Article

new media & society
1–21

DOI: 10.1177/1461444820934033
journals.sagepub.com/home/nms

The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment

Sarah Turner, July Galindo Quintero, Simon Turner, Jessica Lis, and Leonie Maria Tanczer
University College London, UK

Abstract

The right to data portability (RtDP), as outlined in the European Union's General Data Protection Regulation (GDPR), enables data subjects to transmit their data from one service to another. This is of particular interest in the evolving Internet of Things (IoT) environment. This research delivers the first empirical analysis detailing the exercisability of the RtDP in the context of consumer IoT devices and the information provided to users about exercising the right. In Study 1, we reviewed 160 privacy policies of IoT producers to understand the level of information provided to a data subject. In Study 2, we tested four widely available IoT systems to examine whether procedures are in place to enable users to exercise the RtDP. Both studies showcase how the RtDP is not yet exercisable in the IoT environment, risking consumers being unable to unlock the long-term benefits of IoT systems.

Keywords

Data portability, data subject rights, European Union, General Data protection Regulation, Internet of Things, regulation

Corresponding author:
Leonie Maria Tanczer, Department of Science, Technology, Engineering and Public Policy (STEaPP), University College London, Shropshire House (4th Floor), Capper Street, London WC1E 6JA, UK.
Email: l.tanczer@ucl.ac.uk

Introduction

In May 2018, the European Union's (EU) General Data Protection Regulation (GDPR) came into force. The regulation provides an 'individual-centric' approach, giving EU citizens more control over their personal data (European Commission, 2012). This approach can be observed through the expansion of data subject rights (ICO, 2017), including the right to data portability (RtDP; Article 20).

The concept of portability is not new, with precursors in telephone number portability, as well as initiatives like *midata* in the United Kingdom (Erkmen and Aydın, 2019). The former allows customers to keep their numbers when changing providers (Sutherland, 2007) with the latter offering means to transmit personal data between UK utilities and other service providers (Buehler et al., 2005). Drawing on a similar premise, the RtDP enables data subjects to port personal data from one service provider to another. This potential has been considered as an avenue to enhance user empowerment and competition (De Hert et al., 2018). Comparable portability requirements have been legislated for in the United States (California), Brazil, Philippines and Australia, or are subject to scrutiny as in the case of India's privacy law bill.

Since the GDPR became operational, only a selected number of studies have inspected the RtDP, with even fewer publications offering empirical examinations. For example, Wong and Henderson (2018) exercised their RtDP against 230 data controllers across various sectors, including social media platforms. Li (2018) explored the conflict between the RtDP and the right to be forgotten (Article 17) and Urquhart et al. (2018) investigated the theoretical application of data portability to the Internet of Things (IoT).

The current article sets out to expand this evidence-base and delivers the first empirical investigation on Article 20's exercisability in the nascent IoT environment. IoT is hereby understood as an umbrella term encompassing the diversity of 'smart' systems with the focus of the current research being centred on household devices, such as smart home assistants or thermostats (Tanczer et al., 2019). To test the RtDP's exercisability, two interrelated studies were conducted. In Study 1, we reviewed 160 privacy policies of IoT vendors whose products are available for purchase in the United Kingdom to understand the level of information offered to data subjects relating to data portability. In Study 2, we tested four widely available IoT systems (two wearable fitness trackers and two smart home assistants) to examine whether procedures are in place to enable users to exercise the RtDP. Together, both studies expose how users will find it challenging to access meaningful information about the RtDP, and impossible to transmit their personal data from one IoT service provider to another.

Data portability

Data portability, as outlined in Article 20 of the GDPR, is defined as the ability for a user 'to obtain her data and to transfer it to, or substitute data stored on, a compatible platform' (Ursic, 2018). Thus, a data subject (i.e. an individual person who can be identified or who is identifiable) can request information from a data controller (i.e. any person or institution that determines the purposes and means for the processing of personal data). Article 20 states that the data should be received in a *structured* (i.e.

data stored in databases and accessible through applications), *commonly used* (i.e. the format of choice must be widely-used and well-established), and *machine-readable* format (i.e. in a format that can be automatically read and processed by computing systems).

Specifically, Article 20 applies whenever (a) personal data processing takes place by automated means, and when (b) data have been provided based on the data subject's consent, or (c) the processing is necessary for the performance of a contract (Hoofnagle et al., 2019). The applicability of the RtDP to data provided by the data subject means that the RtDP is different in scope than the right of access (Article 15). The latter only supports data subjects to obtain a copy of the personal data or supplementary information from the data controller. Article 15 is consequently half a step removed from the RtDP, which would allow a user to then also transmit the data to the next data controller. However, Article 20 does not cover inferences drawn from collected personal data, which the right of access does (Tolmie et al., 2016; Urquhart et al., 2018; WP29, 2016).

The RtDP provides two available procedures for the transmission (and reuse) of data: First, a data subject has the right to transmit data to another controller without hindrance from the original controller to which the personal data have been provided (Article 20(1)). This means that there should be no unjustified legal, technical or financial obstacles that could prevent transmission. Second, a data subject is entitled to request from the original controller the *direct transmission* of available personal data to another controller, where technically feasible (Article 20(2)). In this instance, a user should be able to ask one data controller to 'send' the information they hold of this particular user to the next data controller. Both processes should make it easier to swap providers, for example. See Figure 1 for a graphical representation of the two options.

IoT

A statutory ability to transmit information across several services and platforms seems particularly useful considering the proliferation of so-called 'smart', Internet-connected devices. The move towards IoT implies 'the direct and indirect extension of the Internet into a range of physical objects, devices, and products', with a broad range of applications (Tanczer et al., 2019). These devices and services collect reams of information from their surroundings, including the personal data of individuals in their vicinity. Consumer IoT devices are those created to be used by end-users in a personal capacity or within the home setting. Such devices include, for instance, smart speakers, wearables, and security systems (DCMS, 2018).

Guaranteeing the RtDP in this IoT environment is challenging. IoT devices are not only diverse, but competing vendors collect, store, and process data differently. In particular, technical complexities, such as missing IoT and interoperability standards (Brass et al., 2018), the scale and extent of collected data (Van Deursen et al., 2019), as well as data subjects' lack of awareness of the nature of data processing can hinder the transmission of data across different systems (Jakobi et al., 2019). These aspects make the implementation of the RtDP arduous. Besides, IoT devices are often intentionally designed to be invisible to their users, at the cost of insight as to what the devices do, or what they are capable of (Fritsch et al., 2018). Urquhart et al. (2018) argue that the RtDP may empower

IoT users and 'enable greater literacy around how devices use their data'. This idea makes the exercisability of the RtDP paramount for such educational efforts.

The present research

Given the lack of empirical research on the RtDP in the IoT environment, we set out to determine the ability of a data subject to exercise and to access information about the RtDP as laid out in Article 20 of the GDPR. Specifically, we conducted two studies considering data portability in relation to consumer IoT products available in the United Kingdom. Study 1 is a review study. We undertook an analysis of 160 privacy policies of consumer IoT devices and assessed eight hypotheses as to the availability, content, and information on the RtDP provided to users. Study 2 is an experiment. We zoomed in on four widely used consumer IoT devices and tested whether they allow users to exercise the RtDP's two transmission procedures as outlined in Article 20(1) and Article 20(2). Both studies were approved by the university's Ethics Committee, with their methodology and results summarised in the respective sections below. We end the article with a general discussion and evaluate the insights in light of the current literature, limitations, and future research needs.

Study 1: privacy policy review

To test the availability of information provided to users on the RtDP, we undertook a review of privacy policies offered by IoT vendors. Privacy policies/notices derive from GDPR's obligation of transparency (Article 12–14, GDPR) and describe how a data controller processes personal data (Mulder and Tudorica, 2019). They are essential when it comes to data subjects' 'informational empowerment' and considered to be the primary source of information to enable the exercise of data subjects' rights in the context of online services (Ausloos and Dewitte, 2018). This review tested the hypotheses showcased in Table 1.

Method

Procedure and sampling. We compiled a list of IoT producers, using products featured on amazon.co.uk. Amazon was the fifth largest retailer and most extensive online retailer in the United Kingdom in 2018 (Stevens, 2018). Product listings generated when using the website as a guest (i.e. not logged into an account) were a realistic proxy for the likely exposure a UK-based consumer would have to IoT products on the market.

Search term generation. The search of IoT producers and the list compilation was performed between 22 and 31 May 2019. The search terms to identify product listings were generated in part through a word frequency analysis of academic articles (Ignatow and Mihalcea, 2017). The terms 'Internet of Things AND smart home' and 'Internet of Things AND wearable' were entered into the Web of Science database in May 2019. The terms were chosen in line with the IoT devices being used for the practical experiments throughout this research. The top 50 results (ordered by 'relevance') of each search were

Table 1. Privacy policy review framework.

Hypotheses	Questions
H1. Every producer has a privacy policy that explains their obligations under the GDPR, including the RtDP under Article 20	Is there a privacy policy? Does the policy reference the GDPR? Is the policy linked on the website front page?
H2. The majority of privacy policies (>50%) provide an explicit reference to the right of a data subject to receive their data, under Article 20(1)	Is the information on the RtDP searchable in the policy? What phrase was used to explain the RtDP?
H3. The majority of privacy policies (>50%) provide an explicit reference to the right of a data subject to transmit their data to a separate data controller, under Article 20(1)	Is the information on the RtDP searchable in the policy? What phrase was used to explain the RtDP? Is there any reference to the transmission of data under Article 20(1)?
H4: The majority of privacy policies (>50%) provide an explicit reference to the right of a data subject to request direct transmission of their data to another data controller, under Article 20(2)	Is the information on the RtDP searchable in the policy? What phrase was used to explain the RtDP? Is there any reference to the transmission of data under Article 20(2)?
H5. The majority of privacy policies (>50%) explain the situations under which RtDP can be made (where there is a contractual or consent-based relationship with the data subject), and the type of data that can be returned (data provided by the data subject)	Does the policy make it clear what data a user can expect to receive back (data a user has provided)? Does the policy make it clear under what processing and consent arrangements the RtDP requests must fall?
H6. The majority of privacy policies (>50%) of the sample) explain what 'structured, commonly used, and machine-readable' means in relation to the data that will be returned	Does the policy use the phrase 'structured, commonly used and machine-readable'? Does the policy define (or give reference to definition) of 'structured, commonly used and machine-readable'?
H7. The majority of privacy policies (>50%) give clear guidance as to how to exercise data subject access rights	Is the information on how to exercise data subject rights searchable in the privacy policy? Exercise by button or email (or other)?
H8. The contacts listed within the majority of privacy policies (>50%) are for staff responsible for privacy or data protection, not consumer support staff, as data subject rights are fundamental, not consumer rights	Who owns the exercise procedure (data protection or privacy team or consumer care)?

GDPR: General Data Protection Regulation; RtDP: right to data portability.

consequently downloaded. Of the 100 papers that were identified, six were unavailable for download and three duplicated. As such, 91 individual papers were subjected to the word frequency analysis.

The word frequency analysis using NVIVO Pro 12 returned the 50 most common words among these papers (of five letters or more). Of these 50, the top result was 'smart'. The decision was made to pair up the remaining 49 words with 'smart' (e.g. 'smart

system') and use those pairs to search for the first 100 IoT-based results on amazon.co.uk. Of the 49 words, only nine returned 100 or more results on amazon.co.uk. Besides, as a result of the devices to be used in Study 2, the terms 'home assistant' 'smart watch' and 'fitness tracker' were also added to the search process, meaning the final number of search results was 12: (a) smart systems; (b) smart devices; (c) smart sensor; (d) smart applications; (e) smart security; (f) smart wearable; (g) home assistant; (h) smart watch; (i) fitness tracker; (j) smart cloud; (k) smart health; and (l) smart monitoring;

Duplicates and non-smart products (i.e. products that were listed but were devices that could not be connected to the Internet) were removed from the product lists. This process resulted in the detection of 401 individual IoT producers. The research team conducted Google searches with the keywords 'company name' + 'product being sold on Amazon' (e.g. BleepBleeps children bedside lamp; Mobvoi smart watch). The Google search engine was used as it is the search engine of preference in the United Kingdom with an 87% market share (Statista, 2019). Out of the 401 producers, only 216 had identifiable websites. A full list of all IoT producers analysed for this study as well as the papers analysed for the word frequency analysis can be found in the Supplemental Material.

Review measures. We drew up several questions to be answered when reviewing the privacy policies of each IoT producer which directly linked to the hypotheses listed in Table 1. In some instances, the items fed into the findings of more than one hypothesis – these questions are duplicated in the table. The decision was taken to time-limit each review to 5 minutes, following Boniface et al. (2019). We considered that 5 minutes was the upper-most amount of time a user would be prepared to spend searching for information on the RtDP. We also reduced the acceptability threshold for H2 – H8 to 50% in light of the novelty of the GDPR, the geographical split of the IoT producers (with only 76, or 35%, of producers based in the EU), and the lack of positive results generated in prior research (Ausloos and Dewitte, 2018).

Results

Of the 216 identified IoT producers' websites, 160 (74%) had a privacy policy that was included on the website (H1 reject). When considered by geographical region, 84% of IoT producers with a country of incorporation in the EU together with 92% of those incorporated in the United States, offered privacy policies. In contrast, only 48% of Chinese IoT producers offered a privacy policy on their website. It is also important to emphasise that the analysed IoT data controllers have a dual role whenever a data subject is reading a privacy policy online. In this instance, there is an expectation that the data controller will explain both how their *website* (i.e. how they process any personal data a person provides through the page) and how their *device* works (i.e. how they process personal data provided and collected through the IoT product). Some data controllers amalgamate this information in one document, while others separate privacy policies for different services and systems.

We subsequently reviewed the 160 privacy policies. Of these, only 63 (39%) explicitly referenced data portability within the text. Alternative wording that did not include the word 'portability' was a negative result. Of the 63 privacy policies that referenced

data portability, 42 (67%) mentioned the right under Article 20(1) to receive data back as a data subject (H2 accept). However, in 56 out of the 63 cases, there was only one reference to the word 'portability' or 'port', and this was typically in the inclusion of statements like 'you have a right to data portability', with minimal further explanation. The research team felt that this created a tension between the wording and the intent of H2. Hence, while the inclusion of the term 'portability' was met, its usage without any further explanation does not facilitate the RtDP's exercisability nor its adoption.

Twenty-three (36% of the 63) privacy policies referenced the right of a data subject to transmit the data received to another data controller under Article 20(1) (H3 reject), and 17 (26% of the 63) referenced the direct transmission option as laid out in Article 20(2) (H4 reject). An essential corollary to these two findings: no privacy policies outlined how the data subject should go about approaching the data controller to import their data.

Few privacy policies (16, or 25% of the 63) were explicit in detailing the situations under which data would be subject to data portability. Fewer still explained the circumstances when data portability would apply (just 5, or 8% of the 63; H5 reject). Similarly, while 18 of the policies (29% of the 63) used the phrase 'structured, commonly used and machine-readable', no privacy policy offered or linked to a definition of the RtDP (H6 reject). In policies which provided specific details on the circumstances in which the RtDP can be exercised, it was often found that the text was directly copied from the GDPR. The latter is written in a legal and rather intricate language, infringing on the policies comprehensibility and readability.

Information on how to go about exercising data subject rights, such as whom to contact, was more freely available than specific information on a data subject's RtDP. Of the 160 privacy policies reviewed, 94 (59%) had some reference to how a data subject would exercise their data subject rights. The most popular method of exercising the right referenced was email (80 policies; 85% of the 94 policies), with clickable buttons and forms making up the remainder (14 policies; 15% of the 94 policies; H7 accept). Of those policies that explained how to exercise the right, 55 policies clearly stated that contact should be made with a privacy or data protection employee/team (59% of the 94 policies). Thirty-seven policies stated that requests to exercise data subject rights should be addressed with customer care or support teams (39% of the 94 policies), with two policies saying the right should be addressed to other areas (marketing, or, in one case, to a generic email address; H8 accept).

Discussion

Study 1 reveals that data subjects may expect difficulties to understand the purpose and meaning of the RtDP solely through reading a data controller's privacy policy. Even before starting to look at policies, the researchers found it challenging to determine the producers of several highly ranked devices listed on the Amazon platform, and subsequently, to identify their online presence. Of the 160 analysed privacy policies, barely any explicitly referenced data portability within the text (39%). Of the hypotheses, H3 was rejected, which is unsurprising given the lack of websites that contained privacy policies in general. H2 and H6 posited that more than 50% of privacy policies would have specific types of information relating to the RtDP within their privacy policies. Yet, as less than

39% contained a reference to the RtDP, H2 and H6 were rejected. H7 and H8 estimated that more than 50% of IoT producers would offer guidance and contact information on the RtDP within the privacy policies. As this was the case, both H7 and H8 were accepted.

Study 1 also exposes that a data subject's ability to act upon the information provided in the privacy policies is diminished by the opaque language commonly deployed. This finding echoes Renaud and Shepherd (2018) who critiqued the complex formulations of such notices. Policies also lack specificity. Some privacy policies state that data subjects have rights 'in certain circumstances', or that one 'may be entitled' to exercise the right. Insufficient information about how to contact a person (rather than a department) at a data controller also makes the application of the RtDP harder (Renaud and Shepherd, 2018). The most common means of exercising the right was through email. However, email is known to aggravate a shared understanding of any specific matter (Johnson, 2002).

The current study also shows a lack of information on the transmission process of data from the original data controller to a secondary controller. None of the reviewed privacy policies explain how a data controller would receive and ingest data transmitted to them or facilitate direct transmission to another data controller. As data portability is a novel data protection right, data controllers may lack clarity as to how it should be interpreted and deployed (De Hert et al., 2018). This gap is empirically evidenced in this study and showcases the requirement for stakeholders, such as industry actors or policy officials to agree to potential data transmission mechanisms.

Study 2: device experiment

To further contextualise the findings of Study 1, Study 2 was designed as a first empirical test to identify the ability of a data subject to exercise the RtDP under Article 20(1) and Article 20(2). Article 20(1) enables the data subject to receive earlier provided personal data from an original data controller, so that the *data subject may transmit* the data to a second data controller. Article 20(2) enables the data subject to request the *direct transmission* of provided personal data from an original data controller to a second data controller. We designed an experiment that examined the procedures available to exercise the right under Articles 20(1) and 20(2) on four widely available consumer IoT devices.

Following on from the work of Wong and Henderson (2018, 2019), who performed data portability requests via a standardised email template, the researchers expected that: (a) given the wording of Article 20(1), it would be possible to receive all relevant personal data in a structured, commonly used, machine-readable format, but not to use that data to transmit to a second data controller and (b) given the wording of Article 20(2), it would not be possible to fulfil the direct transmission of data from one data controller to another. The data controllers contacted were made aware during the experimental process that a study was taking place.

Method

Devices. Experiments with four ubiquitous consumer IoT devices were conducted between 6 June and 25 July 2019. Four researchers used a device each (Device 1) and

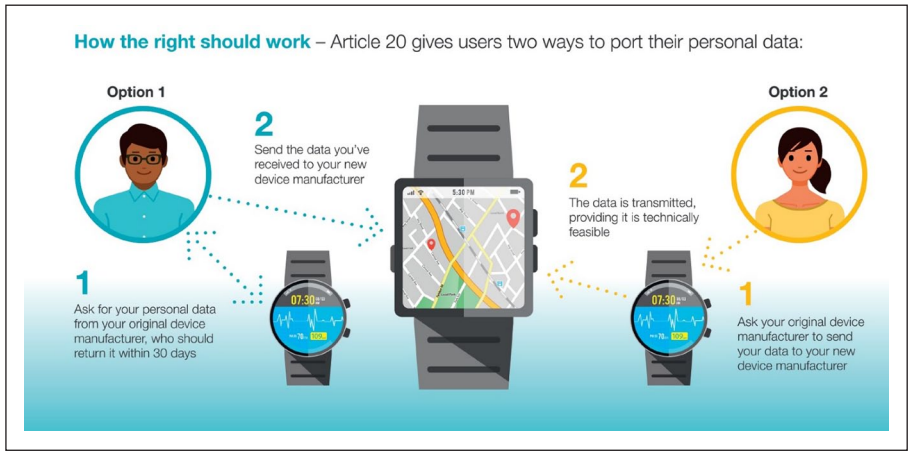

Figure 1. Article 20 exercise options.
Graphic amended from Turner et al. (2019).

attempted to port their data to a secondary device (Device 2). The devices included two wearable fitness trackers (a) Garmin vívosmart 4 (software version 2.90.0.0), (b) Fitbit Charge 3 (firmware version 28.20001.60.39), and two home assistants (c) Amazon Echo (software version 641575220) and (d) Google Home (firmware version 156414). The devices were chosen based on the assumption that they were most likely to be deployed by an average IoT consumer (Tech UK, 2018).

Procedures

Article 20(1). The four devices were used by the research team throughout the course of three weeks. Each of the researchers set up a new account on one of the devices and used it as intended. The period of three weeks provided sufficient time to allow for the collection of personal data, which would form the basis of the Article 20(1) request: first to receive the data provided from the original data controller, and then to transmit the data to the corresponding second data controller (i.e. Garmin to Fitbit, Amazon to Google).

At the end of the 3 weeks, each researcher used the process outlined by the relevant data controller to request and receive their data. This took the form of three automated processes: one instantaneous download tool (Google), two buttons leading to a personalised link being sent to the researcher (Garmin, Fitbit), and one form filled in on the data controller's website, leading to a personalised link being sent to the researcher (Amazon). The researcher downloading Fitbit data also tested the instantaneous download function of a smaller subset of 31 days of specific categories of data. This allowed us to understand whether it was possible to receive provided personal data, without hindrance, to facilitate the transmission step of Article 20(1).

Once each researcher had received the responses from the data controller, the devices were swapped (e.g. the researcher who used the Fitbit exchanged the device for the Garmin and vice versa). New profiles were set up on the exchanged systems. The researchers then requested that their data, received from the original data controller, to be

imported by the second data controller. This process involved emailing the contacts listed in the privacy policies of all four data controllers. However, one data controller (Garmin) had an upload tool available for specific data types. This approach enabled us to understand if the transmission of the provided personal data was possible.

Article 20(2). As with the experiment to exercise the right under Article 20(1), the researchers created their data profiles for 3 weeks on a new IoT device. The intention was to test whether the direct transmission of provided personal data from the original data controller to the second data controller would be technically feasible. At the end of the period, we contacted both the original and second data controllers to express a direct transmission request. This procedure took the form of three email communications (Fitbit, Garmin and Google) and one online form (Amazon).

Results

Article 20(1). The findings derived from each exercise of Article 20(1) were measured against five elements (see Table 2), three of which were taken from the wording of Article 20(1): was it possible to (a) receive provided data in (b) a structured, commonly used, machine-readable format and was it possible to (c) transmit the data to a second data controller? Additional elements were considered: what was the (d) method of communication with the data controllers and was the (e) data received within the limits of 30 days (or an extension sought; as set out in 12.3, GDPR).

While none of the four devices supported requesting data from the associated smartphone apps, all data controllers returned the data in a timely fashion with varying response times. Google was instantaneous, Garmin and Fitbit fulfilled the data request within a week, and Amazon took the full 30 days to respond to the request.

The researcher that downloaded their data from Google discovered that only the basic details, such as email address, name, and location associated with the device were available to download as explicit 'Google Home' data. All activities performed on the IoT device were amalgamated with the researcher's other Google activities (e.g. web searches). The data could consequently not be downloaded as 'Google Home activities', despite them being visible in the accompanying mobile app.

Amazon took 30 days to respond. The reply was titled 'Your Data Access Request' and made no mention of portability, hinting that Amazon saw this process solely in relation to the right to access (Article 15). The email included a link to take the researcher to a page where they could download all the data associated with their Amazon account up to the day the researcher made the request. The data generated between the date of the data portability request and receiving the details from Amazon were not made available, meaning that there was a gap of 30 days.

Google was the only data controller in the study that provided a clear explanation within its download tool as to what data could be expected by the data subject. However, the amalgamated data from all Google products meant it was not possible for a user to download solely their Google Home activity but instead had to filter this information manually. Neither Fitbit nor Garmin provided explanations as to the structure and contents of the data received.

Table 2. Article 20(1) result overview.

Device 1 → Device 2	(a) Received personal data	(b) Structured, commonly used, machine-readable	(c) Import possible	(d) Request method	(e) Timely	Issues encountered
Garmin → Fitbit	Yes	Yes	No	Button	Yes	File/folder structure; lack of explanation of files
Fitbit → Garmin	Yes	Yes	No	Button	Yes	Data within CSV files not structured to be machine-readable
Amazon Echo → Google Home	Yes	n/a	No	Form	Yes	Account exercise requested for not account used in the initial exercise
Google Home → Amazon Echo	Yes	Yes	No	Button	Yes	Home search activity amalgamated with general search activity

CSV: Comma Separated Values.

The data were returned in commonly used, machine-readable formats. Yet, the data were not always structured within the files. There were also differences in how the data were saved and the content's level of complexity. Garmin returned 20 top-level folders which contained further sub-folders, JSON files and 219 FIT files. Amazon's response contained folders entitled 'Audio and Transcripts' and 'Preferences' containing Comma Separated Values (CSV) files or WAV for audio files in no chronological order. Google returned one single JSON file. Fitbit additionally provided access to the latest 31 days of data in a CSV file. Notably, different date formatting was used throughout.

The research showed that it was not possible to transmit data from one data controller to another under Article 20(1). As none of the privacy policies of the four data controllers explicitly outlined the process of importing data under Article 20(1), we sent a request to understand the feasibility of importing the data that had been received by the other data controller. The vendor's data protection team and customer services team confirmed that the import of an individual's data was not currently possible.

Garmin was the only data controller to offer an online import functionality for specific data: through its Garmin Connect web portal, it is possible to upload XLS, XLSX or CSV files of Fitbit 'body or activity data'. No further guidance as to the structure of the files is given, or the format of data that will be successfully imported. In the current instance, the CSV file of Fitbit data was unable to be uploaded to Garmin, with no specific error messages being offered to explain why the failure was occurring.

Article 20(2). The findings for the exercise against Article 20(2) were measured across four elements (see Table 3): (a) does requesting direct transmission from an original data controller take the same form as requesting data under Article 20(1); (b) is the option of a direct transmission mentioned in the privacy policy; (c) upon request, was direct transmission possible from the original data controller; and (d) was the second data controller able to receive a direct transmission.

Across all four tested IoT devices, the direct transmission was never possible, and all four elements (a–d) were not fulfilled. There were no buttons or forms to submit an RtDP request. Similarly, direct transmission of data was not mentioned in any of the data controller's four privacy policies. The responses from customer services for all data controllers said it was not possible to import data directly from one data controller to another. The responses received from data protection teams (Fitbit and Google) highlighted the necessity of a business-to-business transmission of data. Google referenced its ongoing work in *The Data Transfer Project*, which is an open-source initiative that actively looks to facilitate portability between data controllers where appropriate use-cases are present (e.g., sharing photos between platforms). Moreover, Fitbit suggested that the researcher should approach Garmin and lobby for them to work on a direct transmission mechanism using Fitbit's developer platform.

Discussion

Study 2 showcases that data subjects encounter barriers when exercising the RtDP on IoT devices, both under Articles 20(1) and 20(2) of the GDPR. While we received, in three of the four experiments, a copy of the personal data provided to the data controller, it was

Table 3. Article 20(2) result overview.

Device 1 → Device 2	(a) Direct transmission follows same process with Device 1 as receipt of data in Art 20(1)?	(b) Direct transfer mentioned in privacy policy?	(c) Direct transfer technically feasible for Device 1?	(d) Direct transfer technically feasible for Device 2?
Garmin → Fitbit	No	No	No	No
Fitbit → Garmin	No	No	No	No
Amazon Echo → Google Home	No	No	No	No
Google Home → Amazon Echo	No	No	No	No

not possible to transmit that data to a second data controller; neither was it possible to request the direct transmission of data from the original to the second data controller.

Study 2 highlighted that upon request data could be returned to a data subject in commonly used, machine-readable formats. Yet, the received data do not lend itself being transmitted and, thus, is not reusable to other IoT providers of similar nature. For instance, the inability to import the data received from Fitbit into Garmin Connect's upload function exhibits the need for legible data structures that allow portability. This echoes previous research findings, which see the pressing need to agree on interoperability standards that thereupon could allow data portability to work (Wong and Henderson, 2019). Conversely, the demand to make data available in machine-readable formats can stand in the way of making the data potentially legible for users who may struggle to decipher file names and content.

Study 2 also uncovered the difficulty data subjects might encounter in understanding the nature and extent of data they will receive. Three of the four data controllers that returned data (Garmin, Fitbit and Amazon) did not explain the structure of the data provided. This impacts the ability of a data subject to reuse their data. It further contradicts WP29 (2016) requirements, which states that 'it is crucial that the individual is in a position to fully understand the definition, schema and structure of the personal data that could be provided by the data controller'. Without this understanding, reuse and transmission of data become much harder, if not impossible.

The data received because of a portability request may further not correspond to all of the personal data provided by a user. In the case of Google Home, data that are generated through activities is associated with the user's *account* and not to the device. Therefore, data portability requests currently require the user to filter any activity they wish to port. The majority of data that were returned during our experiments was limited to the setting up of a device, restricting the potential to reuse a broader amount of pertinent personal data. Furthermore, although there is an effort from Garmin to ingest Fitbit's data, Study 2 shows that it is not possible for a user to reuse all their data when moving between services. Neither does the RtDP allow for nor do data controllers provide inferential data. The usability of the RtDP consequently lacks in the design of current IoT systems.

The study also pinpoints towards developments that aim to facilitate data portability. For instance, Garmin's Connect upload functionality features the potential for direct transmission under Article 20(2). Fitbit and Google responded to requests for direct transmission by promoting the necessity of a business-to-business exchange as a design feature of any product or service. Due to these gathered responses, we suspect the RtDP will be facilitated where there is a proven business and shared stakeholder interest, which can lead to respective design amendments to be adopted.

General discussion

The present research explored the exercisability of the RtDP in the IoT environment. Explicitly, we set out to study the status quo of data portability as laid out in Article 20 of the GDPR in relation to consumer IoT products available in the UK market. Across two studies, we showcased how the RtDP is not yet actionable and identified limitations to the provision of the RtDP that hinder data subjects' control of their data.

In Study 1, the research team reviewed a total of 160 privacy policies of IoT producers to ascertain the availability of information around the RtDP in these notices. Our analysis revealed that details and instructions regarding the RtDP are minimal. Of those policies reviewed, less than half mention data portability in any capacity. Besides, not a single privacy policy provided information as to how a data controller would handle the import of personal data essential for the completion of the transmission process. This is indicative of the lack of ability that data controllers have to ingest data from other sources on a bilateral basis. It also showcases the difficulty that data subjects have in trying to effect change through exercising the right. It is not possible to use details in a privacy policy alone to understand how a full request under either strand of Article 20 would be executed. In addition, unlike the better-known Article 15, the UK's Information Commissioner (ICO, n.d.) does not provide a data subject with a template letter to exercise the RtDP.

In Study 2, we tested the ability of data subjects to receive their personal data from a data controller and transmit it to a second data controller (under Article 20(1)), as well as to request the direct transmission of personal data from one data controller to another (under Article 20(2)). The results of this experiment determined that while data subjects are able to receive their data from data controllers, typically through the same tools that data controllers have created to manage requests under the right of access (Article 15), they are not always able to do so 'without hindrance'. Furthermore, Study 2 showed an inability for data subjects to exercise either the manual or the direct transmission of personal data as envisaged in Articles 20(1) and 20(2). This implies that there is a gap between the intention and the execution of the RtDP, which demands design interventions to enable the adoption of the right in practice.

Together, both studies expose that the RtDP does not function across the examined IoT systems, adding not only to the existing work by scholars, such as Urquhart et al. (2018) and Wong and Henderson (2018, 2019), but also pointing out fundamental challenges that both industry and regulators have to address. Authors such as Li (2018) and De Hert et al. (2018) have already identified practical roadblocks to the RtDP's implementation, with our findings offering an empirical analysis of the practical challenges data portability faces in the consumer IoT market.

The research shows that reasonable expectations of the RtDP are not met in the status quo. Data subjects face a lack of information as to how to exercise the RtDP as well as what they can expect to receive as a result of having made a data portability request. This lack of information coupled with data subjects lack of awareness of the GDPR (Obar and Oeldorf-Hirsch, 2018) are anticipated to be critical obstacles for the empowerment of IoT users and the realisation of the RtDP as set out by the WP29 (2016). Indeed, an ICO survey shows that only 30% of 2259 surveyed UK citizens knew of the RtDP (Harris Interactive, 2019). This suggests that most citizens do not know or do not believe that they have the right to ask for their data for portability purposes. Together with the low public's perception and expectation of how companies use and treat user data, any unmet rights will only further entrench the public's position on data protection (European Commission, 2019).

In particular, our research uncovers the need to increase the usability of the RtDP, which, in its current implementation, puts a burden on the user. Restricting consumers to emailing IoT producers requires data subjects to be able to articulate not only their

request for data portability but also to be able to clearly explain the types of data that they hope to transmit. The provision of a telephone number or other channels of communication could help minimise such barriers. Besides, design features such as buttons or forms to submit and automate the full execution of data portability requests may help to increase the uptake of the RtDP. Garmin's Connect upload functionality may act as a starting point.

Another vital insight deriving from this research relates to the question of interoperability. The latter describes the ability to exchange data and to make use of this data within the receiving system (Tolk, 2013). As the GDPR refrains from enforcing standardisation and instead encourages industry to develop interoperable formats, a continued emphasis on developing portability use-cases may be needed. Examples of the sectoral approach of other portability frameworks in the United Kingdom (e.g. Open Banking, telephone number portability) or the Australian Consumer Data Right (CDR) Act may consequently be helpful (Meese et al., 2019). Standardisation bodies, such as British Standards Institution or the International Organisation for Standardisation, are therefore urged to make data portability across IoT platforms subject of further developments and discussions. These advances can complement activities of regulatory or quasi-regulatory bodies which can take active roles in ensuring their implementation (Erkmen and Aydın, 2019).

While a gap in any formal standard or regulatory approach exists, efforts to use application programming interfaces (APIs) to facilitate direct transmission between data controllers in specific cases may move towards making the right under Article 20(2) a reality. Previous attempts that draw on APIs include *The Data Portability Project*. Google and Facebook became members of the project in 2008 (Ursic, 2018; van der Auwermeulen, 2017). Similarly, *The Data Transfer Project*, launched in 2018, is an open-source initiative that actively looks to facilitate portability between data controllers where appropriate use cases are present (e.g. sharing photos between platforms; Data Transfer Project, 2018). There is a risk that the reliance upon industry-determined use cases and the dominance of APIs developed by the major technology firms may work to limit the scope of data portability, and increase, rather than diminish, the role and power of large corporations in the process (Qiu, 2017). While similar initiatives in the IoT sector are missing, the here named projects may act as exemplars for IoT producers.

Finally, formal guidance on the applicability of data portability is more than needed. To date, the only official guidance is limited to that proposed by the WP29 (2016). This document, written before the GDPR was implemented, has the limitation of being non-technologically specific. Parties such as the Centre for Information Policy Leadership (2017) have argued that further explanation of, among other things, the responsibilities of the sending and receiving data controllers and the status of shared and third-party data, are required to avoid hindering the effective implementation of the RtDP. As De Hert et al. (2018) signal, until such further direction is given, it is entirely possible that Article 20 could be read in different ways. Furthermore, international legislation (such as California Consumer Privacy Act, Australia's CDR) promote different forms of data portability. Should these varying manifestations of data portability continue to spread, the EU risks that the globally accepted standard of data portability will not be that envisaged in the GDPR.

Limitations

Due to the nature of the research question and project scope, there are some limitations to the research. In Study 1, the examined privacy policies were restricted to the results derived from our keyword search on amazon.co.uk. The research team recognises that there are other IoT producers that may not have been listed on this website but feels confident we have covered some of the most popular IoT consumer devices currently offered on the UK market. Study 2 is based on a limited sample size, using the experience of four researchers only. Besides, three of the four studied IoT vendors are large, US-based companies that hold a significant market share. We were also limited by time. The entire collection and exercise process was conducted over 6 weeks. It is unclear if results would have differed over a longer timeframe and using different providers, but we are confident to have provided a robust and replicable analysis on the intersection of the RtDP and IoT.

Conclusion and further work

The present research explored the status quo of the RtDP versus the text of GDPR's Article 20 in relation to consumer IoT products available in the United Kingdom. Across two studies, we showcased how the RtDP in its current form is neither meaningfully explained to the user, nor is it possible to transmit personal data from one IoT service provider to another. The research, thus, contributes to the identification of limitations of the RtDP that hinder data subject's control of their data and offers one of the first user-centric, empirical investigation of the applicability of current EU data protection rights within the IoT environment.

Further research on the RtDP may choose to examine the exercisability of the implementation of the RtDP not only in consumer IoT devices, but also in more extensive IoT systems. Besides, upcoming studies may carefully analyse portability's relationship to competition law and the security and privacy risks that emerge from the transmission of data between data controllers and subjects. Researchers may thereby draw on our privacy policy review framework and test the RtDP throughout the entire IoT supply chain. Besides, inferential research on interoperability and data exchange standards, both within the EU and globally is critically needed. Such work could provide the offer the needed foundations upon the RtDP can operate.

Overall, we see an apparent demand for further stakeholder involvement to guarantee the RtDP's full realisation as outlined in the GDPR. This, however, seems to be dependent on future developments, such as increased user awareness, regulatory pressures, and industry cooperation. While some users may choose to wait for these changes to occur, the GDPR offers data subjects an avenue to take these matter into their own hands: Article 80 GDPR states that data subjects can mandate NGOs or consumer rights organisations to initiate administrative or judicial actions where there has been a potential infringement of GDPR as a result of non-compliant personal data processing. Should this route be taken, the use of Article 80 could provide an opportunity for the relevant authorities to examine the functioning of the RtDP and its implications to date. This process may be drastic but could serve to finally provide more detailed guidance on the RtDP's exercisability which will help all technology vendor to comply with the spirit of this promising data subject right.

Author's note

Sarah Turner is now affiliated with the University of Kent, UK. All authors have agreed to the submission.

Acknowledgements

The authors are indebted to the Open Rights Group, the PETRAS Internet of Things Research Hub, and UCL STEaPP for their support throughout the research process. Special thanks go to Javier Ruiz Diaz, Ed Johnson-Williams, Janis Wong, Tristan Henderson, Joris van Hoboken, Rene Mahieu, Michael Veale, Lilian Edwards, Gilad Rosner, Huw Jones for their time and input, and all those who participated in the Open Rights Group workshop and who attended any of the research team's presentations. The authors would also like to express their gratitude to the editor and two anonymous referees who kindly reviewed earlier versions of this manuscript and provided valuable suggestions and comments.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The research was supported by the Engineering and Physical Sciences Research Council and partner contributions under grant EP/N02334X/1.

ORCID iD

Leonie Maria Tanczer https://orcid.org/0000-0002-2618-6208

Supplemental material

Supplemental material for this article is available online.

References

Ausloos J and Dewitte P (2018) Shattering one-way mirrors: data subject access rights in practice. *International Data Privacy Law* 8(1): 4–28.

Boniface C, Fouad I, Bielova N, et al. (2019) Security analysis of subject access request procedures: How to authenticate data subjects safely when they request for their data. Annual Privacy Forum 2019, Rome, Italy. Available at: https://hal.inria.fr/hal-02072302/document

Brass I, Tanczer LM, Carr M, et al. (2018) Standardising a moving target: the development and evolution of IoT security standards. In: *Proceedings of the living in the Internet of Things conference 2018*, London, 28–29 March. New York: IEEE. Available at: https://ieeexplore.ieee.org/document/8379711

Buehler S, Dewenter R and Haucap J (2005) Mobile number portability in Europe. *Telecommunications Policy* 30(7): 385–399.

Centre for Information Policy Leadership (2017) Comments by the Centre for Information Policy Leadership on the Article 29 data protection working party's 'guidelines on the right to data portability'. Available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_wp29_data_portability_guidelines_15_february_2017.pdf

Data Transfer Project (2018) White Paper. Available at: https://datatransferproject.dev/dtp-overview.pdf

DCMS (2018) Code of practice for consumer IoT security. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

de Hert P, Papakonstantinou V, Malgieri G, et al. (2018) The right to data portability in the GDPR: towards user-centric interoperability of digital services. *Computer Law and Security Review* 34(2): 193–203.

Erkmen A and Aydın MN (2019) A comparison between right to data portability and United Kingdom's *midata* initiative. In: *Proceedings of the 5th international management information systems conference*, Ankara, 17–19 October.

European Commission (2012) Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. Available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm

European Commission (2019) Special Eurobarometer, a487. Available at: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/86886

Fritsch E, Shklovski I and Douglas-Jones R (2018) Calling for a revolution: an analysis of IoT manifestos. In: *CHI conference on human factors in computing systems 2018*, Montreal, Canada, April. Available at: https://dl.acm.org/citation.cfm?id=3173876

Harris Interactive (2019) Information rights strategic plan: trust and confidence. Available at: https://ico.org.uk/media/about-the-ico/documents/2615515/ico-trust-and-confidence-report-20190626.pdf

Hoofnagle C, van der Sloot B and Zuiderveen Borgesius F (2019) The European Union general data protection regulation: what it is and what it means? *Information & Communications Technology Law* 28(1): 65–98.

ICO (2017) Overview of the general data protection regulation. Available at: https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf

ICO (n.d.) Your right to data portability. Available at: https://ico.org.uk/your-data-matters/your-right-to-data-portability

Ignatow G and Mihalcea R (2017) *Text Mining: A Guidebook for the Social Sciences*. Thousand Oaks, CA: SAGE.

Jakobi T, Patil S, Randall D, et al. (2019) It is about what they could do with the data. *ACM Transactions on Computer-Human Interaction* 26(1): 1–44.

Johnson LK (2002) Does E-mail escalate conflict? *MIT Sloan Management Review* 44(1): 14–15.

Li W (2018) A tale of two rights: exploring the potential conflict between the right to data portability and the right to be forgotten under the general data protection regulation. *International Data Privacy Law* 8(4): 309–317.

Meese J, Jagasia P and Arvanitakis J (2019) Citizen or consumer? Contrasting Australia and Europe's data protection policies. *Internet Policy Review* 8(2): 1–16.

Mulder T and Tudorica M (2019) Privacy policies, cross-border health data and the GDPR. *Information & Communications Technology Law* 28(3): 261–274.

Obar JA and Oeldorf -Hirsch A (2018) The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information Communication and Society* 23(1): 128–147.

Qiu Y (2017) The openness of open application programming interfaces. *Information Communication & Society* 20(11): 1720–1736.

Renaud K and Shepherd LA (2018) How to make privacy policies both GDPR-compliant and usable. In: *Proceedings of the 2018 international conference on cyber situational awareness, data analytics and assessment*, Glasgow, 11–12 June. Available at: https://arxiv.org/abs/1806.06670

Statista (2019) Leading search engines ranked by market share UK. Available at: https://www.statista.com/statistics/280269/market-share-held-by-search-engines-in-the-united-kingdom/

Stevens B (2018) Amazon now 5th largest retailer in UK. *Retail Gazette*, 16 April. Available at: https://www.retailgazette.co.uk/blog/2018/04/amazon-now-5th-largest-retailer-uk/

Sutherland E (2007) Mobile number portability. *Info* 9(4): 10–24.

Tanczer LM, Brass I, Elsden M, et al. (2019) The United Kingdom's emerging Internet of Things (IoT) policy landscape. In: Ellis R and Mohan V (eds) *Rewired: Cybersecurity Governance*. Hoboken: John Wiley & Sons, pp. 37–56.

Tech UK (2018) The state of the connected home: edition two. Available at: https://www.techuk.org/insights/news/item/13914-connected-home-device-ownership-up-but-consumers-remain-sceptical

Tolk A (2013) Interoperability, composability, and their implications for distributed simulation. In: *Proceedings of the 17th international symposium on distributed simulation and real time applications*, Washington, DC, 30 October–1 November. New York: ACM. Available at: https://dl.acm.org/citation.cfm?id=2570870

Tolmie P, Crabtree A, Rodden T, et al. (2016) 'This has to be the cats': personal data legibility in networked sensing systems. In: *Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing*, San Francisco, CA, 27 February–2 March. New York: ACM.

Turner S, Turner S, Galindo J, et al. (2019) *New Device? Looks Nice: But What's Going to Happen to Your Data?* London: University College London. Available at: https://portmydata.github.io/

Urquhart L, Sailaja N and McAuley D (2018) Realising the right to data portability for the domestic Internet of Things. *Personal and Ubiquitous Computing* 22(2): 317–332.

Ursic H (2018) Unfolding the new-born right to data portability: four gateways to data subject control. *SCRIPTed: A Journal of Law, Technology & Society* 15(1): 42–69 .

Van der Auwermeulen B (2017) How to attribute the right to data portability in Europe: comparative analysis of legislations. *Computer Law and Security Review* 33(1): 57–72.

Van Deursen AJAM, van der Zeeuw A, de Boer P, et al. (2019) Digital inequalities in the Internet of Things: differences in attitudes, material access, skills, and usage. *Information Communication and Society*. Epub ahead of print 27 July. DOI: 10.1080/1369118X.2019.1646777.

Wong J and Henderson T (2018) How portable is portable? In: *Proceedings of the 2018 ACM international joint conference and 2018 international symposium on pervasive and ubiquitous computing and wearable computers*, Singapore, 8–12 October. New York: ACM. Available at: https://dl.acm.org/citation.cfm?id=3274152

Wong J and Henderson T (2019) The right to data portability in practice: exploring the implications of the technologically neutral GDPR. *International Data Privacy Law* 9(3): 173–191.

WP29 (2016) Guidelines on the right to data portability. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

Author biographies

Sarah Turner is a PhD Researcher at the School of Computing at the University of Kent, and a member of the Kent Interdisciplinary Research Centre in Cyber Security (KirCCS). She was Research Assistant for the PETRAS Internet of Things Research Hub in 2019 and finished her MPA in Digital Technologies and Policy at University College London in the same year. Her research interests lie in how people live with digital technologies, particularly how individuals manage the privacy and security of smart, Internet-connected devices.

July Galindo Quintero is an independent scholar and consultant. She is a Law and Public Policy professional, with an MPA in Digital Technologies and Policy from University College London, an LL.M from UC Berkeley, and former Research Assistant for the PETRAS Internet of Things Research Hub. Her research covers the intersection of law, policy and emerging technologies, privacy and ethical dilemmas.

Simon Turner is an independent scholar and former MPA Candidate in Digital Technologies and Policy at University College London. He was a Research Assistant for the PETRAS Internet of Things Research Hub in 2019 and finished a Bachelors in 2018. His interests include the intersect of international relations and digital technologies.

Jessica Lis is an analyst focusing on emerging technologies and sustainability. She is a former MPA student at UCL's Department of Science, Technology, Engineering and Public Policy (UCL STEaPP) where her research focused on privacy and technology policy.

Leonie Maria Tanczer is Lecturer in International Security and Emerging Technologies at University College London. She is affiliated with UCL's Academic Centre of Excellence in Cyber Security Research (ACE-CSR), the PETRAS Internet Of Things Research Hub, and the Digital Technologies Policy Laboratory at UCL STEaPP. Her research focuses on questions related to Internet security, specifically smart, Internet-connected devices.