# Implementing GDPR for Mobile and Ubiquitous Computing

Carlos Bermejo Fernandez
Hong Kong University of Science and Technology
Hong Kong
csbermejo@ust.hk

Tristan Braud
Hong Kong University of Science and Technology
Hong Kong
braudt@ust.hk

Pan Hui
Hong Kong University of Science and Technology, Hong Kong
University of Helsinki
Finland
panhui@ust.hk

## ABSTRACT

The General Data Protection Regulation (GDPR) presents directives to give data subjects control over their personal data. These directives impose data-collecting and processing organizations to take concrete actions for privacy preservation of users and non-users alike. Significant challenges arise when applying these directives to mobile and ubiquitous computing. Mobile and ubiquitous computing aim for computer use to be as transparent and seamless as possible. Inconspicuous devices continually sense their environment, often without the data subject's knowledge. This context significantly complicates the implementation of core GDPR directives, such as informing the user and collecting consent. In this paper, we challenge the mobile computing research community on how to address such issues in practical implementations that combine the philosophy of mobile and ubiquitous computing with often constraining privacy-regulations.

## CCS CONCEPTS

• **Human-centered computing** → **Ubiquitous and mobile computing**; • **Social and professional topics** → **Privacy policies**.

## KEYWORDS

GDPR, Mobile computing, Ubiquitous computing, Pervasive sensing

**ACM Reference Format:**
Carlos Bermejo Fernandez, Tristan Braud, and Pan Hui. 2022. Implementing GDPR for Mobile and Ubiquitous Computing. In *The 23rd International Workshop on Mobile Computing Systems and Applications (HotMobile '22), March 9–10, 2022, Tempe, AZ, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3508396.3512880

## 1 INTRODUCTION

Ubiquitous computing aims to *weave itself into the fabric of everyday life* [49] by deploying a myriad of inconspicuous and highly specialized internet-connected devices. These devices continually collect, analyze, and transmit data on users and their surroundings, often without their knowledge or consent [26]. The European Union's General Data Protection Regulation (GDPR) [35] attempts to regulate data collection and processing. It specifies practical requirements for data collecting entities (*data controllers*) to restitute control of personal data to the concerned individuals (*data subjects*). These requirements include informing the data subjects on their data usage, collecting consent, and providing facilities for users to access, rectify, and erase their data.

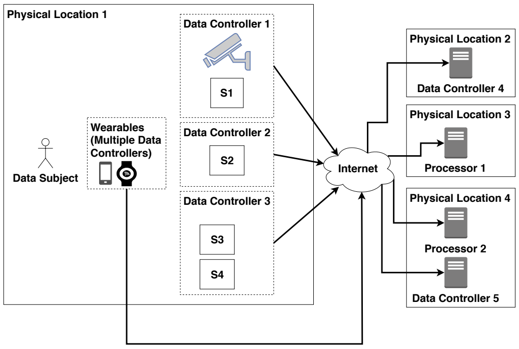

**Figure 1: Typical mobile and ubiquitous computing environment. Multiple sensors sense the data subject and transmit the data to servers in different locations, owned by separate entities. The subject carries sensors that can track him over several locations at all time.**

The GDPR led to significant changes in data-related environments, such as websites and cookie consent notices [4]. However, this example sheds light on one of the fundamental incompatibility of the GDPR with ubiquitous computing. Consent notices impede the user experience by increasing the interaction cost. In ubiquitous computing environments, every increase of the interaction cost becomes highly invasive for the user. Besides the user experience, ubiquitous computing also raises privacy issues that cannot be solved with the traditional privacy frameworks considered by the GDPR. Overall, the lack of generality of the GDPR articles not only complicates compliance by data controllers but also reduces the effectiveness in protecting users' privacy.

In this paper, we dissect the GDPR requirements to assess how to ensure compliance for data collectors in the general scenario represented in Figure 1. A multitude of fixed sensors belonging to several data controllers sense the user within a given physical location. These sensors transmit the data for processing to cloud servers located in different physical locations that potentially belong to different entities (*data processors*). The data subject also carries wearables and mobile devices, which continually sense the data subject and his environment. In this scenario, enforcing the

*HotMobile '22, March 9–10, 2022, Tempe, AZ, USA*

ACM ISBN 978-1-4503-9218-1/22/03…$15.00
https://doi.org/10.1145/3508396.3512880

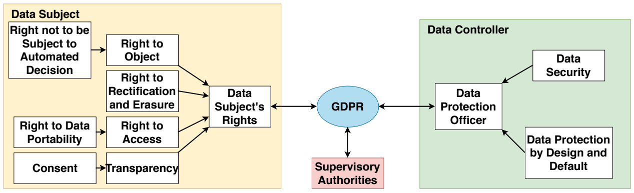

**Figure 2: The GDPR at the interface between data subjects, data collectors, and supervisory authorities.**

data subject's privacy is a challenging task, and the lack of one-size-fits-all solution further complicates the process for data controllers, let alone implementing the GDPR's requirements.

## 2 GDPR OVERVIEW

The GDPR specifies rules related to the protection of personal data and the transfer of data within or outside the European Union (EU). It ensures that data is processed lawfully, fairly, and transparently, for a specific and legitimate purpose, with a focus on data security. This section summarizes the primary components (see Figure 2).

### 2.1 Rights of the Data Subject

**Transparency and Consent**. The GDPR states that the data controller shall inform in a clear and intelligible fashion the data subjects (i.e., identified or identifiable natural person) on how their data is collected and processed. The data subject must **consent** to data collection after being informed.

**Right of Access**. The data controller must enable the data subjects to access their personal data. In the case of automated decision making, the data collector shall provide "meaningful information" on the process and its consequences. The **right to data portability** seconds the right of access. The data controller shall provide machine-readable data for transfer to another data controller.

**Rectification and Erasure**. The data subjects can request the rectification or complete deletion of their information. This "right to be forgotten" extends to when data is no longer necessary, data was collected unlawfully, or data subjects withdraw consent.

**Right to Object**. The data subject has the right to object to the processing of data, especially in case of profiling for marketing purposes or automated decisions (Article 22).

### 2.2 Obligations of the Data Controller

**Controller and Processor**. The controller must ensure that processing follows the regulation. Controllers outside of the EU must appoint a representative within a member states where data subjects are located. The controller remains responsible for the data at all times. It must thus ensure that any external processor meets the GDPR's requirements.

**Data Protection by Design and by Default**. Data protection shall be at the core of the data controller's operation. Besides, the data controller must only collect and process data necessary for the established purpose.

**Records of Processing Activity**. Data controllers and processors have to maintain a record of all processing activities on personal data and should be provided to the supervising authority on request. Such records are mandatory for all companies if the processing is of high-risk nature.

**Data Security**. The GDPR requires data controller to maintain the confidentiality, integrity, and resilience of the data. Data controllers shall thus regularly test and audit the system. In the event of a privacy-threatening breach, the controller must notify the data subjects and the supervising authority.

**Data Protection Officer**. Data controllers must appoint a data protection officer when data processing may impact the data subjects' privacy. This officer is an expert in data protection laws and practices. Her/his role is to advise the data controller, monitor compliance, and act as an interface between the supervising authority and the data controller.

### 2.3 Implications and Consequences

Data collectors must ensure compliance with the GDPR. To this date, the supervising authority has issued more than 900 fines [1]. Most infractions concern data controllers and processors' design principles, architectures, and operational practices [42]. 52% of data collecting companies are concerned they will be subject to a fine, 65% will change their business strategy due to the GDPR, and 30% will increase their budget to implement the new regulations in their business [41]. The following data controller and processors' practices are the most common obstacles to GDPR compliance: storing data forever, reusing data, black markets, data processing risks, hiding data breaches, explainability, and security.

## 3 GDPR IN UBIQUITOUS SYSTEM

Ubiquitous systems collect vast amounts of data that can offer detailed insights about data subjects' behaviour [20]. These systems continuously store, share, and process the data across multi-level architectures (sensor, edge, and cloud), spreading the risk of interception or misuse. Besides such a risk, the linkage of data from multiple sources can lead to detailed inferences on the subjects' private lives (e.g., movement patterns) [20]. For example, cameras can count individuals. However, they tend to collect much personal identifiable information (*PII*) such as appearance, age, facial features as a byproduct. Local protection techniques should thus be applied to obfuscate the collected *PII*. However, other scenarios require preserving such *PIIs*, for instance, smart cameras installed at home to protect against burglars. Complying with the GDPR while preserving utility is a significant challenge in such scenarios.

The GDPR also requires well-identified data controllers and processors [10]. However, the line between both parties is often blurry in ubiquitous computing. Despite having vastly different roles, device manufacturers and third-party developers that manage smart devices both qualify as data controllers. Assessing the role of each party is critical for GDPR compliance, as data controllers and processors have different responsibilities.

**Mobile and ubiquitous computing challenges.** The ubiquity and mobility of pervasive networks challenge the implementation of GDPR regulations [7, 26]. For example, how can we inform data subjects about the vicinity of monitoring devices such as movement sensors used to infer the number of individuals in an area conveniently? In mobile or pervasive environments, data rectification and erasure are even direr issues than in centralized architectures [38]. The protection of data subjects' privacy during the storage, transmission and processing of the collected information can also be difficult due to lack of processing power of smart devices (e.g., sensors) [50], the use of lower power transmission protocols (e.g., LoRa, Zigbee) [13], and the myriad of technologies (standards, languages, databases) used in these scenarios. Examples such as collaborative learning (e.g., federated learning) present privacy-preserving approaches to train/test algorithms without any collection of data in the cloud [44]. Finally, the ubiquitous presence of smart devices reveals new security threats, where the devices can be tampered with or hacked, compromising the privacy and security of data subjects' information [3]. The following sections focus on four core aspects of GDPR in mobile and ubiquitous systems.

## 3.1 Privacy by Design

The GDPR requires the data controller to integrate privacy by design and by default. However, the vast heterogeneity of smart systems complicate the application of the regulation [40]. In [21], the authors propose an abstract system specification technique to facilitate the design and implementation of GDPR-compliant systems. The specifications can be used with major programming languages for high-security environments such as Scala. Privacy-enhancing technologies (*PETs*) that de-identify individuals' data are a common approach to GDPR compliance as the data is not susceptible to re-identification attacks [2]. However, the limited processing capabilities of sensor devices prevents the application of the most sophisticated techniques. The *Databox* [32] project is an initiative to bring control of the collected data to data subjects. The project offers a collection of software and hardware components to manage and protect the personal data collected by other parties. Third parties can still access the data collected by using database queries. Health-related data architectures follow similar approaches to store and process data of patients [37]. Despite providing increased privacy protection and ownership, these approaches may thus be not compliant with the current legal framework.

## 3.2 Consent

The GDPR states that data subjects have the right to control their privacy. Data controllers shall request data subjects' consent and inform them on the data processing policies [31], e.g., the purpose of the processing, categories of personal data involved, and recipients [7]. Most works [8, 9, 31] rely on companion devices such as smartphones or smartwatches to request consent and interact with the systems. The companion devices notify the users of any sensing device in their vicinity. The users can configure their privacy preferences using their smartphones, which are sent back to the sensors (data controllers). These approaches are commonly used in scenarios with smart devices, where the device owner (the data controller) register the device in a centralized system with the location and the sensors (data types). To reduce the users' fatigue responding to consent notices in pervasive environments, the authors in [8] store the different accepted consent notices and the types of collected data, so the system automatically responds to new consent notices with similar types of collected data requests. Similarly, the authors in [9] propose a mobile application (*IoT Assistant*) to discover and control the collection of information of smart devices in the vicinity.

Non-companion device approaches are more challenging. A touch-screen near smart devices can inform individuals about monitoring activities and let them input their preferences [30]. Natural user interfaces [43, 45] can also let individuals to configure their privacy preferences by gesture interactions when the data subjects know the exact location, time, and duration of sensing. Although these solutions address the delicate issue of collecting consent, they do not scale well to ubiquitous computing scenarios. With the multiplication of devices surrounding the users, providing consent can become overwhelming. New solutions to provide "default" privacy preferences or even different virtual entities (virtual face, id) predefined by data subjects [48] to protect individuals' personal information in such scenarios. When multiple individuals can be monitored together in public spaces, the challenges of collecting consent are greater than in traditional scenarios [47]. Different individuals may have different privacy preferences, and each individual's preference may affect neighbouring data subjects.

## 3.3 Transparency

The principle of transparency according to the GDPR requires that the collection and processing of information can be easily accessible and easy to understand in clear and plain language. Service providers are required to inform individuals about their data collection and processing practices. However, these notices are usually long and complicated, contradicting the GDPR's requirement to inform the data subjects in a straightforward and understandable fashion. Several works [17, 28] propose summarization tools to classify and better inform data subjects about the complex and often cumbersome privacy policies involving smart devices and service providers. Authors in [29] propose an SDK that sensitises developers to data disclosure risks and transparency. The SDK includes all the necessary GDPR features and information (into the app) to provide the information end-users require. These techniques help individuals understand the complex and often cumbersome privacy policies involving smart devices and service providers. In summary, there are challenges in informing data subjects about the current privacy policies of service providers and how applications and systems obtain individuals' information without either their consent or awareness.

The GDPR also requires for the algorithms driving privacy-sensitive automated decision to be explainable. The use of profiling algorithms can be discriminatory as subjects are categorized in so-defined groups during the profiling process. As a reflection of our social practices, the collected data to train algorithms thus mirrors any possible trace of inequality or discrimination [15]. Kumar et al. [24] suggest the establishment of a platform for data providers, AI developers and external auditors to improve data and AI transparency. However, automated decision systems present more challenging problems than explainability and interpretability.

## 3.4 Automated Decisions and GDPR

AI/ML and automated decisions have become exponentially important. The enforcement of GDPR in AI-based systems may bring significant changes in their architecture.

#### 3.4.1 *AI and ML.*

The current data volumes create novel opportunities to understand human behaviour through deep learning [46]. If a data subject requests the deletion of his data ('right to be forgotten'), the data collector and processor's systems should delete all data and AI/ML models should be retrained without that data (although not fully defined by the GDPR and technically challenging [6]).

Data collectors and processors are developing *PETs* such as *differential privacy* [11] and federated learning [44] (training local models on users' devices) to protect individuals' personal information during the train/test phases of AI/ML systems. Federate learning approaches can also reduce the complexity in scenarios where the users request the deletion of their information, as the global models do not include any individual's personal information. Ubiquitous scenarios where data does not need to be shared continuously with data collectors can benefit from such techniques. However, it requires local devices to train AI models and store the training data. Although federated learning seems a feasible approach to comply with the GDPR as no individuals' data is shared and memorised by the system, researchers [19] have found that the model's parameters, and therefore the global models, are susceptible to privacy attacks. Therefore, the above methods still require further research to improve their security and privacy. *Zero-knowledge proof* systems [14] use cryptographic algorithms to verify information without disclosing any *PII*. Ubiquitous systems can take advantage of zero proof methods to share the collected data while protecting the *PII*.

#### 3.4.2 *Edge Computing.*

Pervasive computing architectures leverage computing resources at the edge of the network to provide data collecting and processing capabilities closer to users. These approaches raise challenges to ensure data security and privacy protection according to regulations [16, 32] Projects such as *Databox* [32] and *Securebox* [16] use edge computing architectures to provide data subjects with the control of their collected data and securely manage pervasive devices. The data remains closer to the data subject and so does the processing [29] Pervasive application developers should be concerned in their design of edge applications according to GDPR in two areas: (i) transparency and (ii) assessing and appropriately reducing risk [29].

## 4 IMPLEMENTING THE GDPR FOR MOBILE AND UBIQUITOUS SYSTEMS

There is no one-size-fits-all solution for privacy preservation in ubiquitous systems, let alone implementing the GDPR. In this section, we attempt to develop an architectural implementation of the GDPR in the ubiquitous computing scenario described in Section 1. This architecture is inspired by state-of-the art solutions that recentralize data collection to restitute users control over their personal data [16, 32]. However, all these prior works rely on a remote server, complicating their usage in mobility scenarios. Moreover, none of these solutions addresses the issue of collecting consent as is required by the GDPR. In comparison, we specifically target GDPR compliance to enforce the data subjects' rights while simplifying data-related issues for the data controller.

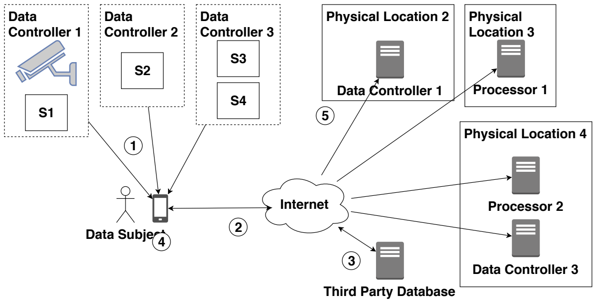

**Figure 3: Smartphone-centric privacy preservation in ubiquitous applications. Sensors no longer communicate the data directly to the processing entity.**

### 4.1 The Smartphone: Interface to Privacy

Smartphones are an intrinsic part of ubiquitous computing. Users keep their smartphone nearby most of the time [36], the device presents multiple interfaces and sensors and is continually connected to the Internet. The increase in computing power together with advances in ML/AI technologies for embedded devices [25] present new opportunities for on-device ML/AI. As such, smartphones are the ideal tool to centralise the user's privacy and implement the GDPR's requirements. In comparison with previous works [9, 16, 32] our solution keeps the identifiable information in data subjects' control while allowing the process of information by data controllers.

*Architecture.* We propose the architecture described in Figure 3. Compared to the original scenario presented in Figure 1, the data flows are recentralized at the data subject's smartphone. The sensors first transmit the data to the smartphone, structured in a machine-readable format (1). The smartphone then queries a third-party database (similarly as in [9]) (2) for more information about the sensor monitoring capabilities. The information includes the type of data collected, its usage, rules available (to protect users' privacy) for that data, and how to read and edit the data (3). Depending on the users' preferences and data type: the smartphone then edits the data (4) and transmits it to the appropriate data collector (5); or transmits the corresponding privacy-enhancing preferences or virtual entity [48] to the data collector (5). The smartphone can retrieve ML models from third-parties databases or the sensor itself to privacy-protect the data transmitted from the sensor. It is possible to combine such an architecture with a distributed ledger in order to keep track of data collection operations publicly and facilitate control by the local supervisory authority.

*Rules.* Users can apply rules to limit the data processor's inference capabilities on the collected data. These rules define the data to transmit for collection and processing, with eventual privacy-preserving modifications. Such rules may include *homomorphic encryption* to protect the information contained in the data, *time-to-live* so the data processor can only use the collected data for a specific period, *de-identification* to remove identifying features [45]. The application of rules on the collected data follows a similar approach to [39], where an abstraction layer called policy-carrying data embedded attribute-based encryption in the shared data. Our system builds on top of the above policy-carrying with de-identification techniques to avoid sharing unnecessary information. For example, users who do not want their face recorded by a smart camera will configure a rule that de-identify the sensors' capture video [18, 34]. In scenarios where the users define a rule to allow the process of a particular type of data for some time, a time-to-live policy will be embedded with the data and shared with the data controller.

When confronted with data collection, the system automatically enforces the existing rules without user intervention and uses a context-based approach to generate rules on the fly (if the data collection follows a suitable ruleset) [33]. Therefore, it does not interrupt the user experience for informing and gathering consent, preserving the philosophy of ubiquitous computing. If the predefined ruleset does not cover a use case, the smartphone issues a notification for the data subject, displaying the consent notice in a standardized way. These rulesets consist of conditional predicates that users can comprehend, configure, and update configure [9, 27, 39]. The set of attributes that users can construct rules using the predicated-based technique can cover various situations and data collection types. Moreover, users can continue updating and refining their rules to accommodate new sensors, different types of data, or new privacy techniques. The system is designed to regain control over users' personal data.

## 4.2 Enforcing the GDPR

This architecture gives the data subjects fine-grained control of the collected data. Moreover, it allows non-users to keep control of their personal data. As such, this system enforces the **transparency** and **consent** requirement, the **right to object**, and the underlying **right not to be subject to automated decisions**. It also simplifies the application of the **right to rectification and erasure**, the **the right to access**, and the **right to data portability** as it directly provides the data in machine-readable form and offers the possibility to edit before transmission. However, dataset-level access and edition require external procedures. On the data collector's side, the system allows for pseudonymization and de-identification at the source, enforcing **data protection by design and by default**. It also provides the first line for **data security** before the data reaches the data controller. By combining this architecture with a distributed ledger such as a blockchain, the system can also address the obligation to **provide records** of data collection and processing.

## 4.3 Challenges

An important challenge facing this system is the agreement of a standard between data controllers, device manufacturers, and app developers required to deploy this solution. The rules will be constructed as policies that all parties, including regulators (e.g., GDPR), should agree on. Due to the additional transmission rounds, real-time applications may experience longer latencies. The data transmission between data collectors and smartphones requires a fast, efficient, and low-power wireless protocol suitable for the collected data bandwidth (e.g., BLE, 6LoWPAN). The data edition process on users' smartphones or edge/sensors requires efficient, accurate, and fast ML/AI algorithms to protect users' private information on sensor data. Deep [25] and federated learning for embedded devices [44] and secure communication protocols [22] can also introduce constraints and incompatibilities with our system regarding speed, efficiency, security, and privacy during the editing phase on the users' smartphone. Our proposed solution can also mitigate the challenges of data deletion ('right to be forgotten'). The smartphones will protect personal information (in suitable situations such as visual privacy) by applying PETs to the data before sending it back to the data controllers. Finally, data processors can use different collected data to infer new information about the data subject, despite our system's privacy-protections, which are still challenging to estimate [23].

Several studies [9, 12] and commercial examples (e.g., Amazon Echo Show (2nd Gen.) includes a slider to cover camera) show that consumers want devices that can be configured to mitigate risks of privacy violations. This can lead to more fine-grained decisions on the trade-off between benefits and privacy risks when users share their data [5, 12].

As we mentioned before, there are existing approaches to provide users' privacy preferences when they do not have a companion device [30, 45]. Our solution could provide similar techniques to allow rules input using gestures or via an external device at the location. In the current form, smartphones are an extension of the user in our proposed system. If it is lost or stolen, the users will have to re-configure their privacy preferences. Although, solutions that rely on edge computing devices or centralized databases [9] would allow users to assign a new device to their profile (with the current configurations in terms of rules). Also, future versions of our system should incorporate additional security measures to prevent device tampering and compromise.

# 5 CONCLUSION

In this paper, we exposed the challenges presented by the GDPR for upcoming mobile and ubiquitous applications. The GDPR requirements contradict not only the ubiquitous computing philosophy of providing a seamless user experience with minimal interaction but also completely disregard some of the technologies behind ubiquitous computing. We proposed a novel architecture for the data subjects to control their personal data while not interrupting the user experience. This architecture addresses the most constraining requirements of the GDPR relative to the pervasive environment sensing and the distribution of processing in multiple locations. Besides, it provides the building blocks for data controllers to further implement other requirements such as the right to access, rectify, and erase personal data. This architecture can provide a new perspective for GDPR-compliant, more generally, privacy-respectful data processing in ubiquitous computing environments.

# 6 ACKNOWLEDGEMENTS

This research has been supported in part by project 16214817 from the Research Grants Council of Hong Kong, and the 5GEAR project (Grant No. 318927) and the FIT project (Grant No. 325570) funded by the Academy of Finland.

## REFERENCES

[1] Privacy Affairs. 2022. GDPR Fines Tracker & Statistics. https://www.privacyaffairs.com/gdpr-fines/. [Online; accessed January-2022].

[2] Mohammad Al-Rubaie and J Morris Chang. 2019. Privacy-preserving machine learning: Threats and solutions. *IEEE Security & Privacy* 17, 2 (2019), 49–58.

[3] Ioannis Andrea, Chrysostomos Chrysostomou, and George Hadjichristofi. 2015. Internet of Things: Security vulnerabilities and challenges. In *2015 IEEE Symposium on Computers and Communication (ISCC)*. IEEE, 180–187.

[4] Carlos Bermejo Fernandez, Dimitris Chatzopoulos, Dimitrios Papadopoulos, and Pan Hui. 2021. This Website Uses Nudging: MTurk Workers' Behaviour on Cookie Consent Notices. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–22.

[5] Carlos Bermejo Fernandez, Lik Hang Lee, Petteri Nurmi, and Pan Hui. 2021. PARA: Privacy Management and Control in Emerging IoT Ecosystems using Augmented Reality. In *Proceedings of the 2021 International Conference on Multimodal Interaction*. 478–486.

[6] Lucas Bourtoule, Varun Chandrasekaran, Christopher Choquette-Choo, Hengrui Jia, Adelin Travers, Baiwu Zhang, David Lie, and Nicolas Papernot. 2019. Machine Unlearning. *arXiv preprint arXiv:1912.03817* (2019).

[7] Claude Castelluccia, Mathieu Cunche, Daniel Le Métayer, and Victor Morel. 2018. Enhancing transparency and consent in the IoT. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 116–119.

[8] Mathieu Cunche, Daniel Le Métayer, and Victor Morel. 2018. A generic information and consent framework for the IoT. *arXiv preprint arXiv:1812.06773* (2018).

[9] Anupam Das, Martin Degeling, Daniel Smullen, and Norman Sadeh. 2018. Personalized privacy assistants for the internet of things: providing users with notice and choice. *IEEE Pervasive Computing* 17, 3 (2018), 35–46.

[10] Eing Kai Timothy Neo Dr. Davide Borelli, Ningxin Xie. 2018. The Internet of Things: Is it just about GDPR? https://www.pwc.co.uk/services/risk/technology-data-analytics/data-protection/insights/the-internet-of-things-is-it-just-about-gdpr.html. [Online; accessed 10-September-2021].

[11] Cynthia Dwork. 2008. Differential privacy: A survey of results. In *International conference on theory and applications of models of computation*. Springer, 1–19.

[12] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

[13] Branden Ghena, Joshua Adkins, Longfei Shangguan, Kyle Jamieson, Philip Levis, and Prabal Dutta. 2019. Challenge: Unlicensed LPWANs Are Not Yet the Path to Ubiquitous Connectivity. In *The 25th Annual International Conference on Mobile Computing and Networking*. 1–12.

[14] Oded Goldreich and Hugo Krawczyk. 1996. On the composition of zero-knowledge proof systems. *SIAM J. Comput.* 25, 1 (1996), 169–192.

[15] Bryce Goodman and Seth Flaxman. 2017. European Union regulations on algorithmic decision-making and a "right to explanation". *AI magazine* 38, 3 (2017), 50–57.

[16] Ibbad Hafeez, Aaron Yi Ding, Lauri Suomalainen, Alexey Kirichenko, and Sasu Tarkoma. 2016. Securebox: Toward safer and smarter IoT networks. In *Proceedings of the 2016 ACM Workshop on Cloud-Assisted Networking*. 55–60.

[17] Hamza Harkous, Kassem Fawaz, Rémi Lebret, Florian Schaub, Kang G Shin, and Karl Aberer. 2018. Polisis: Automated analysis and presentation of privacy policies using deep learning. In *27th {USENIX} security symposium ({USENIX} security 18)*. 531–548.

[18] Rakibul Hasan, Yifang Li, Eman Hassan, Kelly Caine, David J Crandall, Roberto Hoyle, and Apu Kapadia. 2019. Can privacy be satisfying? On improving viewer satisfaction for privacy-enhanced photos using aesthetic transforms. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[19] Briland Hitaj, Giuseppe Ateniese, and Fernando Perez-Cruz. 2017. Deep models under the GAN: information leakage from collaborative deep learning. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 603–618.

[20] Zhiren Huang, Ximan Ling, Pu Wang, Fan Zhang, Yingping Mao, Tao Lin, and Fei-Yue Wang. 2018. Modeling real-time human mobility based on mobile phone and transportation data fusion. *Transportation research part C: emerging technologies* 96 (2018), 251–269.

[21] Florian Kammueller. 2018. Formal modeling and analysis of data protection for GDPR compliance of IoT healthcare systems. In *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, 3319–3324.

[22] Jiawen Kang, Zehui Xiong, Dusit Niyato, Yuze Zou, Yang Zhang, and Mohsen Guizani. 2020. Reliable federated learning for mobile networks. *IEEE Wireless Communications* (2020).

[23] Abhishek Kumar, Tristan Braud, Young D Kwon, and Pan Hui. 2020. Aquilis: Using Contextual Integrity for Privacy Protection on Mobile Devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4, 4 (2020), 1–28.

[24] Abhishek Kumar, Benjamin Finley, Tristan Braud, Sasu Tarkoma, and Pan Hui. 2021. Sketching an AI Marketplace: Tech, Economic, and Regulatory Aspects. *IEEE Access* 9 (2021), 13761–13774.

[25] Nicholas D Lane and Pete Warden. 2018. The deep (learning) transformation of mobile and embedded computing. *Computer* 51, 5 (2018), 12–16.

[26] Marc Langheinrich. 2001. Privacy by design—principles of privacy-aware ubiquitous systems. In *International conference on Ubiquitous Computing*. Springer, 273–291.

[27] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. 2017. Securing augmented reality output. In *2017 IEEE symposium on security and privacy (SP)*. IEEE, 320–337.

[28] Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. 2020. The privacy policy landscape after the GDPR. *Proceedings on Privacy Enhancing Technologies* 2020, 1 (2020), 47–64.

[29] Tom Lodge, Andy Crabtree, and Anthony Brown. 2018. Developing GDPR Compliant Apps for the Edge. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 313–328.

[30] Mateusz Mikusz, Steven Houben, Nigel Davies, Klaus Moessner, and Marc Langheinrich. 2018. Raising awareness of IoT sensor deployments. (2018).

[31] Victor Morel, Mathieu Cunche, and Daniel Le Métayer. 2019. A generic information and consent framework for the IoT. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 366–373.

[32] Richard Mortier, Jianxin Zhao, Jon Crowcroft, Liang Wang, Qi Li, Hamed Haddadi, Yousef Amar, Andy Crabtree, James Colley, Tom Lodge, et al. 2016. Personal data management with the databox: What's inside the box?. In *Proceedings of the 2016 ACM Workshop on Cloud-Assisted Networking*. 49–54.

[33] Katarzyna Olejnik, Italo Dacosta, Joana Soares Machado, Kévin Huguenin, Mohammad Emtiyaz Khan, and Jean-Pierre Hubaux. 2017. Smarper: Context-aware and automatic runtime-permissions for mobile devices. In *Security and Privacy (SP), 2017 IEEE Symposium on*. IEEE, 1058–1076.

[34] Tribhuvanesh Orekondy, Mario Fritz, and Bernt Schiele. 2018. Connecting pixels to privacy and utility: Automatic redaction of private information in images. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 8466–8475.

[35] European Parliament. 2016. General Data Protection Regulation. https://data.europa.eu/eli/reg/2016/679/2016-05-04. [Online; accessed 2-February-2022].

[36] IDC Research. 2013. *Always Connected – How Smartphones And Social Keep Us Engaged*. Technical Report. https://www.nu.nl/files/IDC-FacebookAlwaysConnected(1).pdf [Online; accessed 24-March-2020].

[37] Mouna Rhahla, Takoua Abdellatif, Rabah Attia, and Wassel Berrayana. 2019. A GDPR controller for IoT systems: application to e-health. In *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. IEEE, 170–173.

[38] Subhadeep Sarkar, Jean-Pierre Banatre, Louis Rilling, and Christine Morin. 2018. Towards Enforcement of the EU GDPR: Enabling Data Erasure. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 222–229.

[39] Stefan Saroiu, Alec Wolman, and Sharad Agarwal. 2015. Policy-carrying data: A privacy abstraction for attaching terms of service to mobile data. In *Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications*. 129–134.

[40] Cigdem Sengul. 2017. Privacy, consent and authorization in IoT. In *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)*. IEEE, 319–321.

[41] Junwoo Seo, Kyoungmin Kim, Mookyu Park, Moosung Park, and Kyungho Lee. 2017. An analysis of economic impact on IoT under GDPR. In *2017 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 879–881.

[42] Supreeth Shastri, Melissa Wasserman, and Vijay Chidambaram. 2019. The Seven Sins of Personal-Data Processing Systems under GDPR. In *Proceedings of the 11th USENIX Conference on Hot Topics in Cloud Computing* (Renton, WA, USA) *(HotCloud'19)*. USENIX Association, USA, 1.

[43] Kirill A Shatilov, Dimitris Chatzopoulos, Lik-Hang Lee, and Pan Hui. 2019. Emerging Natural User Interfaces in Mobile Computing: A Bottoms-Up Survey. *arXiv preprint arXiv:1911.04794* (2019).

[44] Reza Shokri and Vitaly Shmatikov. 2015. Privacy-preserving deep learning. In *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*. 1310–1321.

[45] Jiayu Shu, Rui Zheng, and Pan Hui. 2018. Cardea: context-aware visual privacy protection for photo taking and sharing. In *Proceedings of the 9th ACM Multimedia Systems Conference*. 304–315.

[46] Mingcong Song, Kan Zhong, Jiaqi Zhang, Yang Hu, Duo Liu, Weigong Zhang, Jing Wang, and Tao Li. 2018. In-situ ai: Towards autonomous and incremental deep learning for IoT systems. In *2018 IEEE International Symposium on High Performance Computer Architecture (HPCA)*. IEEE, 92–103.

[47] Madiha Tabassum, Jess Kropczynski, Pamela Wisniewski, and Heather Richter Lipford. 2020. Smart home beyond the home: A case for community-based access control. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–12.

[48] Sandra Wachter. 2018. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer law & security review* 34, 3 (2018), 436–449.

[49] Mark Weiser. 1999. The Computer for the 21st Century. *SIGMOBILE Mob. Comput. Commun. Rev.* 3, 3 (July 1999), 3–11.

[50] Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Athanasios V Vasilakos. 2017. Security and privacy for cloud-based IoT: Challenges. *IEEE Communications Magazine* 55, 1 (2017), 26–33.