the opportunity to seek consent may not even arise.

[8] See Article 6(1)(a) EU GDPR.

It may also be possible that where an individual does consent to processing of identifiable data, this will then be combined with other data arising from his or her devices and interactions, and may not knowingly understand that this is now linked together. Extending the previous example, if the customer decides to eventually sign up to a loyalty scheme, all future and past purchasing may be studied, alongside other data. All the intelligence gleaned from all purchases can then be combined and focused on the individual, or, using the additional information from the individual, be used to further inform the datasets on all activities by all customers.

That is why the new instrument should consider the role of the device manufacturers. Even though the device is owned by the individual, there is often no meaningful control over its activities or even transparency about its operation. Accordingly, individuals need to have enforceable rights against the manufacturers and retailers of products they buy including around data access, algorithmic transparency and the digital footprint created by the device and any third party software on it.

4.2 Legitimate interest

The EU GDPR permits the processing of personal data where it is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."[9]

Increasingly the capacity to analyse vast amounts of data gathered from a range of devices is employed by a range of actors to predict individuals' behaviour and to make decisions based on such predictions. This may be done through simple data sifting, profiling, the application of algorithms, and machine learning.

As noted by the Working Party 29, "in the context of the IoT [Internet of Things], the processing of an individual's personal data is likely to affect significantly his/her fundamental rights to privacy and the protection of personal data in situations where, without IoT devices, data could not have been interconnected or only with great difficulty. Such situations may happen when the data collected relate to the individual's state of health, home or intimacy, his/her location and many other aspects of his/her private life. In the light of the potential seriousness of that interference, it is clear that such processing will hardly be justified by merely the economic interest which an IoT stakeholder has in that processing."[10]

The new instrument should seek to clarify the scope of these grounds of processing (consent and legitimate interests) as they apply in the context of processing the plethora of new data that is being or may be generated by our devices.

[9] Article 6(1)(f) EU GDPR.

[10] Opinion 8/2014 on the on Recent Developments on the Internet of Things, available here: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

5. Principles to limit processing of data

The successor to the e-Privacy Directive should clarify the scope of the application of the EU GDPR's principle of minimisation to the processing of personal data.

Data controllers should ensure that, by default, only data that are necessary for each specific processing purpose are processed. This applies to the amount and type of data generated, collected, the extent of their processing, the period of their storage and their accessibility. A service that holds itself out as a social network, for example, must only collected and process data for that purpose. Should they wish to process data for any other purpose, this must be made known to the user with the same prominence and frequency as any other purpose.

Already the EU e-Privacy Directive recital notes that "digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualised traffic information and guidance to drivers. The processing of such data for value added services should only be allowed where subscribers have given their consent. Even in cases where subscribers have given their consent, they should have a simple means to temporarily deny the processing of location data, free of charge."[11]

This principle should be re-stated and specified in the new instrument. In particular, it should be made clear that the principle of minimization should apply to the generation of data, as well as all the other stages of processing. This is crucial to help addressing one of the key challenges to protection of personal data posed by new technologies, namely the ever-increasing number of devices that generate a range of different types of data (location, movement, temperature, timing, other related or nearby identifiers, etc.), feeding into the algorithms used to infer information and make decisions about individuals, groups, organisations, and even whole societies.

Further the new instrument should include requiring that any personal data processed should be reduced to the least-invasive type needed for the relevant (initial or subsequent) purpose for which they are collected and used, and deleted as soon as they are no longer needed for the initial or subsequent purpose. For example, deletion of data should occur as soon as the data required for the processing has been extracted (in principle as close as possible to the point of data collection.) The new instrument should clarify that this principle applies irrespective of the grounds for processing (consent, contractual obligation, delivery of value added service, etc.) and it applies at all stages of processing, including at the point of generation of the data.

[11] EU e-Privacy Directive, recital 35.

6. Prevention and risk assessment

Automated decision making based on processing of data by algorithms is increasingly affecting individuals in a wide range of contexts. For example, a credit scoring algorithm that would allow a lender to examine the credit ratings of members of the individual's social network.[12] We have already seen indications of discriminatory pricing based on device types and browsers.[13] Targeting advertisements and content at people based on some identifiers that are not unique will disclose preferences to others, e.g. IP address-based ads will reveal the interests of others who share the network in a home for instance. The mere availability of data is affecting the allocation of resources, for instance through the use of app data to identify deficient road surfaces in need of repair,[14] but that only applied to areas where residents had mobile phones that could generate such data.[15]

In light of the increasing complexity of data processing and the use of automated decision making and its effects on individuals, data controllers - including manufactures of devices designed to generate, store and transmit data - should be required to adopt policies to assess risks of the use of data and its impact on individuals' rights and on society in general. This should also include the adoption of ethical guidelines and the setting up transparent and independent ethical boards to review envisaged data generation and processing.

The new instrument should include a requirement for data controllers to conduct such risk-assessment (privacy and data protection impact assessment) of the potential impact of data processing on the rights to privacy and data protection.

This assessment should include "not only individual privacy and data protection, but also the collective dimension of these rights", including by considering "the social and ethical impact". For instance, we would like controllers to consider more about who is included unnecessarily and sometimes excluded unnecessarily as a result of these processing activities. We would also like to see more consideration of the intelligence and power dynamics that these non-consensual and vast data processing capabilities may give rise to.

7. Confidentiality

The current EU e-Privacy Directive requires states to ensure confidentiality of communications and related traffic data (Article 5). A right to confidentiality of communications is enshrined in Article 7 of the EU Charter on Fundamental Rights and Article 8 of the European Convention on Human Rights.

[12] According to a Facebook's patent application "if the average credit rating of these members is at least a minimum credit score, the lender continues to process the loan application. Otherwise, the loan application is rejected." See http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=9100400.PN.&OS=PN/9100400&RS=PN/9100400 and the report on this story, such as http://www.theatlantic.com/technology/archive/2015/09/facebooks-new-patent-and-digital-redlining/407287/

[13] See http://personalization.ccs.neu.edu/PriceDiscrimination/Press/

[14] See http://nms.csail.mit.edu/papers/p2-mobisys-2008.pdf

[15] See http://foreignpolicy.com/2013/05/10/think-again-big-data/

Technology has increased the capacity to monitor individuals' behavior. These range from capturing location data to browsing data to information such how hard one hits the keys, how fast one types, how loud or fast one talks and the time taken to complete tasks (such as the time to read each page on an e-Reader.)

The revised instrument should expressly clarify that the right to confidentiality applies to these and similar types of data. There is a vast gulf between the data and information that an individual may wish to share and disclose, and the data, information and intelligence that is inferred, including mood, financial status, health, relationships.

Any installation of software into the individual's terminal equipment to gain access to information stored (or generated) should only be allowed on the condition that the individual concerned is provided with clear and comprehensive information "inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller."[16] There should be multiple ways of limiting the data generation, when possible.

For example, the provision of a hardware switch for microphone and camera on devices such as smart TV or video game consoles, rather than just software based options, which can offer better protection to confidentiality, as well as enhance individual's control and security against unauthorized access (see below.)

The new instrument should clarify that this applies irrespective of the nature of the data being stored or accessed (i.e. it would apply even to data that does not fall under the definition of "personal data".)[17]

It should clarify that "terminal equipment" would mean any object capable of storing or generating such data (notably in light of the proliferation of devices generating and transmitting data.)

The new instrument should provide guidance on how individuals can effectively exercise the right to refuse the installation of such software. For example, the denial of consent to a tracking cookie may not result in denial of any public service. A public service should, by definition, be available to the general public and availability should not be based on the acceptance of a tracking cookie.

8. Information/transparency

The requirement of transparency and information contained in Article 6 of the current EU e-Privacy Directive needs to be further elaborated in the new instrument. There are two main aspects of transparency/right to information relevant in the context of modern electronic data processing, which the new instrument should address.

[16] See Article 5.3 of the current EU e-Privacy Directive.
[17] See Working Party 29 Opinion 02/2013 on apps on smart devices.

Firstly, particularly in the context of excessive data generation, disclosure and data analytics, the data being processed may come from different sources: not only (and increasingly less so) data individuals have knowingly given (such as for example when filling in an online form); but also data obtained from online tracking devices like cookies, log data and other data emerging from the interactions, data obtained through public sources, and inferences based on "observation"/behaviour monitoring. Advertisements on social media are not just generated by what an individual chooses to type into their status updates and share actively with others using the service provider.

Irrespective of the origin of the data, the new instrument should give individuals the right to know: what the data pertaining to them is; how it was collected, generated or discerned; and from where and from whom the controller obtained it.

Secondly, lack of transparency in the decision making involved in modern data processing is a significant concern. A 2014 report by the US White House noted "some of the most profound challenges revealed during this review concern how big data analytics may [...] create such an opaque decision-making environment that individual autonomy is lost in an impenetrable set of algorithms".[18]

It's not just that algorithms may be opaque, but the process of machine learning is growing more challenging to audit. Unless we can understand what data is being fed into the processing, and what the outcomes are, and any eventual learning, and see and audit this entire process, it will not be possible to assess the fairness of the processing, including ensuring it treats individuals without discrimination. For example, difference in treatment must be justified and machine learning systems must be able to account for their change in behavior to show it is not arbitrary or based on protected characteristics. Auditing algorithms and machine learning processes raise also issues about balancing accountability and transparency with privacy (for example it cannot be the case that transparency must involve disclosure of the sensitive data in the system in order to fully audit it.)

The EU GDPR builds upon the EU Data Protection Directive on right to information of data subject, by including "the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing".[19]

The new instrument should develop and clarify this provision, including by requiring that the data controller pro-actively discloses the logic involved in the processing of data, including an explanation in plain language of the working of algorithms and sufficient information about the consequences of the processing.

9. Right to access to personal data and data portability

Among the fundamental developments contained in the EU GDPR is the right

[18] Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President, May 2014, page 10.
[19] EU GDPR, recital 63.

to data access and ultimately to portability, i.e. the right of data subject "to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance".[20]

Just as it has taken years to help explain to people and policy-makers the importance of location data and metadata, an educational exercise is urgently required on the value of data generated by sensors. People need to understand what is the new forms of metadata today – what information is known on them as a byproduct of their daily interactions with their devices, environments, and with services. There is a need to develop innovative user-interfaces on devices, but also explanations of sensor networks deployed in public and semi-public places, and stronger enforcement on the disclosure of information about processing that comes before the subject access request.

The right of the individual to access his or her data in the future will mean the right of the individual to know what data is being generated and under what circumstances. We should be able to know what sensors exist in our midst, and whether they are under our control and if not ours, who else is under control of those sensors. All inferences made about our identity and attributes must also be disclosed.

The EDPS opinion on Big Data identifies some of the requirements related to data portability, including requiring data controllers "to provide individuals with access to their own data in portable, interoperable and machine-readable (in other words, usable and reusable) format; allow them to modify, delete, transfer, or otherwise further process their own data; allow them to switch providers (e.g. transfer their photos, banking or fitness records, or emails to a different service provider); and allow them to take advantage of other third party applications to analyse their own data and draw useful conclusions (e.g., change dietary or exercise habits, get personalized health care, make wiser investment decisions, switch to a cheaper electricity provider)."[21]

The technical measures necessary to effectively implement this right are complex and the Article 29 Working Party has identified this provision among the priorities requiring the development of guidance for data controllers and processors.[22]

The new instrument replacing the EU e-Privacy Directive should contain provisions to further clarify the legal and technical requirements on data controllers to effectively guarantee data portability in the context of modern technologies of generation, storage and communications of data.

10. Security of data

Article 4 of the current EU e-Privacy Directive requires communications services

[20] EU GDPR, Article 20, paragraph 1.

[21] Opinion 7/2015, Meeting the Challenges of Big Data, available here: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf

[22] See Working Party 29 2016 Action Plan for the implementation of the EU GDPR, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf

providers (together with the communications network providers) to put in place appropriate security safeguards for their services.

It is important that the new instrument reflects the enhanced requirements of the EU GDPR, including in relation to security breach notification.

There is a growing concern about the security vulnerabilities many products designed to collect and transfer data. Concern has been expressed about whether the manufactures of these devices have adequately considered the risks of unauthorized access (whether by private individuals, by companies or by state agencies) to the devices as well as whether they have the willingness or the capacity to develop and distribute security updates when vulnerabilities are detected.[23] Where any updates to a device or service will require a change in the relationship between the user and provider, this must be made clear. In some cases, it is preferable for a device to cease operating than to operate with out-of-date software.

Similarly, because of the type of technology use and limited processing powers, there are concerns about whether some of these devices are designed in a way that would permit the transfer of data securely, including for example by using encryption.

This poses serious challenges to the security and safety of the data that these devices generate and transmit, as well as in determining the responsibility of the relevant actors involved in the design, manufacturing of devices that generate and transmit data.

The Working Party 29, in its Opinion on the Internet of Things, noted, with regards to manufacturers:

"Device manufacturers in the IoT do more than only sell physical items to their clients or white label products to other organisations. They may also have developed or modified the "thing's" operating system or installed software determining its overall functionality, including data and frequency of collection, when and to whom data be transmitted for which purposes (for instance, companies could price the insurance of their employees based on the data reported by the trackers they make them wear14). Most of them actually collect and process personal data which is generated by the device, for purposes and means which they have wholly determined. They thus qualify as data controllers under EU law."[24]

The new instrument should consider ways to capture the responsibility of these manufactures and other actors, for example by considering them as joint data controllers, given that they may determine the purposes and means of processing of personal data.

[23] See, for example, concerns expressed by the Federal Trade Commission in the U.S.: https://www.onthewire.io/ftc-warns-of-security-and-privacy-risks-in-iot-devices/

[24] Opinion 8/2014 on the on Recent Developments on the Internet of Things, available here: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf