International Journal on Data Science and Technology
2023; 9(3): 35-40
http://www.sciencepublishinggroup.com/j/ijdst
doi: 10.11648/j.ijdst.20230903.11
ISSN: 2472-2200 (Print); ISSN: 2472-2235 (Online)

SciencePG
Science Publishing Group

The Internet of Things and Privacy Concerns: The Applicability of the GDPR Transparency Principle to the Internet of Things

Senna Mougdir

Department Private Law, University of Amsterdam, Amsterdam, The Netherlands

Email address:
s.y.mougdir@gmail.com

To cite this article:
Senna Mougdir. (2023). The Internet of Things and Privacy Concerns: The Applicability of the GDPR Transparency Principle to the Internet of Things. *International Journal on Data Science and Technology*, *9*(3), 35-40. https://doi.org/10.11648/j.ijdst.20230903.11

Received: September 23, 2023; **Accepted**: November 1, 2023; **Published**: December 28, 2023

Abstract: The use of the "Internet of Things" (IoT) is rapidly increasing. The European Union (EU) is expected to make major investments in areas such as smart homes, personal health and wearables, smart energy, smart cities and smart mobility. IoT applications are emerging in many areas such as healthcare, transportation and traffic control, public space and environmental monitoring, social interaction, personalized shopping and commerce, home automation and more. These IoT devices are constantly collecting vast amounts of personal data, such as location data and health data, in order to function properly or to optimize and customize their services. IoT is defined by connectivity and linking services, tailored to the specific needs of users. Objects and services must interconnect and share data about specific users in order to provide connected services, not just the direct interaction of users with specific nodes. Networked seamless services are not possible without repeated and consistent user identification. However, the pursuit of user identification and personalization comes with privacy risks. Privacy is a major concern as the Internet of Things develops, especially in regard to information to users and consent. Data collection devices and all necessary information about them should be made available electronically to all data subjects within range of the devices, with the data subjects being able to reply electronically and express their own privacy preferences as well. In this paper, examples of technologies and initiatives are presented and discussed in light of the GDPR and additionally, the WP29 recommendations are discussed.

Keywords: GDPR, Internet of Things, Transparency, Privacy by Design, Anonymization, Pseudonymization

1. Introduction

The use of the "Internet of Things" (IoT) is rapidly increasing. The European Union (EU) is expected to make major investments in areas such as smart homes, personal health and wearables, smart energy, smart cities and smart mobility. [1] IoT applications are emerging in many areas such as healthcare, transportation and traffic control, public space and environmental monitoring, social interaction, home automation [2], personalized shopping and commerce [3] and more. These IoT devices are constantly collecting vast amounts of personal data, such as location data and health data, in order to function properly or to optimize and customize their services. IoT is defined by connectivity and linking services, tailored to the specific needs of users. Objects and services must interconnect and share data about specific users in order to provide connected services, not just the direct interaction of users with specific nodes. Networked seamless services are not possible without repeated and consistent user identification. However, the pursuit of user identification and personalization comes with privacy risks. Data controllers can draw inferences from these data. [4] Users can easily find these insights intrusive, unexpected, and unwanted. Inferential analysis and linking of different records can also lead to discriminatory treatment [5], which limits user analysis. [6] The inability to anonymize data [7] and weak cybersecurity standards often due to the limited computing power of identification technologies exacerbate privacy risks. Taken together, these risks make free and informed consent in the IoT a challenge. Privacy policies often do not clearly communicate the risks of data processing and links to user records requiring consistent user identification. [8] The EU General Data Protection Regulation (GDPR) could improve this situation. The regulation went into effect in May 2018 and addresses many of these risks. [9]

The GDPR sets out data processing principles (Articles 5 and 25) and establishes privacy standards related to IoT devices. Harmonized standards on declarations of consent, reporting obligations, privacy by design and privacy by default, data protection impact assessment, algorithm transparency, automated decision-making and analytics apply across Europe. IoT devices and services tend to collect, share, and store vast amounts of different types of personal data, operate seamlessly and covertly, personalize features based on prior behavior and these standards are being breached. Analysis shows that new approaches to increasing transparency and user awareness are critical to balancing privacy and identifiability and addressing potential discrimination, security, anonymization gaps and informed consent. [10] Rather than promise privacy that is always guaranteed in the IoT, transparency, awareness, and honesty about possible risks, such as about notifications or access rights, is required.

The paper is structured as follows: Section 2 describes the rights of data subjects when it comes to the IoT. Section 3 then reviews if and how transparency is applicable in the IoT. Section 4 explores the tension between user privacy and the connection enabled by IoT identification technologies. Section 5 concludes that future directions of research, design, and business practice must attempt to strike a balance between privacy and identifiability. To minimize the privacy impact of the conflict between data protection principles and identification in the IoT there is an urgent need to further specify and implement several GDPR standards in the design and deployment of IoT technologies.

2. Rights of the Data Subject

Data subjects are provided with rights in regard to their personal data under the GDPR, such as the right to access [11] and the right not to be subjected to automated individual decision-making. [12] These rights are also applicable to organizations using IoT technology. Because IoT technologies process enormous amounts of data, their many sources, and the complexity of analytics, it may be difficult for organizations to comply with this requirement and provide the data subject with all the information about that particular individual.

Transparency can be utilized to hide data when it is decisively uncovered so that it is unfeasible or outside the realm of possibilities for a layperson to filter through. [13] An example is the capacity to recover individual data assembled about an individual user from organizations like Google and Facebook. While this might permit clients to see what data is gathered about them, the information might be too wide and not organized such that they can comprehend. [14] In spite of the way that the GDPR precludes such exercises, as the clarifications in Recital 58 propose, the details leave a ton of room for understanding. With cloud mechanical technology and IoT applications, this issue could turn out to be much more terrible, as the information assembled about a client and their encounters turns out to be more muddled and challenging to unveil. Thus, it is basic to think about the revealed data, yet additionally the work, abilities, and necessities expected to decipher the data. [15]

Right to be Informed and Right of Access

A data controller must notify data subjects about automated decision-making that relies solely on automated processing, such as profiling, that leads to legal or similar effects, due to the GDPR. [16] Considering the possible risks to the rights of data subjects that may arise from profiling it is imperative that data controllers ensure that information about profiling is both available to and brought to the attention of data subjects. [17]

In accordance with articles 13(2) (f) and 14(2) (g) of the GDPR, controllers are required to implement measures to inform individuals about automated decisions, based solely on automated processing, including profiling, that have legal or similar significance.

The data controller is required under Article 15(1) (h) of the GDPR to inform data subjects of solely automated decision making, including profiling, in the same manner as Articles 13(2) (f) and 14(2) (g) of the GDPR. The data controller is required to:

1. inform the data subject that they are engaging in this type of activity;
2. provide meaningful information about the logic involved and;
3. explain the significance and envisaged consequences of the processing.

The A29WP refers to Article 15(1) (h) of the GDPR and points out that a data controller "should provide the data subject with information about the *envisaged consequences* of the processing, rather than an explanation of a *particular* decision." This is further clarified in Recital 63 of the GDPR: "Every data subject should have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing." The A29WP states that "the controller should provide the data subject with general information (notably, on factors taken into account for the decision-making process, and on their respective 'weight' on an aggregate level) which is also useful for him or her to challenge the decision."

The controller is obligated to provide information that is sufficiently comprehensive for the data subject to understand what the reason is for the decision making. The A29WP points out that due to the complexity of machine-learning it could be challenging for data subjects to understand how an automated decision making process works. The A29WP emphasizes that complexity is not an excuse for failing to provide information to data subjects and refers to Recital 58 of the GDPR, which states that “the principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualization be used.” [18] Data controllers should keep in mind that “this is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising.” Therefore, the controller is required to find a simple way to explain the logic involved with automated decision making, such as the rationale behind the decision.

3. Transparency

In recent years, the EU has increasingly advocated that individuals have an effective control over their personal data, which has become a key component of their data protection position and strategy. Recital 7 of the GDPR states that “natural persons should have control of their own personal data” while the current draft of the ePrivacy Regulation [19] refers to natural and legal persons having the right to control their electronic communications. Although the GDPR does not define control specifically, it contains a number of provisions that reinforce controllers' responsibilities regarding transparency and consent. Although interpreting the GDPR requirements is not straightforward, especially in the context of IoT, two guidelines have recently been published by the WP29 on transparency and consent. In addition, the WP29 has published two opinions on IoT development [20] and on the draft ePrivacy Regulation. In terms of transparency, the GDPR introduces requirements concerning acceptable communication formats, as well as categories of information to be provided to data subjects, including identifying information for the controller, the purpose of the processing, the categories of personal data involved, and the recipients of the data. Recital 39 of the GDPR states that “the principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used”. The Guidelines on transparency under Regulation 2016/679 states that “the data controller must take active steps to furnish the information in question to the data subject or to actively direct the data subject to the location of it (e.g. by way of a direct link, use of a QR code, etc.). The data subject must not have to actively search for information covered by these articles amongst other information, such as terms and conditions of use of a website or app.”[21] Additionally, in the Guidelines on transparency under Regulation 2016/679 the WP29 suggests that IoT devices contain QR codes that can be scanned in order to display transparent information. It is questionable, however, if informing data subjects via QR codes or signposting is consistent with the idea, also advanced by WP29, that “the data subject must not have to take active steps to seek the information covered by these articles or to find it amongst other information”. Data subjects should be able to access all required information electronically and without exerting any effort on their part. The fact that IoT devices are by definition electronic objects collecting data from subjects does not preclude their use for “informing” those subjects as well. In order to meet this requirement, the IoT infrastructure will need some adjustments, which are not insurmountable, neither from a technical nor economic standpoint. Additionally, the GDPR also specifies several conditions that constitute valid consent: it must be freely given, specific, informed and unambiguous. As a result of these other conditions, the IoT presents new challenges. For instance, Recital 42 states that “consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment”. The data subject should not be able to turn off their Wi-Fi and, therefore, be deprived of useful services, if there is no alternative to physical tracking in the context of the IoT. To keep consent clear, the GDPR specifies that it must be "given by a clear affirmative act." This does not permit the acquisition of identifiers such as MAC addresses without the consent of the user. Due to the GDPR's requirement to prove that valid consent was obtained, these issues are all the more important for data controllers. For the IoT, the WP29 advocates the design of new consent mechanisms on the devices themselves, such as privacy proxies.

3.1. Implementation of Transparency

One option for implementing transparency and data declaration is to directly connect data collection devices to devices carried by users, for example smartphones. With this option, devices that collect information share their presence, privacy policies and capabilities with a communication channel within the area they operate in. Direct declaration is advantageous in two ways: it reduces the risk of further tracking by a remote entity because the communications are local and it does not require internet access. Direct declaration is usually implemented using wireless technologies like Wi-Fi and Bluetooth, which provide medium and short-range communication. The protocol for these technologies could be extended to include the transmission of privacy policies. Wi-Fi and Bluetooth technologies offer mechanisms for mutual identification and mutual discovery of each other’s services, and the exchange of detailed system information about both technologies. Prior to association the access-point service discovery functionality of Wi-Fi allows stations to discover the access-point by transmitting advertisement frames. Data collectors can use Information Elements to broadcast information such as identifiers and supported capabilities. This could be used by data controllers to announce their presence, the type of data they collect, and their privacy policies. Besides the standard service discovery protocol, Bluetooth also features the advertising packets, which can advertise its presence with a short description. With Bluetooth and Wi-Fi technologies, low-cost solutions could be implemented, as wireless beacons and nano-computers could currently be purchased for around $20 apiece. [22] If the device has a Bluetooth or Wi-Fi interface, this extension is almost cost-free.

Creating a registry for data collection devices could also be an option as a method of establishing transparency. An online registry is a database which stores data collection device information including for example information such as the nature of the data collection device, its range, its privacy policy and any other information required by law. An IoT registry can be accessed from a website or through an application and can offer information in machine-readable and human-readable formats before entering an IoT area.

3.2. Privacy by Design

Privacy by Design should be treated as a requirement rather than as a feature when developing IoT systems. Cavoukian [23] outlines the seven core principles that will guide the implementation of Privacy by Design:

1. Proactive, not Reactive

The proactive strategy prevents privacy invasions from occurring in the first place instead of responding to them after the fact. It is a defensive rather than a proactive approach.

2. Privacy as the Default Setting

Privacy by design is met when a system that activates privacy by default does not require user input to enable privacy. A preliminary step in data collection is to identify the purpose of the collection, to limit the collection to what is necessary, to reduce the acquisition of personally identifiable data, and to control how the data is used, retained and disclosed.

3. Privacy Embedded into Design

In contrast to being an option feature, Privacy by Design is seen as an integral part of a system's basic functionality.

4. Full Functionality

When integrating Privacy by Design, it should not be done at the expense of other features based on the belief that they are impossible to integrate, but rather integrated alongside all needed functionalities, which includes security, with a positive mindset that they can all work together.

5. End-to-End Security

In order to safeguard private data end-to-end from collection to destruction, Privacy by Design should be integrated with data security.

6. Visibility and Transparency

By implementing fair information practices such as accountability, openness and compliance, an IoT system can be guaranteed transparency and visibility for its stakeholders.

7. Respect for User Privacy

As a data controller or service provider, Privacy by Design encourages you to keep individuals' information private by incorporating safeguards such as proper notification, resilient privacy defaults, proper notification and creating comprehensible alternatives, while maintaining a user-centric approach.

4. Privacy as a Property

Under the GDPR pseudonymization is specified as a privacy feature that should be applied to provide an extra layer of protection for personal data in information systems, such as the IoT. Anonymization differs from pseudonymization in that it does not require user consent. The GDPR defines pseudonymization as handling personal data without being able to identify it as belonging to a particular individual.

Pseudonymization and anonymization are both processesed by which identifiable data is transformed so that the user cannot be tracked. The difference between these processes is that once the data has been altered, these procedures cannot be done. It is crucial for data processors to understand when each of these features can be used in IoT scenarios, even though they add a layer of privacy. For example, when it comes to healthcare, making the data impossible to identify may prevent medical service providers from responding to notification of patients because they won't be able to identify the specific patient that needs help. Data breaches, however, may lead to identification of the data subject via other means of identification, so it is important for the data not to be linked back to an individual.

5. Conclusion

As suggested in this paper, the implementation of the measures would contribute to reducing the imbalance of power between data controllers and data subjects without imposing prohibitive costs or unacceptable constraints on data controllers. Despite adopting more ambitious interpretations of the implementation of transparency and consent on some aspects than the WP29, the positions advocated here are consistent with the spirit of the GDPR. For example, the WP29 states that "an appropriate measure for providing transparency information in the case of data controllers who maintain a digital/online presence is to do so through an electronic privacy statement/notice."[24] However, the WP29 considers other forms of communication acceptable, such as "public signage" or "visible boards". There is doubt as to whether such forms of communication would pass the WP29's own efficacy testing. WP29 opinions mention the importance of preventing "user fatigue", another issue alluded to in their opinions, which usually results in situations in which users reluctantly provide consent by reflex clicking. The solution to this issue is to use privacy proxies or privacy agents instead. A privacy agent is defined as a software component that offers two essential functions: a user interface dedicated to the interaction with data subjects, normally so that they can define their privacy preferences and a data manager who controls the release of his personal data according to his choices and the declarations of the data controller. By acting as data subject's privacy agents, they are able to fulfil their preferences without being disruptive or requiring repeated permissions. In its proposals, the WP29 appears to be promoting this approach, however, it is unclear whether the conditions outlined by the WP29 for the validity of consent are consistent with this approach. For example, a WP29 stance stresses that consent should "name controllers". By excluding generic consent based on reference to a purpose, such as counting people in a retail establishment without specifically naming a data controller, it includes a specific form of consent. The suggestions in this paper are also relevant to the ePrivacy Regulation discussions that are currently underway. As mentioned by the WP29, the current draft "gives the impression that organizations may collect information emitted by terminal equipment to track the physical movements of individuals (such as Wi-Fi-tracking or Bluetooth-tracking) without the consent of the individual concerned." [25] Clearly this would be in violation of the GDPR if the text were to be adopted with this wording. It would be all the more unacceptable if, as mentioned earlier in this paper, solutions could be developed to increase information and consent, without imposing excessive restrictions on either the data controller nor the data subject.

Disclaimer

The author wishes to mention explicitly that this paper has nothing to do with her current profession and that she did not write this paper on behalf of the Dutch Data Protection Authority.

References

[1] European Commission, 'Commission Staff Working Document: Advancing the Internet of Things in Europe' (European Commission 2016) SWD (2016) 110 final 31 *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016SC0110&from=EN.*

[2] Gonçalves, F., Macedo, J., João Nicolau, M. and Santos, A. (2013) 'Security Architecture for Mobile E-Health Applications in Medication Control' <*https://repositorium.sdum.uminho.pt/bitstream/1822/26379/1/rfid-e-health-security-v3.pdf*>.

[3] Sicari, S., Rizardi, A., Grieco, L. A. and Coen-Porisini, A. (2015) 'Security, Privacy and Trust in Internet of Things: The Road Ahead', Computer Networks, Vol. 76, pp. 146–64.

[4] Eskens, S. J., (2016) '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?' Social Science Research Network <*https://papers.ssrn.com/abstract=2752010*>.

[5] Barocas, S. and Selbst, A. D. (2016) 'Big Data's Disparate Impact' California Law Review, Vol. 104, pp. 671–732.

[6] Wachter, S. (2017) 'Privacy: Primus Inter Pares — Privacy as a Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rights' Social Science Research Network <*https://papers.ssrn.com/abstract=2903514*>.

[7] Ohm, P. (2010) 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.*

[8] Tene, O. and Polonetsky, J. (2013) 'Big Data for All: Privacy and User Control in the Age of Analytics' Northwestern Journal of Technology and Intellectual Property *http://heinonlinebackup.com/hol-cgi bin/get_pdf.cgi?handle=hein.journals/nwteintp11&section=20.*

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th 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).

[10] Wachter, S. (2018) 'Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR' Computer Law & Security Review <*https://www.sciencedirect.com/science/article/abs/pii/S0267364917303904*>.

[11] GDPR, Article 15.

[12] GDPR, Article 22.

[13] Ananny, M. and Crawford, K. (2018) 'Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability', New Media & Society, p. 973–989.

[14] Curran, D. (2018) 'Are you ready? Here is all the data Facebook and Google have on you', The Guardian <*https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy*>.

[15] Kemper, J. and Kolkman, D. (2018) 'Transparent to whom? No algorithmic accountability without a critical audience', Information, Communication & Society.

[16] GDPR, Articles 13(2) (f) and 14(2) (g).

[17] GDPR, Recital 60.

[18] Article 29 Working Party (A29WP), 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (2017), p. 27. The Article 29 Working Party, which was established by Directive 95/46/EC, has been replaced by the European Data Protection Board (EDPB) on 25 May 2018.

[19] Article 29 Working Party (A29WP), 'Guidelines on consent under Regulation 2016/679', adopted on 4th May, 2020.

[20] Article 29 Working Party (A29WP), 'Opinion 8/2014 on the Recent Developments on the Internet of Things', adopted on 16th September, 2014.

[21] GDPR, Recital 32.

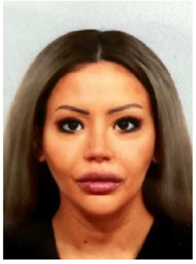
[22] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)', adopted in January 2017.

[23] Cavoukian, A. (2009) 'Privacy by design: The 7 foundational principles', <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>.

[24] Article 29 Working Party (A29WP), 'Guidelines on transparency under Regulation 2016/679', adopted on 29th November, 2017, as last revised and adopted on 11th April, 2018, p. 25.

[25] Article 29 Working Party (A29WP), 'Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)', adopted on 4th April, 2017, p. 18.

Biography



Senna Mougdir is a supervision officer at the Dutch Data Protection Authority. Her work focuses on providing information regarding the protection of personal data and handling data protection complaints.