Ethical and normative challenges of identification in the Internet of Things

Sandra Wachter*

⋆Oxford Internet Institute, University of Oxford, 1 St Giles, Oxford, OX1 3JS, United Kingdom; and The Alan Turing Institute, British Library, 96 Euston Rd, London, NW1 2DB, United Kingdom

Keywords: Identification, Internet of things, Profiling, Discrimination, GDPR.

Abstract

A defining characteristic of the Internet of Things (IoT) is pervasive collection and linkage of user data to provide personalised experiences. To enable this functionality, IoT devices and services must be connected and share data about users' interactions with multiple nodes in the network. Consistent identification of users and devices across the network is likewise necessary. These aspects of the IoT can pose risks to user privacy. Potentially invasive inferences can be drawn from linked datasets, including data generated through usage of connected devices and services. The forthcoming General Data Protection Regulation (GDPR) contains numerous provisions relevant to the risks posed by identification technologies. However, the strict legal requirements defined in the Articles of the GDPR may be insufficient to ensure a fair balance is struck between user's interests in privacy and the interests of IoT developers and data controllers. To address this gap, this paper proposes a three-step transparency model based on known privacy risks of the IoT, weaknesses in relevant legally binding provisions in the GDPR, and the GDPR's governing principles. Eleven guidelines aimed at IoT developers and data controllers are described addressing how information about the functionality of IoT devices and services should be shared with users. The guidelines describe ethically desirable standards to be adhered to in addition to the GDPR's legally binding requirements. To demonstrate how the guidelines could apply in practice and alter the design choices and practices of IoT developers and data controllers, connected cars are considered as a use case.

1 Introduction

The 'Internet of Things' (IoT) is a rapidly growing technology sector. In the EU, development and adoption of the IoT can be seen in areas such as health and wellness [1–3], utilities [1, 4], urban planning and management [1, 4], logistics and supply chain management [4–6], agriculture, and commerce [4]. Vast amounts of personal and usage data are now collected and shared by IoT devices and services.

A defining characteristic of the IoT is pervasive collection and linkage of user data to provide personalised experiences [7, 8]. To enable this functionality, IoT devices and services must be connected and share data about users' interactions with multiple nodes in the network. Consistent identification of users and devices is likewise necessary. Identity management systems enable access and communication between trusted and intended users, while also providing the necessary infrastructure for potentially invasive linkage of virtual identities and profiling.

User identities in the IoT can be understood as a profile consisting of all information describing the user that is accessible to a decision-maker, based on observations or prior knowledge (e.g. age, location), or inferences about the user (e.g. behaviours, preferences, predicted future actions). Digital identity both uniquely 'singles out' users (i.e. for authentication) and contains information (e.g. inferences) about them. The information constituting this identity can be constructed and managed by both the user and external entities. As a result, the user may lack control or oversight of the content of their identity, how it changes over time and shapes their experiences when the identity is known to other users [9]. Further, users are often unable to assess the validity and quality of inferences made about them.

These aspects of the IoT can pose risks to user privacy [8, 10]. Potentially invasive inferences can be drawn from linked datasets, including data generated by connected devices and services [11, 12]. Inferential analytics drive personalised, potentially discriminatory decision-making [13]. The impossibility of anonymising data [14] and weak cybersecurity standards [15] can similarly exacerbate privacy risks.

In Europe, risks of profiling and invasive inferential analytics enabled by pervasive data collection and linkage are reflected in the regulatory landscape [16]. The forthcoming General Data Protection Regulation (GDPR) contains numerous provisions relevant to the risks posed by identification technologies. However, the strict legal requirements defined in the Articles of the GDPR may be insufficient to ensure a fair balance is struck between user's interests in privacy and the interests of IoT developers and data controllers.

To address this gap, this paper proposes a three-step transparency model based on known privacy risks of the IoT, weaknesses in relevant legally binding provisions in the GDPR, and the GDPR's governing principles. Eleven guidelines aimed at IoT developers and data controllers are described addressing how information about the functionality of IoT devices and services should be shared with users. Specifically, user trust and acceptance can be increased by (a) openly describing the possible risks (e.g. discrimination) of IoT systems; (b) demonstrating the existence of mechanisms to restrict inaccurate or unwanted inferential analytics and

profiling; and (c) showing contingency plans are in place to mitigate risks if systems are compromised. The guidelines describe ethically desirable requirements to be adhered to in addition to the GDPR's legally binding requirements. To demonstrate how the guidelines could apply in practice and alter the design choices and practices of IoT developers and data controllers, connected cars are considered as a use case.

2 Background

A recent literature review highlighted a tension between privacy and identification in the IoT [8]. The review identified four primarily challenges relevant to the design and regulation of identification technologies in the IoT, which are highly inspired by Peppet's [10] harm taxonomy of IoT systems: (1) profiling, inference, and discrimination; (2) control and context-sensitive sharing of identity; (3) consent and uncertainty; and (4) honesty, trust and transparency [8]

a) Profiling, inference, and discrimination

Profiling and tracking of users remains an unresolved privacy challenge in the IoT. There are at least three possible ways of monitoring and profiling that offer grounds for discrimination in IoT systems: (a) data collection that leads to inferences about the person (e.g. internet browsing behaviour); (b) profiling at large through linking IoT datasets (sometimes called 'sensor fusion'); and (c) profiling that occurs when data are shared with third parties that combine data with other datasets (e.g. employers, insurers). According to Roman et al., users can have "access to an unprecedented number of personalized services, all of which would generate considerable data, and the environment itself would be able to acquire information about users automatically" [15].

Unpredictable, invasive profiling and inferential analytics can result from data sharing. By linking multiple devices and the data they produce to a single user identity, the usage of a device or service can be personalised, based upon past behaviours and preferences, and inferences drawn from these data [17]. While potentially offering a 'better' user experience, linkage and personalisation across multiple IoT devices and services nonetheless pose risks to user privacy. Data controllers can draw inferences about the user unrelated to the intended operation of the devices and services she uses [17]. Controlling profiling is difficult due to the uncertain value of data that sensors generate [10].

Inferential analytics and profiling can lead to unfair discrimination (e.g. economic or gender based) [7, 10]. The potential for discrimination holds true even when using non-sensitive data categories, from which sensitive information can still be inferred [18]. Third parties with access to IoT data linked to an identified target can use these data for purposes with which the user would not agree if asked.

b) Control and context-sensitive sharing of identity

Users are often powerless to prevent potentially discriminatory profiling due to a lack of control over their data [19]. It is both infeasible and typically undesirable with respect to privacy to fully reveal one's identity, or as much information as possible about oneself. Segmentation of a user's overall identity can involve the creation of multiple virtual identities that are used to connect to specific networks, devices, or services [20]. Mechanisms to support targeted disclosure of identity may thus facilitate protection of privacy. However, this benefit only occurs if meaningful controlled disclosures are possible; granting disclosure control to users who do not understand the potential risks and benefits of revealing different aspects of their identity can actually expose users to greater privacy risks.

Users often lack any ability to define such context-sensitive constraints on identity disclosure. Devices acting on the user's behalf often similarly lack comparable context-sensitive constraints on identity and personal data disclosure. Multi-user and multi-controller models of ownership of objects also challenge control of identity and personal information disclosure in the IoT. A single-user, single-device model cannot be assumed [20]. Devices can have multiple identities across networks using different identification standards and access controls. Similarly, multiple users can use the same device, meaning a device identity does not connect to a single user identity. The inverse is also true [20].

c) Consent and uncertainty

Identity management and access control systems frequently use a user-centric definition of privacy and trust [7, 21]. Accordingly, a system is considered privacy- and trust-enhancing if it grants the user oversight and choice over the way in which their IoT devices communicate and take actions on their behalf, and thus how their IoT-generated data are shared with IoT devices, other users, and data controllers. Enforcement of privacy preferences prior to communication between IoT devices can protect context-sensitive and subjective expectations of privacy [22].

Users may be unaware of the scope and granularity of their data, and its potential value and inferences that can be drawn from it, as well as the extent to which their data are accessible to third parties outside the context or purpose for which it was created [23, 24]. The uncertain risks accompanying identification technologies, coupled with the conflicting need for users to make an informed choice when setting access permissions (or, at a higher level, choosing to use an IoT device or service in the first instance), undermines the actual protection that user-centric identity management and access controls can offer. If the uncertainty of inferential analytics prevents users from making an informed choice when adopting and using an IoT system (including setting subjective privacy-preserving access permissions), consent cannot be said to be fully informed. Communicating this uncertainty to users remains an outstanding challenge for IoT controllers seeking informed consent [19, 25].

d) Honesty, trust, and transparency

Trust relationships for sharing data can be defined at a device-to-device, device-to-user, and device-to-controller level, with permissions attached to the identity of specific devices, users, and controllers. Trust between objects refers to authentication prior to communication and data access. Prevention of unauthorized objects and actors from accessing a system can

enhance confidentiality, and thus increase user trust [4]. Establishing trust remains challenging since known risks in IoT systems are "security, liability, privacy and data protection" [26]. To achieve trust in an IoT system, developers must demonstrate how they plan to mitigate the significant legal and ethical risks associated with their devices. Processing data in a way that complies with user's rights and expectations can enhance user trust [4]. Similarly, transparency plays an essential role in increasing users' trust [7, 27].

Addressing these challenges proactively requires ethical and legal alignment of IoT design choices, business practices, and regulatory provisions. Given the necessity of pervasive collection and linkage of personal data to enable identification in the IoT, data protection and privacy law are particularly relevant. Data protection law explicitly deals with the question of how to balance privacy with the free flow of data and other business interests. In Europe, the legal landscape is set to substantially change from May 2018 when the GDPR comes into force. The GDPR aims to create harmonised data protection standards across the EU. The framework intends to strike a balance between the free flow of data and the fundamental interests of data subjects (e.g. privacy).

The GDPR will introduce new governing data protection principles (Article 5 and 25) and standards to be complied with by developers and data controllers for IoT devices and services. The wide applicability of the GDPR across all sectors that process personal data - and beyond the border of the European Union (for data controllers processing personal data of European residents) - makes it an ideal basis to evaluate non-sectoral requirements to protect privacy interests in relation to identification technologies. Standards relating to informed consent, notification duties, privacy by design and privacy by default, data protection impact assessment, algorithmic transparency, automated decision-making, and profiling will apply across Europe, and may help address the tension between privacy and identification in the IoT.

The aforementioned review critically examined specific provisions of the GDPR relevant to privacy and identification in the IoT, including transparency (Article 5), data storage, access, rectification, and deletion (Articles 5, 15-17), informed consent (Article 7), notification duties (Articles 13-14 and 33-34), automated decision-making and profiling (Articles 21-22), privacy by design and privacy by default (Article 25), cybersecurity (Articles 33-34), and data protection impact assessment (Article 35-36).

The review concluded that several of these provisions urgently require further specification and implementation into the design and deployment of IoT technologies to minimise the privacy impact of profiling and identification technologies in the IoT. Key concepts are left undefined in the GDPR. This creates ambiguity in how to balance the interests of data subjects in privacy, and the interests of data controllers in identification and providing linked-up IoT services. For example, requirements to notify data subjects in case of data breaches (Article 34) apply only to breaches likely to impose a "high risk to the rights and freedoms of natural persons." Unfortunately, 'high risk' is left undefined, leaving unclear what use sectors or specific data types are seen to pose a high risk.

Elsewhere, limitations are imposed on the scope of protections to be offered by data controllers, minimising the protection they offer against privacy invasive identification, inferential analytics, and profiling. For example, Article 22, which addresses automated decision-making and profiling, limits the definition of 'automated individual decision-making' to decisions affecting data subjects "based solely on automated processing, including profiling, which produces legal effects…or similarly significant affects him or her with legal or similarly significant effects." As several commentators have noted [28–31], this definition includes undefined terminology (i.e. 'solely automated', 'legal or similarly significant effects') that may introduce a loophole in which nominal human involvement in a decision-making process renders the provisions inapplicable.

Several specific points of conflict or ambiguity between GDPR provisions and identification in the IoT were also noted. First, IoT devices and services are often characterised by 'data maximalism', or the excessive collection, storage, and sharing of personal data on the basis that it may prove useful in the future. This tendency directly conflicts with calls for data minimalism or purpose limitation (Article 5(1)(b)), informed consent for specific and well-defined purposes (Article 7), and privacy by design (Article 25).

Second, complex inferential analytics used to profile users and provide personalised services can reveal unforeseen correlations and information about data subjects. This aspect of the IoT again conflicts with expectations that informed consent will be granted for specific and well-defined purposes (Article 7). Further, data controllers are expected under specific circumstances to conduct a data protection impact assessment (DPIA; Article 35) in which the potential risks of processing are to be identified. The uncertain value of personal data generated and processed by IoT devices and services necessarily limits the scope of risks that can be foreseen, and thus the protection offered by DPIAs.

Third, recognising this uncertainty, notification requirements imposed on data controllers (Articles 13-14) may be insufficient to convey the complexity and uncertainty of using the IoT, and its associated data linkage, profiling, and inferential analytics. Data controllers may, for example, be allowed to communicate risks via generic templates or icons aimed at lay audiences. But this mechanism is insufficient to inform properly individuals about their subjective risks or loss of control over their identity [29].

Finally, it remains unclear how much protection data subjects' interests will receive when in conflict with the 'legitimate interests' of data controllers. In connection with the principle of transparency (Article 5), Articles 15 to 17 specify several rights for data subjects to exercise control over disclosures of personal data, and thus prevent invasions of privacy or discriminatory treatment fuelled by the IoT. These rights can, however, be overridden by the 'legitimate interests' of data controllers in some cases. Guidance to strike

a fair balance between the interests of both parties is not offered by the GDPR.

3 Governing principles of the GDPR

Given the privacy risks of the IoT and the lack of clarity in key provisions of the GDPR relevant to the IoT, going forward data subjects may be exposed to devices and services that strike a legally compliant but ethically undesirable balance between privacy and identification. The GDPR may, however, provide alternative grounds to resolve tensions between privacy and identification in the IoT. In particular, the GDPR's governing principles of lawful data processing (Article 5) may provide grounding to make recommendations above and beyond the specific legal requirements of the Articles of the GDPR on how to address the tension between privacy and identifiability in the IoT. Several points of conflict between the GDPR's governing principles and identification in the IoT can be observed.

The governing principles of the GDPR as defined in Article 5 are:

a) Lawfulness, fairness, and transparency (Article 5(1)a)

This trinity of principles describes data controllers' obligations to have legitimate grounds for processing of personal data. To ensure the lawfulness of the processing, transparency plays a key role. Data subjects should be aware of the processing purposes and should be provided with suitable notification and information regarding its scope. Even though fairness is not defined, the Article 29 Working Party and scholars believe that fairness links to awareness, meaning data subjects should be made aware of data processing [11, 32–34]. This is especially relevant for IoT developers since devices often collect vast amounts of personal data, some of which can be considered sensitive (e.g. FitBit, health data) [35]. The seamless implementation of these techniques can cause users to forget that their data is constantly being collected [11, 36, 37].

b) Purpose limitation (Article 5(1)b)

The principle of purpose limitation refers to the obligation of data controllers to only use the collected data for specific and well-defined purposes. The usage of collected data for other than the initial purpose has to be compatible with the initial purpose. Consent of the data subject or Member State laws can offer grounds to legitimise additional processing not related to the initial purpose [35]. The principle of purpose limitation can pose difficulties for the IoT [38]. Very often vast amounts of data are collected for vague or broadly defined purposes [39]. Sensor fusion [14], or the linkage [40, 41] of existing but previously unconnected datasets, can offer new purposes for data analytics which were not envisioned when the data were collected. Invasive and unpredictable inferential profiling is enabled by identification services that link devices and the data they collect [8].

c) Data minimisation (Article 5(1)c)

Data controllers are required to only use data that are "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [42]; data controllers must also ensure that the collected data are necessary for their intended processing scope, and that excessive data are not collected beyond this scope. For the IoT, data controllers must establish that the data being collected is necessary to deliver their product or services. This principle challenges the typical 'data maximalism' of the IoT and Big Data analytics by extension, which require vast data collection and linkage for the personalisation of services (but not for the immediate functionality of a solitary device or service) [8].

d) Accuracy (Article 5(1)d)

Data controllers are required to only store and use data that are accurate. Accuracy refers to the need for data to be correct and complete with regard "to the purposes for which they are processed." Incorrect data must be rectified or deleted without undue delay [42]. IoT developers face a significant challenge as a result to curate and update their datasets to meet this requirement. Verification of user identity is critical to ensure accuracy, particularly when a device can potentially be used by multiple people. Without verification, usage data from multiple users could be mistakenly recorded under a single user's profile, leading to inaccurate processing.

e) Storage limitation (Article 5(1)e)

Storage limitation obligates data controllers to not store personal data for "longer than is necessary for the purposes for which the personal data are processed." In the IoT, the utility of stored data for the intended purpose of a particular product or service will need to be periodically re-assessed. Storage is also allowed without a link to a specific processing purpose when data "will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes." This principle can conflict with competing interest and rights of data subjects (e.g. right of access, right to be forgotten) or other obligations according to Member State laws that require longer or shorter periods of data storage (e.g. Art 23 GDPR, access to historical data for criminal investigations) [12, 43].

f) Integrity and confidentiality (Article 5(1)f)

Data controllers are required to implement appropriate security mechanisms to guard against unlawful access, data breaches, data losses or leaks. A high cybersecurity standard is established. For IoT developers, high cybersecurity standards and mechanisms must be embedded in the design of devices and services. This requirement can be particularly challenging for technologies with simplistic functionality or low computational power (e.g. RFID or WiFi) that cannot support intensive mechanisms such as encryption.[14] The effectiveness of security mechanisms can quickly fade due to newly identified weaknesses or types of attacks. Integrity and confidentiality, therefore, appear to require long-term commitment by IoT developers to identify new threats, and patch their devices and services accordingly [15].

g) Accountability (Article 5(2))

The principle of accountability should be achieved through three main duties derived from the six preceding principles.[35] First, data controllers are obligated to keep records of their data processing activities. Second, they should implement 'privacy by design' and 'privacy by default' mechanisms. Third, data controllers are required to undertake a data protection impact assessment for high-risk data processing. These provisions aim to ensure that data controllers take their obligations to respect all the aforementioned principles seriously, and can demonstrate compliance as required [35].

4 Guidelines for transparency and trust in the IoT

The seven governing principles of the GDPR are critical for balancing privacy, trust, and identifiability in the IoT. Profiling and discrimination cannot always be prevented. Protection of privacy and the resilience of systems against cyber-attacks similarly cannot always be guaranteed. Rather than only focusing on the untenable promise to guarantee privacy at all times, fostering user trust through transparency and honest communication of risks may be a better option. Openness and honesty about possible risks might be preferable to leading users to believe that their interests will be protected in all cases. Users require high quality, understandable, and sufficiently broad information to make an informed decision about whether to trust and ultimately adopt a system. Dialogue between developers and users is critical because IoT is seamless, often hidden, and can lead to unpredictable and opaque discrimination.

The foundational principles of the GDPR provide a robust foundation to propose supplementary guidelines that seek to close the gap between the GDPR's explicit legal requirements and ethically desirable design and communication in the IoT. A three-step transparency model is proposed to help data subjects comprehend the actual privacy risks of profiling and identification technologies in the IoT, and thus be better placed to control disclosures of personal data and modifications to their identity. The proposals made here meet calls in EU policy to define principles and guidelines for IoT devices [8].

The three-step transparency model takes the form of eleven guidelines responsive to three areas:

(1) the GDPR's governing principles (Article 5);

(2) ambiguities and ethically undesirable limitations in provisions of the GDPR relevant to the IoT; and

(3) known risks to privacy owing to profiling and identification in the IoT.

The guidelines are intended to inform IoT developers and data controllers about how to mitigate some of the risks related to the IoT, and to comply with the spirit of the GDPR's guiding principles when its legally binding provisions offer insufficient protection to data subjects. Rather than heavily focusing on the untenable promise to guarantee privacy at all times, user trust and acceptance should be increased by

a) describing the possible risks (e.g. discrimination) of IoT systems openly (e.g. notification, data protection impact assessment, privacy policies);

b) showing what kind of mechanisms are in place to limit inaccurate or unwanted predictions and assumptions, and consequently discrimination based on profiling (e.g. agile consent models, accurate prediction models, right of access, ethical sharing practises with third parties, opt-out options from profiling, algorithmic transparency and anti-discrimination tools in automated decision-making, and profiling);

c) showing transparent contingency plans to mitigate risks (discrimination) if the system is compromised (e.g. cyber risks, notification of data breaches, privacy enhancing technologies).

4.1 Transparent information about possible risks

Guideline 1: Data Protection Impact Assessment (DPIA)

Whenever "systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling" and new technologies for data processing are used, a DPIA will be mandatory if the processing is 'likely to result in a high risk to the rights and freedoms of natural person'. Due to the growing importance of the IoT and the associated risks for privacy, a DPIA will be mandatory for most IoT devices. IoT developers will need to assess the possible risks of their devices. If their assessment indicates a high privacy risk, prior consultation of a supervisory authority will be mandatory.

Even though the Article 29 Working Party [44] has issued guidelines stating that the DPIA should be (at least in parts) publicly available, their recommendation is not legally binding. The GDPR does not address this issue. However, it is recommended to always publish the results and the methods of the DPIA. This will help data subjects to better understand the possible risks of their usage of an IoT product or service, and to freely consent to data processing. Greater communication of risks can help increase trust in IoT devices. Further, even if a DPIA is not legally mandated, IoT developers should consider evaluating their technologies nonetheless. In cases where a DPIA is deemed unnecessary, a public statement of the reasons behind this decision can have a similar effect. This would help increase trust in IoT devices, as users can see that data controllers take their privacy seriously, evaluated possible risks carefully, and went beyond what is legally mandated to ensure privacy.

Guideline 2: Tailor communication to the needs and abilities of users

Article 12 aims to ensure transparent information and communication to enable data subjects to exercise their rights as defined in the GDPR. The language used should be in a 'concise, transparent, intelligible and easily accessible form, using clear and plain language' [42], indicating that the

imagined audience is a lay person [45]. These requirements are even more important when children are addressed (Art 12 (1)).

While it is intuitively preferable to communicate with data subjects with concise and easily understandable language for the sake of simplicity and to avoid confusion, this approach also limits the quality of the information being conveyed. Possible negative consequences of data collection and processing, including leaks owing to hacking, invasive inferences due to sensor fusion, and the broader predictive and inferential power of big data analytics can be difficult to communicate with easily understandable language. When it comes to communicating possible but uncertain risks (profiling, identification or data breaches), elaborate communication may be necessary.

Guideline 3: Icons might not always be the best tool for communication

To achieve lawfulness, fairness, and transparency, data subject awareness is key. The GDPR implements new obligations related to transparency. This is reflected in Articles 13-14, which create notification duties for data controllers. Amongst other things, data controllers have to inform data subjects about intended data processing purposes, contact details of the data controller, the recipients of the subject's personal data, the period for which the personal data will be stored, the usage of profiling and the right to object to it (Articles 13 (2) (b) and 14 (2) (c)), and the existence of automated decision-making, including profiling (Articles 13 (2) (f) and 14 (2) g)). It is reflected in Art 12 (7) that the information about intended processing purposes referred to in Articles 13-14 can be conveyed using standardised icons. Most IoT devices have small screens which make reading policy statements harder, which can be problematic if freely given and informed consent is required [10].

Similar to the concerns above, since the information provided aims to inform data subjects about what will happen to their data, and to enable them to make an informed decision if they agree to those processes, standardised icons and short descriptions may prove insufficient. In particular, the requirement to inform data subjects about the logic involved in automated decision-making (including profiling) will be challenging in this regard due to the inherent opacity and complexity of algorithmic systems [46].

Even though the simplicity and standardised communication offered by icons are desirable, their educational power is restricted, even if accompanied with short descriptive text. Additional information about the functionality of systems being used, particularly in the case of complex algorithms and machine learning tools, should be provided for users who want to learn more, especially since the opacity and inscrutability of AI based systems offers a great source for discrimination.

Guideline 4: Privacy should not be the foe of transparency

In order to guarantee trust and awareness of data processing, the GDPR not only requires data controllers to notify data subjects about intended processing purposes (Articles 13-14), but also allows data subjects to request more or less the same information at any time under the right of access (Article 15). The right of access empowers data subjects to independently manage their privacy without relying on data controllers to provide appropriate and timely information [47]. However, at the same time Art 15 (4) and Recital 63 allow data controllers to limit the requested information based on conflicts with the rights and freedoms of others. Freedoms of others include privacy rights of other data subjects or interests of data controllers such as trade secrets and intellectual property rights [47]. The GDPR calls for a fair balance between the interests of data subjects and data controllers.

Finding this balance will prove very challenging in cases where information about profiling and automated decision-making is requested. The profiles used are usually built on data from reference groups (e.g. personal data of other users). Group privacy rights are not sufficiently acknowledged in current data protection law as it focuses on the individual data subject rather than the collective [48–50]. This fact could be used as a loophole to not disclose information about profiling, since it could be claimed that this information infringes other data subjects' privacy. Concerns with the privacy of others should not be misused to prevent access to relevant information about the scope and logic of automated processing. New approaches on how to protect 'group privacy' [33, 46, 48, 51, 52] in parallel to individual privacy need to be developed.

4.2 Transparent procedures to mitigate risks of profiling

Guideline 5: Implement anti-discrimination tools and procedures

One of the most pressing problems concerning the IoT is discrimination [10]. Recital 39 GDPR reflects this concern as it states that "online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags" can lead to identification and profiling. This is further acknowledged in Recital 71 where it is stated "the controller should use appropriate mathematical or statistical procedures for the profiling" to prevent discrimination or biases in profiling or automated decision-making. Sensitive or proxy data [13] as well as inaccurate or incomplete data [38] can form the basis for discriminatory effects [46], especially when data sets are linked [40, 41]. This is particularly challenging when multiple users use one device, the usage behaviour impacts the possible predictions of another user.

Critical assessment of the provenance of data is required. Organisational measures should also be implemented to guarantee the accuracy and reliability of the gathered data [7]. Consumers might provide incorrect data or do not fully understand the consequences if their behaviour is constantly monitored. Even when users are aware of the potential consequences of their usage of a device or service, changing settings may prove inconvenient or damaging [53]. Further, data processing can also lead to unexpected biases because

potential relationships between data categories, often revealed only through aggregation and linkage of disparate datasets, may not be known at the time of data collection [54]. Tools such as ethical algorithmic auditing should be implemented to flag up discrimination [28]. Internal auditing schemes should be considered to guard against discrimination of protected groups but also to protect victims of unanticipated discrimination [46, 55].

Guideline 6: Tell users about assumptions and inferences

According to Recital 63 the right of access (Article 15) aims to make users 'aware of, and verify, the lawfulness of the processing'. Direct access to the data that is held should be given if possible. This allows not only for the accuracy of the collected data to be verified, but also rectified if inaccurate. In addition, Article 15 (1) (h) allows data subjects to receive 'meaningful information about the logic involved, as well as the significance and the envisaged consequences' of automated processing including profiling. Disclosing detailed information about the algorithms used for such processes could have adverse effects on data controllers' trade secrets and IP rights.

Tools to provide users with meaningful information about the scope of data being processed and inferences being drawn from it should be implemented. Existing mechanisms such as Google's ad manager provide a model. Such tools can help data subjects understand the assumptions being made, and to correct these assumptions. The same applies to inferences based on their data. This will help to optimise services and increase users' trust and acceptance of identification technologies in the IoT.

Guideline 7: Ethical data sharing practices

Privacy concerns do need necessarily lie with the data controllers who collected the data. Third parties with whom data controllers share the collected data can also pose a risk to privacy of users. As Weber explains, "since the possibility to build extensive personal profiles can be hardly avoided, data anonymization is important in the context of data sharing" [27]. Insurance companies or employers [10] could, for example, have increasing interest to obtain data to assess current behaviour and infer future risks, for instance future likelihood of health impairments inferred from FitBit data. The GDPR requires that the recipients of data have to be disclosed if data sharing is planned (Art 13 and 14).

However, it is recommended that prior to sharing, an assessment of possible risks should be undertaken. Possibilities of, for example, racial and economic discrimination should be evaluated prior to sharing. Users might not foresee the possible risks of inferences drawn from their data, especially when datasets are combined. Edwards et al even suggest that "social impact assessment" should be considered that would "consider the public interest as well as the interests and rights of enterprises and users" [56] and look at factors like sharing practices since "B2B relationships, are not designed with privacy as a prime consideration "[56].

Guideline 8: Agile consent

Art 7 will readjust the power dynamic between data subjects and data controllers. Due to Art 7 (4), the freedom with which consent is given will be evaluated on the basis of whether the obligation to share data is a precondition to use the service. In other words, privacy policies that deny the use of a service because a data subject refused to share all their data (e.g. pre-ticked boxes) [39] will no longer be legal.

In order to meet this requirement an agile and customised consent system is preferable [57]. It should be stated what kind of data is necessary for the offered service and what kind of data can be voluntarily shared.

Guideline 9: Disconnecting and objecting

IoT devices are constantly collecting data about their users, which is why it has been suggested that disconnect options should be considered [58] that disable tracking. This approach is related to a similar provision in the GDPR: the right to object to profiling in Art 21. The framework states that regarding direct marketing purposes, the objection of a data subject will always trump the interest of data controllers. However, since profiling can be used for other purposes as well, e.g. to optimise services, data controllers can overrule the objection by demonstrating legitimate interests.

Data controllers are recommended to evaluate if profiling is necessary for their service and should possibly act according to the request of the user or at least consider opt-out options for specific purposes [59, 60]. To incentivise data subjects to share and consent to processing of their data, data controllers should inform them about social or individual benefits.

4.3 Transparent contingency plans in case of systems failures

Guideline 10: Privacy by default and privacy by design

The GDPR states in its principles and various Articles (e.g.6, 24, 32-34) that 'privacy by default' and 'privacy by design', pseudonymisation, encryption and other privacy enhancing tools (PET) should be used. This approach should help to increase user trust and public acceptance in identifying technologies and protect privacy. However, as Ohm [14] stated, PETs are in most cases flawed. Rather, it must be assumed that a sufficiently motivated adversary will always be able to re-identify a user.

Rather than promising that data can always be protected, ensuring users retain realistic expectations of the extent to which their data can actually be protected should be considered. It is encouraged to explain that data protection will be guaranteed to the best of data controller's abilities. However, data controllers should explain that privacy risks will remain even under optimal conditions. Explaining contingency plans in cases of data breach can help. For example, what measures are in place if systems are attacked? How will the negative consequences of data leaks be mitigated? It is also crucial to state how effective PET's will be in cases of cyber-attacks or data leaks. This will help users to make an informed choice in deciding to use a service, as they will have more realistic expectations of the associated risks and mitigating factors.

Guideline 11: Be honest if cybersecurity fails

Cybersecurity hygiene is closely connected to protection of privacy. Security is one of the major problems in the IoT reflected in the principles and articles of the GDPR and the reviewed literature (e.g. [10, 14, 58]). Article 33 GDPR will require data controllers to notify a supervisory authority when data breaches occur that are posing a 'risk to the rights and freedoms of natural persons'. However, data controllers only need to inform the data subject in serious cases where the consequences of the data breach will likely pose a "high risk" to the data subject (Article 34).

Even though it is understandable that not every leak needs to be communicated, the barrier of "high risk" should be seriously reconsidered, or at least granted a consistent operational definition. It remains unclear who will assess this risk, or how the consequences for users will be framed. Having a lower threshold for communicating data breaches could help to increase users' trust, otherwise they will not be aware of data breaches and leaks. IoT providers can develop internal definitions and codes of conduct to determine when 'high risks' exist, and what should be communicated to data subjects in those cases.

5 Case study: Connected cars

Applying the guidelines described in the previous section to a hypothetical use case will help clarify their potential practical impact on IoT design and deployment. Connected cars are a rapidly growing IoT sector. Estimates suggest that by 2020 connected cars will have a global market of EUR 115.26 billion with a strong focus on safety features, autonomous driving, and (personalised) entertainment (e.g. dash-boards) benefitting from Internet connectivity. Predicted benefits include higher safety standards (e.g. fatigue detection systems, tracking in case of theft), greater energy efficiency, increased productivity (e.g. spending less time en route), and improved convenience (e.g. remotely controlling thermostats) [61].

Despite these potential benefits, problems remain. By definition, connected cars must be able to communicate with other cars, infrastructure, and other devices [61]. This connectivity introduces concerns around cybersecurity (hacking brakes, identity theft), behaviour monitoring as well as data protection and privacy [62]. These concerns could hamper the wide-spread implementation, but the proposed guidelines can increase user trust and foster ethical practices.

Behavioural profiling (e.g. based on driving behaviour; or for entertainment services) is one major concern that can be mitigated through the guidelines. Guideline 1 proposes to make DPIA's public to allow users to inform themselves about the possible risks and assess whether data controllers have sufficiently addressed them. Guidelines 2 and 3 urge data controllers to use easily understandable language, but to elaborate when explaining possible risks, especially relating to profiling and tracking. This is crucial as data collection is seamless and ubiquitous. Data subjects may therefore be unaware of the scope of evaluation undertaken, and unable to predict the inferences drawn about them. Data on braking and accelerating behaviour or location data can, for example, be used to create privacy invasive risk profiles of drivers.

Guideline 5 recommends data controllers to implement anti-discrimination tools and procedures to mitigate unlawful and unintended discrimination to build trust between data subjects and data controllers. However, potential discrimination does not stop with the data controller that collected the data. Thus, guideline 7 is essential, as it calls upon data controllers to have ethical data sharing practices. This means that data controllers should not only inform data subjects about who they share the data with (as per Art 13-14), but also consider whether the data subject would find the recipients acceptable. For connected cars, driving behaviour data can have negative consequences for the data subject if shared with insurance companies to set personalised premiums or advertisers to serve tailored advertisements to in-car displays, for example.

Data subjects should also be given the opportunity to exercise agile consent (guideline 8). In practice, data subjects would need to be able to customise the types of data being collected and processed. But even after consent is given, data subjects should be given opportunities to opt-out, disconnect or disable tracking (guideline 9). Implementation of agile consent and opt-out features require data controllers to re-think their design choices. Ideally, devices and services can be designed to provide full or minimally limited functionality even if a data subject opts-out or does not give consent to the collection, processing, or sharing of certain data types. For connected cars, developers should consider giving drivers and passengers an option to disable the collection of location data, or to have multiple user accounts with customised preferences (e.g. if the car is used by a family rather than a single driver).

Guidelines 4 and 6 aim to grant data subjects oversight and control over how their data is evaluated. If data subjects exercise their right of access to learn about what and how data is being processed, data controllers should provide this information unless overriding interests exist (e.g. privacy of others, trade secrets). These overriding interests should be interpreted narrowly (cf. [63]). However, exercising the right of access can be challenging as connected cars communicate with other cars, exchange and collect other users' data which may infringe on the privacy of others to which the individual may not be entitled. Where access cannot be granted, guideline 6 proposes to, at a minimum, inform individuals of the logic involved in data processing to explain what kind of inferences are being drawn.

Apart from privacy and discrimination issues, cyber-security is another significant area of concern that poses a barrier to trust in connected cars. Known vulnerabilities include remote hacking of brakes, 'virtual keys', and data theft (e.g. credit card details) [61]. Here guideline 10 builds on the principle of privacy by default and privacy by design, advising data controllers to communicate how and to what extent privacy enhancing technologies help to protect privacy even if the system is compromised. This notion of open and honest communication is closely connected to guideline 11 which recommends that data controllers inform data subjects if the system is hacked or data leaks occurred, even if a high risk

for data subjects is not expected. User awareness of the existence and effectiveness of security standards is essential to establish trust in safety critical systems such as connected cars.

6 Conclusion

IoT identification technologies raise many concerns around identification, privacy, and therefore data protection. IoT systems relay on large data collection form diverse sources and data exchange with various devices to provide seamless, linked-up and personalised services. Machine learning and profiling is increasingly used to provide these personalised services. Pervasive data collection and linkage of disparate datasets enables invasive and unpredictable inferences to be drawn about individuals or groups. The inherent vulnerabilities of many IoT systems (due to limited processing power or a lack of commitment by developers) make them vulnerable to cyber-attacks.

The GDPR can help to alleviate many of the identification and privacy risks posed by the IoT. The governing principles (Art 5) explain how European legislators envision fair, transparent and lawful data processing. As IoT systems can conflict with many of these principles (e.g. purpose and storage limitation, data minimisation), developers should be encouraged to go above and beyond the strict legal requirements of the GDPR to design trustworthy and privacy enhancing systems and services. To assist developers in this process, a three-step transparency model in the form of eleven guidelines was proposed. One case study (connected cars) was then analysed to show how the guidelines might apply in practice.

IoT systems bear great societal and economic potential in areas such as transport, health, energy consumption, public space and environmental monitoring, as well as personalised and linked-up services for users. In order to fully harness the potential of this technology, user trust and public acceptance is crucial. The proposed guidelines are a first step to dissolve some of the regulatory ambiguities about how to interpret the GDPR to protect user privacy without hampering the deployment of IoT systems.

Acknowledgements

This paper is part of the Privacy-Enhancing and Identification-Enabling Solutions for IoT (PEIESI) project, part of the PETRAS Internet of Things research hub. PETRAS is funded by the Engineering and Physical Sciences Research Council (EPSRC), grant agreement no. EP/N023013/1.

References

[1] Khodadadi F, Dastjerdi AV, Buyya R. Internet of Things: An Overview. *ArXiv Prepr ArXiv170306409*https://arxiv.org/abs/1703.06409 (2017, accessed 30 June 2017).

[2] Gonçalves F, Macedo J, Nicolau MJ, et al. Security architecture for mobile e-health applications in medication control. In: *2013 21st International Conference on Software, Telecommunications and Computer Networks - (SoftCOM 2013)*. 2013, pp. 1–8.

[3] Cisco. *Securing the Internet of Things: A Proposed Framework*http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html (2016, accessed 6 July 2017).

[4] Sicari S, Rizzardi A, Grieco LA, et al. Security, privacy and trust in Internet of Things: The road ahead. *Comput Netw* 2015; 76: 146–164.

[5] Yuqiang C, Jianlan G, Xuanzi H. The Research of Internet of Things' Supporting Technologies Which Face the Logistics Industry. In: *2010 International Conference on Computational Intelligence and Security*. 2010, pp. 659–663.

[6] Chaves LWF, Decker C. A survey on organic smart labels for the Internet-of-Things. In: *2010 Seventh International Conference on Networked Sensing Systems (INSS)*. 2010, pp. 161–164.

[7] Tene O, Polonetsky J. Big data for all: Privacy and user control in the age of analytics. *NwJ Tech Intell Prop*http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/nwteintp11&section=20 (2013, accessed 2 October 2014).

[8] Wachter S. *Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR*. SSRN Scholarly Paper ID 3083554, Rochester, NY: Social Science Research Networkhttps://papers.ssrn.com/abstract=3083554 (6 December 2017, accessed 12 December 2017).

[9] Floridi L. The Informational Nature of Personal Identity. *Minds Mach* 2011; 21: 549–566.

[10] Peppet SR. Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent. *Tex Rev* 2014; 93: 85.

[11] Eskens SJ. *Profiling the European Citizen in the Internet of Things: How Will the General Data Protection Regulation Apply to this Form of Personal Data Processing, and How Should It?* SSRN Scholarly Paper ID 2752010, Rochester, NY: Social Science Research Networkhttps://papers.ssrn.com/abstract=2752010 (29 February 2016, accessed 8 July 2017).

[12] Hon WK, Millard C, Singh J. Twenty Legal Considerations for Clouds of Thingshttps://papers.ssrn.com/sol3/papers.cfm?abstract_id=2716966 (2016, accessed 8 July 2017).

[13] Barocas S, Selbst AD. Big data's disparate impact. *Calif Law Rev*; 104. Epub ahead of print 2016. DOI: 10.15779/Z38BG31.

[14] Ohm P. Broken promises of privacy: Responding to the surprising failure of anonymizationhttps://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 (2009, accessed 28 June 2017).

[15] Roman R, Najera P, Lopez J. Securing the Internet of Things. *Computer* 2011; 44: 51–58.

[16] Wachter S. Privacy: Primus Inter Pares — Privacy as a Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rightshttps://papers.ssrn.com/abstract=2903514 (2017, accessed 14 September 2017).

[17] Schermer BW. The limits of privacy in automated profiling and data mining. *Comput Law Secur Rev* 2011; 27: 45–52.

[18] Romei A, Ruggieri S. A multidisciplinary survey on discrimination analysis. *Knowl Eng Rev* 2014; 29: 582–638.

[19] Mittelstadt BD, Floridi L. The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Sci Eng Ethics* 2016; 22: 303–341.

[20] Sarma AC, Girão J. Identities in the Future Internet of Things. *Wirel Pers Commun* 2009; 49: 353–363.

[21] Friedewald M, Vildjiounaite E, Punie Y, et al. Privacy, identity and security in ambient intelligence: A scenario analysis. *Telemat Inform* 2007; 24: 15–29.

[22] Nissenbaum H. *Privacy as Contextual Integrity*. SSRN Scholarly Paper ID 534622, Rochester, NY: Social Science Research Networkhttp://papers.ssrn.com/abstract=534622 (31 May 2004, accessed 12 March 2013).

[23] boyd danah, Crawford K. Critical Questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon. *Inf Commun Soc* 2012; 15: 662–679.
[24] Mittelstadt B. Ethics of the health-related internet of things: a narrative review. *Ethics Inf Technol* 2017; 19: 157–175.
[25] Fairfield J, Shtein H. Big Data, Big Problems: Emerging Issues in the Ethics of Data Science and Journalism. *J Mass Media Ethics* 2014; 29: 38–51.
[26] European Commission. *Commission Staff Working Document: Advancing the Internet of Things in Europe*. SWD(2016) 110 final, European Commissionhttp://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN (2016, accessed 8 July 2017).
[27] Weber RH. Internet of things: Privacy issues revisited. *Comput Law Secur Rev* 2015; 31: 618–627.
[28] Wachter S, Mittelstadt B, Floridi L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *Int Data Priv Law*https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469 (2017).
[29] Wachter S, Mittelstadt B, Russell C. Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR. *ArXiv Prepr ArXiv171100399*.
[30] Veale M, Edwards L. *Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling*. SSRN Scholarly Paper ID 3071679, Rochester, NY: Social Science Research Networkhttps://papers.ssrn.com/abstract=3071679 (15 November 2017, accessed 27 December 2017).
[31] Edwards L, Veale M. *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You are Looking For*. SSRN Scholarly Paper ID 2972855, Rochester, NY: Social Science Research Networkhttps://papers.ssrn.com/abstract=2972855 (23 May 2017, accessed 12 August 2017).
[32] Article 29 Data Protection Working Party. *Opinion 8/2014 on the on Recent Developments on the Internet of Things*. 14/EN WP 223http://www.dataprotection.ro/servlet/ViewDocument?id=1088 (2014, accessed 8 July 2017).
[33] Bygrave LA. *Data protection law: Approaching its rationale, logic and limits*. Kluwer Law Intl, 2002.
[34] Costa L, Poullet Y. Privacy and the regulation of 2012. *Comput Law Secur Rev* 2012; 28: 254–262.
[35] Jay R. *Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice*. 4th Revised edition edition. London: Sweet & Maxwell, 2017.
[36] Weiser M. The computer for the 21st century. *Sci Am* 1991; 265: 94–104.
[37] Gershenfeld N. *When things start to think*. Macmillan, 1999.
[38] Moerel L, Prins C. Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things. *Brows Download This Pap*https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123 (2016, accessed 8 July 2017).
[39] de Hert P, Papakonstantinou V. The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Comput Law Secur Rev* 2016; 32: 179–194.
[40] Ruggieri S, Pedreschi D, Turini F. Data mining for discrimination discovery. *ACM Trans Knowl Discov Data TKDD* 2010; 4: 9.
[41] Zarsky T. The Trouble with Algorithmic Decisions An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making. *Sci Technol Hum Values* 2016; 41: 118–132.
[42] European Union. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). 2016/679http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN (2016, accessed 10 November 2016).
[43] Abbas R, Michael K, Michael MG. Using a social-ethical framework to evaluate location-based services in an internet of things world. *Int Rev Inf Ethics* 2015; 22: 42–73.
[44] Article 29 Data Protection Working Party. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. 17/EN WP 248, 2017.
[45] Frank. Art 12 Transparente Information, Kommuikation. In: Gola P, Eichler C (eds) *Datenschutz-Grundverordnung VO (EU) 2016/679: Kommentar*. München: C.H. Beck, 2017.
[46] Mittelstadt B, Allo P, Taddeo M, et al. The Ethics of Algorithms: Mapping the Debate. *Big Data Soc*.
[47] Ehmann E. Art 15 Rechte der betroffenen Person. In: Ehmann E, Selmayr M, Albrecht JP (eds) *DS-GVO: Datenschutz-Grundverordnung: Kommentar*. München: C.H. Beck, 2017.
[48] Mittelstadt B. From Individual to Group Privacy in Big Data Analytics. *Philos Technol*. Epub ahead of print 11 February 2017. DOI: 10.1007/s13347-017-0253-7.
[49] Mantelero A. From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era. In: *Group Privacy*. Springer, 2017, pp. 139–158.
[50] Floridi L. Group privacy: a defence and an interpretation. In: *Group Privacy*. Springer, 2017, pp. 83–100.
[51] Taylor L, Floridi L, van der Sloot B (eds). *Group Privacy: New Challenges of Data Technologies*. 1st ed. New York: Springer, 2017.
[52] Mantelero A. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Comput Law Secur Rev* 2016; 32: 238–255.
[53] Acquisti A, Grossklags J. Privacy and rationality in individual decision making. *IEEE Secur Priv* 2005; 3: 26–33.
[54] Kusner MJ, Loftus JR, Russell C, et al. Counterfactual Fairness. *ArXiv170306856 Cs Stat*http://arxiv.org/abs/1703.06856 (2017, accessed 8 July 2017).
[55] Mittelstadt B. Auditing for Transparency in Content Personalization Systems. *Int J Commun* 2016; 10: 12.
[56] Edwards L, McAuley D, Diver L. From Privacy Impact Assessment to Social Impact Assessment. In: *2016 IEEE Security and Privacy Workshops (SPW)*. 2016, pp. 53–57.
[57] Kaye J, Whitley EA, Lund D, et al. Dynamic consent: a patient interface for twenty-first century research networks. *Eur J Hum Genet* 2015; 23: 141–146.
[58] Weber RH, Weber R. *Internet of things: legal perspectives*. Springer Science & Business Media, 2010.
[59] Rubel A, Jones KML. *Student Privacy in Learning Analytics: An Information Ethics Perspective*. SSRN Scholarly Paper ID 2533704, Rochester, NY: Social Science Research Networkhttp://papers.ssrn.com/abstract=2533704 (3 September 2014, accessed 22 July 2015).
[60] Hildebrandt M. Who Needs Stories if You Can Get the Data? ISPs in the Era of Big Number Crunching. *Philos Technol* 2011; 24: 371–390.
[61] Lengton M, Verzijl D, Dervojeda K, et al. Internet of Things connected cars. *Bus Innov Obs Contract No*; 190.
[62] HM Government. *The Key Principles of Cyber Security for Connected and Automated Vehicles*. HM Governmenthttps://www.gov.uk/government/uploads/system/uploads/attachment_data/file/661135/cyber-security-connected-automated-vehicles-key-principles.pdf (2017, accessed 8 January 2018).
[63] Article 29 Data Protection Working Party. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. 844/14/EN WP 217http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (accessed 8 January 2018).