Computer Law & Security Review 52 (2024) 105912

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

In principle vs *in practice*: User, expert and policymaker attitudes towards the right to data portability in the internet of things

Sarah Turner [a], Leonie Maria Tanczer [b,*]

[a] School of Computing, University of Kent, Giles Lane, Canterbury CT2 7TZ, UK
[b] Computer Science, University College London, Gower Street, London WC1E 6BT, UK

ARTICLE INFO

Keywords:
Data Portability
GDPR
Internet of Things, IoT
Data Subject Rights
Data Protection

ABSTRACT

The right to data portability (RtDP) was enshrined in law with the introduction of the EU's General Data Orotection Regulation (GDPR, Article 20) in 2018. RtDP gives a user the right to obtain and transfer their data to a different service, and the data controller the obligation to facilitate this transfer. Since GDPR's implementation, RtDP has been highlighted in the Digital Markets Act (DMA; 2022) and the proposed Data Act. Despite these reinforcements, there are gaps in understanding of RtDP amongst digital service users. Additionally, many organisations struggle to facilitate data transfer, particularly when it comes to the Internet of Things (IoT). This study examines the attitudes towards IoT data portability by conducting semi-structured interviews with users of consumer IoT devices ($n = 28$), academics/industry experts ($n = 11$) and policymakers ($n = 8$). Results indicate that whilst policymakers and consumers value this right *in principle*, it is rendered meaningless without a data subject's ability to exercise it *in practice*. A lack of guidance for data controllers and consumers has created an atmosphere of uncertainty which urgently needs to be addressed.

1. Introduction

Sparked by spiralling technological advancements, the European Union's ("EU") General Data Protection Regulation ("GDPR") (n.d.) came into force in 2018. The regulation offered a comprehensive overhaul of the EU's previous data protection framework, Directive 95/46/EC. It further saw the materialisation of the fundamental rights of privacy and data protection and the consolidation of EU citizens' control over their personal data.[1] This transformation can be observed in the reinforcement of rights that already existed in the previous Directive as well as the introduction of new *data subject right*[2] (n.d.). These latter rights include, amongst others, the right to data portability ("RtDP"; Article 20) (n.d.), which allows data subjects to port their personal data from one service to another (De Hert et al., 2018). Against this legislative backdrop, the proliferation of "smart", Internet-connected devices led to the collecting and processing of new kinds of data. Such connected systems — ranging from smart speakers, vehicles, to health-care appliances — are generally known as the Internet of Things ("IoT"). Tanczer et al. (Tanczer et al., 2019) described them as "the direct and indirect extension of the Internet into a range of physical objects, devices, and products". In particular, consumer IoT appliances are becoming more prevalent and are created to be used by end-users in a personal capacity or within the home setting (n.d.).

In light of the anticipated spike in IoT adoption, the increasing volume and personal nature of the data these systems collate, plus the malleability of this nascent IoT market, a statutory ability to transmit data across smart services seems pertinent. However, applying RtDP to IoT poses several unique challenges. As Zingales [48:4] describes, "IoT is not just a market, a technology or even an industry. IoT is a technological paradigm", which changes how we interface with computing technologies. Consequently, there are technical difficulties in standardising cross-device data transfer, legal issues around intellectual property (n.d.), and societal barriers around the awareness of the smart system's capabilities (van Deursen et al., 2021; Baldini et al., 2018).

Indeed, RtDP's applicability to the burgeoning IoT ecosystem is yet to be closely examined. Since GDPR's implementation, only a selected

* Corresponding author: Leonie Maria Tanczer, University College London, Computer Science, 169 Euston Road, London NW1 2AE, United Kingdom
E-mail address: l.tanczer@ucl.ac.uk (L.M. Tanczer).

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

https://doi.org/10.1016/j.clsr.2023.105912

Available online 3 November 2023

number of studies inspected the legislation's data subject rights, with most publications focusing on the right of access (Article 15) (n.d.). amongst the few analyses scrutinising Article 20, consumers' and other stakeholders' knowledge and perceptions have not been extensively reviewed. Instead, authors such as Wong and Henderson (Wong and Henderson, 2018) attempted to exercise RtDP on data held by 230 data controllers across various sectors, including social media platforms. Urquhart et al. (Urquhart et al., 2018) investigated the theoretical application of data portability to the IoT landscape, and Basaure et al. (Basaure et al., 2020) constructed an agent-based model to investigate how data portability and interoperability in the IoT affected market dynamics.

This paper adds to this literature and aims to understand — through semi-structured interviews — how RtDP is perceived and valued by users, academic and industry experts (henceforth "experts") and policymakers. In doing so, it contributes the first qualitative study into the attitudes towards RtDP in the IoT context. It shows the difficulty of expecting a piece of novel legislation to gain traction where there is poor user awareness, profound gaps of understanding across stakeholders, and significant technical hurdles to overcome. We start with a literature review and continue with an explanation of the methodology and details of the participants. The results are explored using inductive thematic analysis (Braun and Clarke, 2006); recommendations and conclusions follow.

2. Data portability

Data portability, as outlined in Article 20 of GDPR, is defined as the user's ability "to obtain her data and to transfer it to, or substitute data stored on, a compatible platform" (Ursic, 2018; Wong and Henderson, 2019). Specifically, Article 20 applies whenever (a) personal data processing[3] takes place by automated means, (b) data has been provided on the basis of the data subject's consent, or (c) the processing is necessary for the performance of a contract. Article 20 provides two available procedures for the transmission (and reuse) of such data: firstly, a data subject is allowed to *request* and *receive* personal data provided to a data controller[4] in a structured, commonly used and machine-readable format (Article 20(1)); and secondly, 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)).

Since the passing of GDPR, the EU has moved forward with enshrining data portability within other pieces of legislation. The Digital Markets Act imposes portability obligations on those organisations considered large enough to be a "gatekeeper" (Article 2.1) (n.d.).[5] It aims to create a competitive digital economy (Cabral et al., 2021) by placing regulatory pressure on these "gatekeepers" to enable users to switch between competing digital services. The proposed Data Act, presented by the European Commission in February 2022, takes an even more significant step forward. It would guarantee data portability of both personal and non-personal data and aims to "ensure fairness by setting up rules regarding the use of data generated by Internet of Things (IoT) devices" (n.d.). The documentation about the act states that it will include targeted measures to "increase legal certainty" and "prevent abuse of contractual imbalances" around data portability (n.d.). This is an attempt to encourage more small and medium enterprises (SMEs) to "participate in the data economy", and to empower "users to transfer ("port") their data more easily".

Whilst the DMA and the Data Act boost data portability within the EU, no similar proposals exist in the UK. Since the UK's exit from the EU on 31 January 2020, the UK's legislation has preserved EU law as it stood at the date of its withdrawal. The UK, thus, still guarantees RtDP. However, the UK Government published significant policy documentation that signals a departure from the EU stance in the future (n.d.; n.d.). It seems likely that subsequent EU legislation — such as the DMA and the Data Act — will not be reflected in UK legislation. Nonetheless, the impact caused by these laws may see a carry-over effect, as affected organisations frequently strive to comply only with the most stringent requirements.

2.1. Potential impacts of RtDP

As a data subject right, RtDP is understood to benefit users, providing them with means to access, utilise, and move their personal data. It consequently offers consumers novel opportunities and gives them the autonomy and flexibility to choose how their data is being processed. Next to these data subject benefits, it has also been argued that data portability could help spur market competition (Swire and Lagos, 2013). Below, we discuss some potential positive and negative impacts RtDP creates.

2.1.1. User empowerment

Providing consumers with the ability to change services is commonly framed as an empowering right (Castro, 2021). Ursic (Ursic, 2018) sees four advantages for users, including an enhanced understanding of data flows and control of personal data transfers. Furthermore, she argues that such a right could increase the transparency of data processing and allow individuals to manage personal details collated about their lives. It is, however, unclear whether past efforts to facilitate data portability resulted in consumer benefits. For instance, a 2019 report commissioned by the UK's Information Commissioner's Office ("ICO") showed that only 30 % of 2259 UK citizens surveyed knew of RtDP (n.d.). Additionally, Urquhart et al. (Urquhart et al., 2018) critique that the current lack of data legibility could pose a challenge for users, who may feel insecure about their ability to assess the amount, quality, and purpose of their portable data.

2.1.2. Competition

Amongst the earliest studies on this topic, (Zanfir, 2012) describes data portability as a means to link data protection with fair competition. This is echoed by the Article 29 Working Party (n.d.), which perceives the ability to transmit and reuse personal data as a way of avoiding "lock-in" effects (n.d.; Basaure et al., 2020). RtDP may further permit the development of new business models (Günther et al., 2017) and benefit data controllers who can "collect… [personal data that] they did not have before" (Van der Auwermeulen, 2017, 60). Nevertheless, findings by Basaure et al. (Basaure et al., 2020) dampen these expectations. The authors argue that RtDP alone does not foster competition but instead may lead to the consolidation of monopolies. Their agent-based model of different regulatory scenarios suggests that *interoperability* (i.e., the ability to exchange data, and to make use of this data within the receiving system) and *multihoming* (i.e., the ability for a consumer to use multiple IoT platforms and services together) made for the most competitive marketplace (Tolk, 2013). This is echoed by Zingales (n.d.),

[3] Following GDPR Article 4 (2), "processing" should be understood as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

[4] [4]Following GDPR Article 4 (7), "data controller", as applicable to data portability, should be understood as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".

[5] The DMA defines a gatekeeper organisation as one that has a "strong economic position", a "strong intermediation position" and that these positions are "entrenched and durable" within the market (Article 3) (n.d.). In September 2023, the EU Commission announced that six organisations were initially considered gatekeepers: Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft.

who demonstrates that IoT standardisation, plus the facilitation of access to reuse competitors' data for their own benefit, would lead to the most dynamic and innovative market. RtDP, in the format in which it is provided in GDPR, may consequently not be the driving force for competition but reliant on other factors which influence its applicability and effectiveness.

2.1.3. Difficulties and risks for data subjects and controllers

There are concerns about a data subject's inability to keep control of their data when using RtDP. For one, there are risks during the transfer stage. For instance, it is difficult to transmit data securely, particularly where there is no encrypted platform to download data from nor upload data to (Risks and challenges of data access and sharing, in: En- hancing Access to and sharing of data, 2019). For another, there is no agreed-upon procedure for facilitating portability when the right is exercised (Van der Auwermeulen, 2017). Wong and Henderson (Wong and Henderson, 2018) identified a lack of uniformity across the *ways* that data between data controllers and data subjects is shared, as well as the *types* of data consumers receive. A lack of explicit guidance as to *what* and *how* data must be relayed makes RtDP perilous, as sharing this data in insecure ways could lead to data breaches and leaking (Risks and challenges of data access and sharing, in: En- hancing Access to and sharing of data, 2019). Furthermore, the legal requirement to provide data in a standardised machine-readable format is a complex expectation for data controllers. The latter may not have the necessary technical or staffing capacity to guarantee its adequate implementation (Wong and Henderson, 2019). Data subjects are, therefore, left in a position where the data they receive is not human-readable, plus often indigestible by other, seemingly similar devices and services (Turner et al., 2021).

Given all these challenges, coupled with the increasing ubiquity of consumer IoT — which will exacerbate the volume and nature of personal data collected — we decided that work needed to be undertaken to understand how various groups affected by Article 20 understand RtDP's impacts and benefits. As the legislative interest in data portability within the EU increases, our study offers a timely element to assess the value and usability of this right moving forward.

3. Methodology

To analyse how various stakeholders perceive RtDP, semi-structured interviews were undertaken with three different groups: (a) consumer IoT users; (b) academic/industry experts; and (c) policymakers. The grouping reflected the assumption that diverse stakeholders would have distinct opinions as to the meaning and importance of the right. Ethics approval was received from the relevant university committee before the start of the research.

3.1. Participants and sampling

In total, 47 self-selected interviewees participated in the study. All participants were either:

- Users of consumer IoT devices[6] ($n = 28$): non-expert members of the public.
- Experts on an element of data protection or IoT ($n = 11$): academics and industry participants — referred to henceforth as "experts".
- Policymakers ($n = 8$): those involved in the creation, implementation or maintenance of regulation relating to GDPR and/or IoT, and others (such as non-governmental organisation ("NGO") representatives) who work to ensure appropriate policy and legislative decisions.

Demographic details were not recorded throughout the research process. However, further information about experts and policymakers can be found in Table 1. Participants were recruited in a variety of ways, including through referrals, workshop participation, or personal and professional contacts of the research team. The study was further advertised through various offline and online means. The researchers also presented their work at two events (one academic and one industry event) and distributed flyers at the university campus.

3.2. Data collection

Data collection took place between 19 June and 9 August 2019. A semi-structured interview outline underpinned the research (see Appendix A). The outline consisted of a set of standardised opening questions, exploring the interviewee's use or exposure to IoT products and understanding of GDPR and RtDP. Subsequent questions were specialised depending on the sample group interviewees belonged to (i.e., user, expert, policymaker). Additionally, standardised definitions of both RtDP[7] and consumer IoT[8] were provided. These definitions ensured that interviewees had a consistent understanding of the concepts being discussed.

At the start of the interview, participants were encouraged to explain their interactions, concerns, and positive experiences with IoT devices before considering RtDP. This guaranteed that interviewees grounded their reflections in experiences rather than abstractions. Having reviewed the standardised definitions, the three subject groups were offered slightly diverging questions. Users were asked about their own personal experiences and perceptions, while experts and policymakers were asked to reflect on the concerns and benefits of IoT and data portability, both personally and professionally. On average, interviews lasted around 40 minutes.

3.3. Data analysis

The interviews, once completed, were manually transcribed by the research team. They were transcribed verbatim, except for: (a) those gathered in workshop situations ($n = 20$), (b) one instance where the interviewee did not consent to be recorded ($n = 1$), and (c) two instances where responses were provided over email rather than a face-to-face interview ($n = 2$). An inductive thematic analysis approach was applied (Braun and Clarke, 2006). In particular, two researchers independently familiarised themselves with the data, generated initial codes,

Table 1
Overview of Experts/Policymakers.

Internal Participant Reference Code	Category	Area of Expertise
PE3	Expert	Technology Industry
PM5	Policymaker	EU Policy
PM10	Policymaker	EU Policy
PM11	Policymaker	UK Policy
PM12	Policymaker	US Policy/Civil Society
PE13	Expert	Academia
PM14	Policymaker	EU Policy/Civil Society
PE19	Expert	Academia
PE20	Expert	Academia
PE21	Expert	Academia
PE22	Expert	Academia
PE23	Expert	Academia
PM24	Policymaker	UK Policy
PM25	Policymaker	EU Policy
PE26	Expert	Technology Industry

Note. This list provides details of the areas of expertise for experts and policymakers interviewed. Users have been excluded from this table.

[6] For a definition of consumer IoT devices, see (n.d.)

[7] As taken from (n.d.).

[8] As taken from (n.d.).

and searched for themes. All researchers thereupon refined the themes further before creating the analysis.

The following study uses extracts from the interviews. Participants are referred to as P plus interview group (U = user, E = expert, M = policymaker), and an identifying number representing the chronological order in which the interviews were conducted (e.g., PU1). Interviews were facilitated by four members of the research team, but as the role of the interviewer remained the same for all interviews, they are referred to as IV throughout.

Words and phrases in square brackets have been added by the authors to improve clarity or provide missing context.

4. Findings

An element prevalent across all interviews was a sense of *uncertainty* surrounding RtDP. Many interviewees felt there were contradictions between the importance of the right *in principle* and its implementation *in practice*. Users were typically unaware of the right before the interview. Once informed, some could see its value. Although, in line with experts, they had concerns over their ability to carry out RtDP and were cynical that organisations would be able to facilitate any requests they might make. Meanwhile, policymakers recognised that the embedding of a novel piece of regulation would necessarily be slow, requiring guidance and litigation to define the right further. Nearly all interviewees accepted that barriers exist in Article 20′s present application and raised questions about its feasibility. The following section examines the findings from our interviews in three parts: firstly, by discussing how interviewees perceived the right as it was originally intended (*Intentions*); secondly, by looking at current barriers to implementing the right in practice (*Barriers*); and finally, by examining sentiments about who is responsible for improving the execution of the right moving forward (*Improvements*).

4.1. Intentions

The first theme centres on the aim and purpose of RtDP and zooms in on the aspirations underpinning its creation. The three groups — policymakers, experts, and users — differed in their views of the fundamental objective of the right. In particular, the expectations of policymakers conflict with those of users. The former had hoped to create a right that would be of significant value to consumers, whilst the latter struggled to be aware of its existence. The resulting clash leads to contradictory anticipations of *how* and *what* the right could effectively achieve and dissimilar assessments of the rudimentary benefit of Article 20.

For many interviewees, the intent behind the creation of RtDP was split into two perspectives: to protect and assure a fundamental right to privacy or to foster competition in digital industries. Whilst both ideas are not mutually exclusive, interviewed policymakers heavily concentrated on the idea of data protection:

> This is a data subject right, I have the right to get access to my data, if somebody processes it. Full stop: it's a fundamental right. . . it's basically a right to access your data in an interoperable machine-readable form, you can always upload it somewhere else again, and this possibility is only like telling the company to move it directly to another platform. So that was our idea. (*PM5*)

What becomes clear from this quote is the pre-eminence of the user and their needs. For policymakers, the competition element was "ancillary but welcome" (PM25). Still, it would not surpass their ambition to enshrine a fundamental right in the legislation.

Meanwhile, experts indicated that data controllers had a "very strong commercial incentive" (PE24) to facilitate the evolution of RtDP, because of the potential to foster a more competitive market. This viewpoint assumes an economically-driven mindset had steered Article 20′s creation. However, a competitive market is a dual-edged sword: whilst it can be seen as a benefit to "bring in data from other people to your business…", there remains the risk "that you can lose customers quite easily to competitors", meaning that data controllers are "kind of obliged to work harder… [which] obviously has a cost as well" (PE22).

When prompted, users could often not name many of the fundamental rights guaranteed under GDPR nor articulate the legislators' intention. This arose from the fact that, in contrast to the policymaker and expert groups, users were typically uninformed of their data subject rights, with one user describing being "slightly frightened of the fact that I hadn't thought of it as being a right I have. I think it's a reasonable right to have" (PU6).

Instead, they could mainly talk about the legislation in relation to their employment. GDPR would be "something that comes up through various things at work" (PU2), and they would "know Subject Access Request, again, from a professional point of view that we have to… consider" (PU4).

Interestingly, users had spent minimal time thinking of using any of these legal obligations as data subjects themselves: "…in terms of me, I've never thought about making a Subject Access Request to anybody. Mainly just because I don't have any complaints that I can pinpoint on any particular organisation" (PU4). Such comments showcase the lack of familiarity with the prospects these rights enable. It also highlights that users were more likely to think about GDPR in a negative light: either acting defensively in a professional context or needing to use the data in contentious settings. The combination of the two perspectives is problematic for RtDP. If the right is neither understood nor likely to be used in positive situations (i.e., when changing a device), it will unlikely gain traction amongst consumers.

Once users had time to contemplate the opportunities RtDP offered, the majority saw value in the possibility of receiving and transmitting data between data controllers.

> IV: Would you consider —- would you try and expend energy and whatever into moving that information into another device?
>
> PU6: Shamefully, yes, I would —
>
> IV: That's not shameful! That's the entire point!
>
> PU6: I genuinely would try and do that. Yeah.

This recognition of RtDP as being useful was largely acknowledged in the context of social media, emphasised by statements as the following: "…people have so much information on there [Facebook]" (PU7). Interviewees struggled to conceptualise the same benefits in relation to IoT devices they owned: "I think I'm still in the mindset that these [IoT devices] are fluffy toys…I'm not really sure what Alexa would hold that would need to be portable" (PU2). Participants consequently expressed unawareness of the amount and types of data IoT systems harbour, talked about the invisibility of these devices as one "forget[s about] it" (PU4) because they blend seamlessly into the background, and grapple with missing "traditional user interfaces" (PM10). Hence, interviewees fail to see how any of the collated data points may be useful to them: "I'm not sure I've purposely given her [Alexa] a lot of data?" (PU7).

A notable exception to this perspective were smart health devices. Interviewees presented significant interest in using RtDP for health-related products, whether for an "elderly relative" (PU2) or personal use.

> I've got a prime example, where a friend of mine was going for…the perfect year of having all those [fitness] goals met every day. And he was something like 30 days off of having the perfect year when his phone died. And he re-paired his watch to the new phone and all of that data was lost and he was truly heartbroken that he wasn't going to get his perfect year that he'd worked on. (*PU6*)

Such statements indicate that users could be prompted to reassess the intrinsic value of RtDP. Yet, such a change largely hinges on the level of awareness users must — but currently do not seem to — have on either

GDPR or IoT. To achieve this, users ought to understand the various rights offered by the legislation but also appreciate the volume, type, and value of the data they share with data controllers. Overall, the uncovered lack of uniform understanding of RtDP's intentions foreshadows the difficulty of how Article 20 is put into practice.

4.2. Barriers

The second theme centres on the barriers to the effective implementation of RtDP. Whilst the earlier section focused on Article 20's intended use *in principle*, the upcoming section describes how and why those ideas are not applied *in practice*. Interviewees raised a variety of social and technical barriers to the adoption of RtDP, especially in the IoT context. These sociotechnical hurdles stretch from poor levels of digital competence in the wider population to sheer disbelief that organisations would transmit their data if requested.

Additionally, experts recognised the technical challenges of implementing data portability in the heterogeneous IoT environment. These insights hone in on the underlying feeling of uncertainty that surrounds data portability to date.

Despite their general positive sentiments towards RtDP, users were sceptical that they could exercise the right at this moment in time. As one interviewee suggested "…it's a very good initiative…I'm still very doubtful at the moment that it's properly implemented" (PU7). Users, in particular, were unconvinced of the ability and willingness of data controllers to comply with RtDP. This viewpoint is exacerbated by the strict requirement of RtDP that a direct transfer is only required where *technically feasible* and only applies to data processed by automated means. Hence, RtDP does not obligate industry actors to make portability possible. Instead, data portability becomes an option, with technical feasibility being a likely excuse corporations can hide behind.

Data subjects further assumed they would face barriers to exercising RtDP as guaranteed in the regulation. Experts raised that individuals may not have "enough literacy or enough services" (PE16) to exert the right. The average consumer would lack not only the needed knowledge but also the available choices to make use of its benefits. Similarly, users doubted how they would action Article 20 realistically "I actually have no idea who I would email" (PU7). Users also inferred that they could never be certain of how well the transfer process had actually gone: "… how do I know I'm getting the whole lot? Yeah, how do I know it's coming over correctly?" (PU2).

Indeed, research has shown that it can be difficult for consumers to navigate privacy policies. Aspects such as the use of complex language or insufficient information on, for example, how to contact a data controller have been critiqued (Renaud and Shepherd, 2018). In the current study, participants also argued that data subjects may struggle with deploying the correct, legal terminology and face uncertainty about what to expect when contacting a data controller (Turner et al., 2021).

> What I don't think people understand is where do you go with this, to you know, Currys [a UK electronics retailer], or Samsung or something like that. Do I ring customer services and go "I need all the data you've got on me!" And then what happens?…It seems completely unclear…people find contacting customer service challenging…To go to someone with no conception of what to expect from that, I think that's very challenging. (*PM15*)

When supplied with the ICO's RtDP guidance (n.d.), reactions amongst interviewees were split over how valuable it was for educating individuals without prior knowledge of Article 20. This is noteworthy, as the ICO is UK's national data protection authority and increasing awareness of data subject rights — such as RtDP — is one of its core objectives (n.d.). The overall feeling towards the ICO's guidance were summed up well by PE20, who questioned the document's intelligibility:

> Well, as often I would say, with the ICO information, particularly if I compare it to the information provided by other Data Protection Authorities, it's relatively more useful and clearly written. Often what they write is clearly more clear, written down [than] the law itself. And in most cases, as far as I can see, also correct…But I think for I don't know, whose target group but just an average citizen who thinks like, oh, let's find out what about what are my rights? I think this is still pretty daunting. And they might still think like, so what? (*PE20*)

The ICO's RtDP guidance is hosted on their website. The relevant webpage contains a downloadable link to a generic complaint letter (n.d.). The template makes no reference to Article 20 nor any of the legal obligations associated with it. Instead, it is a template that can be used whenever a person has any sort of concern about the way an organisation handled their personal data. When we showed interviewees this written draft, many considered its non-specific content as bewildering:

> IV: …if you were to go about exercising the right, how would you do it?
>
> PU6: Not with the [ICO] letter in there!

We asked interviewees for their assessment, as the ICO is known to provide pre-drafted letters on several topics. For instance, as part of their advice page on Subject Access Requests (Article 15), the ICO supplies a clearly applicable template which data subjects can appropriate for their personal use when contacting data controllers to request their data (n.d.). However, as of October 2023, the ICO continues to provide no similar letter for exercising Article 20. This means that since we conducted our interviews back in 2019, no relevant amendments and updates occurred.

Next to these practical barriers, several experts talked about technical challenges that prohibit the implementation of RtDP. Notably, the direct transmission of data (under Article 20(2)) was highlighted as uncertain. One expert accentuated the "modularity" (PE23) of IoT: a single IoT system comprises perception, network, and application layers (Mahmoud et al., 2015), all of which are a "mix and match" (PE23) of components, each made by separate manufacturers. The heterogeneity of these systems oftentimes implies non-standard data processing (Mahmoud et al., 2015). This diversity leads to complications in the ability to transmit data seamlessly between products or services.

> This is where we've been struggling because we haven't had a common ontology. Sometimes we have a common syntax, but we don't have common semantics between different service providers that they essentially map that the data in a particular way. And then from when on an ontology, a data ontology perspective, structure it in a particular way. So that's why it's not always possible to transfer it easily from one device. (*PE19*)

Furthermore, users and experts stressed that there could be hazards in implementing RtDP in an insecure way. As one interviewee commented, RtDP may be "a requirement [that] actually increases the data protection risks that could occur" (PE13). For instance, an organisation's inability to provide a safe mechanism to download and transfer one's data could cause unauthorised parties to gain access to sensitive, personal information. Yet, building out sufficiently secure infrastructure may be onerous for some manufacturers.

In sum, the second theme revealed the breadth of challenges that impede the adequate enactment of RtDP. These obstacles include a lack of digital literacy, regulatory guidance, and technical standards to translate the opportunities offered by Article 20 into reality. In particular, consumers' insufficient digital skills create a frustrating loop where users' inability to recognise and, thus, exercise the right, removes the incentive for organisations to search for technical solutions, and in turn, may lead to data protection breaches caused by patchy, insecure RtDP implementations. These tensions are heightened in the IoT environment, where far more nuanced and granular data is collated, and data protection risks are consequently intensified.

4.3. Improvements

The third and final theme centres on *where* and *with whom* the responsibility must lie for resolving the above-outlined barriers and contradictions between RtDP's intent *in principle* and its actual implementation and adoption *in practice*. Interviewees see the requirement for data subjects to act as catalysts for a successful RtDP implementation as problematic, yet vital to attain traction with manufacturers. Experts pushed the burden to regulators by underlining the necessity of gaining more formal guidance on the technicalities of Article 20. Conceptual clarity, according to them, would allow manufacturers to move forward with its realisation. Still, policymakers viewed industry actors as being in charge of developing RtDP and should aim to improve standardisation and data interoperability.

The consensus amongst experts was that RtDP must not result in a burden for data subjects. Instead, consumers should experience ease when moving data from one data controller to another, evidenced in quotes such as the following:

> I think that the desired outcomes should not be that individuals should have the responsibility to gather this data in a machine-readable format and themselves trying to transfer it to another service provider or another device. (*PE19*)

However, imbalances between the authority and dominance of industry stakeholders could subdue the rights and needs of average consumers. As one expert reasoned, the "power differential" (PE20) between data subjects and data controllers could never gain sufficient traction if left to the consumer's responsibility. As it stands, data subjects do not have enough leverage to make a data controller provide data under RtDP. Indeed, previous studies have shown (Wong and Henderson, 2018; Turner et al., 2021) that if a data controller does not respond to a data portability request, or considers the request technically infeasible, a data subject has very little recourse.

Policymakers were less concerned with these asymmetries but agreed that there was a need for further guidance about implementing GDPR, especially for specific technologies such as IoT products. These instructions should, nonetheless, come from data protection authorities — such as the ICO — and be developed based on "case law" (PM15), as one participant indicates:

> It's a very general law, and also very technology neutral. So that's why we need the guidance from guidelines from the data protection authorities, which already are there in many cases – maybe not in terms of data portability, then of course the end, for specific cases, it will be up to the courts to really spell out in detail what it means in specific cases, but that's normal for any law. (*PM5*)

Most interviewees also agreed that the future success of RtDP would require industry collaboration. As one policymaker suggested, "it will depend upon the manufacturers" (PM5) to implement Article 20. They inferred that this demand for industry intervention would align with GDPR's original intention. However, such sentiments only go so far. Considering manufacturers have not yet voluntarily spent time, money, and personnel on the practical realisation of Article 20, it is likely organisations must eventually be mandated to make RtDP effectively work.

The call for industry collaboration also involved an appeal for better standardisation. Standards are commonly understood as "an agreed way of doing something…the distilled wisdom of people with expertise… that help drive innovation" (n.d.). Across all interviews, experts and policymakers accepted that these processes would be driven by the tech sector. Experts also reflected upon lessons learned from Open Banking and telephone number portability: "I think that's actually a big lesson for the success of data portability in the future" (PE24).

Future work could take the form of formal data standards which would underpin interoperable frameworks required for data exchanges. Application Programming Interfaces (APIs; i.e., cloud-based interfaces that can be used to develop software which links in with data provided by another company) were also considered to be useful by some experts "to make it really practical for anybody" (PE3). Creating these APIs open source (i.e., a term used by developers to refer to non-proprietary software for which the code is freely and publicly available) could resolve issues with power imbalances between established corporations and SMEs since anyone could use them without reliance on a third party. Nevertheless, the issue with open source development is that it is "piecemeal" (workshop participant). Thus, it relies on the interest of developers to take it forward.

Whilst most interviewees tended to agree that industry would play a large role in standardisation, experts were concerned by the lack of specific regulatory guidance. They said that "…further guidance and possible better clarification" (PE32) is necessary, as its absence poses a risk to both data subjects and data controllers. A lack of direction pushes data controllers into inertia until there is certainty as "the ROI [return on investment] isn't high enough" (PE3) to attempt to be a first mover in the field. Besides, "…the manufacturer of the device…may be out of the EU…and may not hold any of the data. Uh, so what are the obligations when it comes to a structure like that?" (PE16).

Policymakers also raised the difference in capacity, funds, and legal expertise between large technology corporations and SMEs. "Large companies have the means to implement [RtDP], but that may not be the case for SMEs, and that is a risk" (PM10). This was echoed by expert participants: "I think it's very difficult for smaller data controllers to actually implement interoperability. And so, and it might result in a disadvantage if the authorities pursue that track forever" (PE13). More than 99 % of private sector businesses in the UK are SMEs with less than 250 employees (n.d.).

Evidently, this theme reiterates the sense of uncertainty surrounding RtDP, which prevailed in the analysis. The ongoing tensions between the right's intention and ultimate execution became obvious in light of the inconsistent expectations on the role and responsibilities of users, policymakers, and industry actors. Whilst most interviewees agreed that the private sector has a considerable duty, numerous users and experts felt businesses could not be left alone in this process. Undoubtedly, the tech sector must be supported by appropriate guidance and the establishment of case law, which, over the last years of GDPR's existence, seems to have gone amiss.

5. Discussion

This study indicates that RtDP is bogged down in contradictions — between the value and intentions of the right *in principle* and the implementation and usability of the right *in practice*. Uncertainties — caused by factors such as a lack of digital literacy, inadequate regulatory guidance as well as missing technical standards — underpin the current adaption of Article 20. Across three themes, we examined IoT users, academics/industry experts, and policymakers' attitudes towards RtDP in consumer IoT. We highlighted different perspectives and gaps in understanding of the aim and purpose of Article 20 (*Intentions*), considered barriers to the effective implementation of data portability (*Barriers*), and uncovered varying viewpoints on who should bear responsibility for resolving RtDP's ambiguities moving forward (*Improvements*).

Throughout our interviews, users presented an alarming lack of awareness of GDPR's data subjects rights and confusion about how RtDP would apply in the IoT context. This confusion is only exacerbated by the specificity of the data covered by RtDP (i.e., only data processed by automated means), a nuance that even an interviewed policy official failed to acknowledge (see the quote from PM5 in Section 4.1). Policymakers underlined the value of RtDP as a fundamental right and placed responsibility for implementing Article 20 on industry stakeholders and developing case law. Academic and industry experts argued that technical challenges, such as the absence of guaranteed interoperability, stand in the way of facilitating RtDP for IoT. These differing viewpoints

exhibit tensions in the expectations and understanding of the RtDP that must be addressed. Whilst disagreements in the interpretation of a novel piece of legislation are not unusual, we want to use the upcoming section to discuss these points in turn: firstly, issues around data subjects' awareness of RtDP; secondly, possible improvements to Article 20's regulatory guidance; and thirdly, technical challenges inherent in requiring data transmission between IoT devices. We end by examining how the portability provisions in the DMA and the proposed Data Act may address these problems.

5.1. Data subject awareness

Across our research, interviewed users showcased a lack of awareness on two fronts: on the one hand, they struggled to conceptualise the emerging IoT environment. This is evidenced by consumers not knowing *what* data IoT devices collect nor being able to envision *why* this information is valuable and might warrant reuse. Insights like this echo findings from past studies, which revealed how consumers hold skewed perceptions around the way smart, Internet-connected systems operate (Abdi et al., 2019). Incomplete mental models about IoT devices' data processing, learning, and storage lead to a "neglect [of data] protection" (Williams et al., 2017): 9]. This, in turn, results in users not having enough information to assess their trust in these products and the respective vendors, which interviewees frequently alluded to.

On the other hand, users also grappled with simply *knowing* about their data subject rights whilst failing to perceive them as something meaningful and positive. As the interview quotes display, users primarily encounter GDPR in their employment and in moments of contestation and dispute. This unfavourable attitude stands in the way of RtDP being viewed as a fundamental right or — alternatively — a means to increase competition. Whatever perspective users, policymakers, or experts take, average consumers of IoT products and services can and should benefit from RtDP in some form or another. However, as of now, the here-uncovered insufficient understanding of the regulation and its Articles stand in the way of data subjects experiencing any of the possible advantages that this legislation created.

Together, the combination of these factors — in particular, the expressed lack of interest in one's data plus the felt indifference towards data protection — illustrate why reservations towards RtDP may be sustained. There is a gap in understanding the potential benefits of RtDP exhibited by users that prevents them from expecting, advocating, and even envisioning it as part of their normal long-term IoT usage. More public information and awareness-raising campaigns that frame RtDP along the lines of a consumer right could hereby be pragmatic. However, such a framing will counteract the ambitions policymakers had initially upheld for data portability (i.e., as a fundamental right) in the first place.

5.2. Regulatory guidance

As a novel data subject right, RtDP is in urgent demand of further guidance for all parties affected. The uncertainties and tensions explored in this paper arise because no one party – whether users, manufacturers, or policymakers – seems to have a reason to break from the status quo and work toward active adoption. Further guidance might help break this deadlock, by providing advice on how to exercise, execute — and once actually used — possibly even complain about Article 20. As experts pointed out, there is no first-mover advantage in technically implementing RtDP. Besides, these efforts will most likely be driven by big players, rather than smaller corporations. In the absence of industry interest in making RtDP workable, bodies such as the ICO must be prompted to step in. Best practice examples of what *good* may look like for manufacturers are essential and could encourage them to boost data subject's understanding of what benefits RtDP provides. Similar practices have been offered for other data subject rights, such as the ICO's detailed explanation and letter for the exercising of Article 15 (Kim et al., 2017). Indeed, if offering details on how to standardise data remains too complex, expectations around minimum security considerations when sharing data with data subjects form a reasonable start.

Moreover, legal precedents must be set. Judicial decisions on this topic will act as a means to showcase to businesses that companies will be held accountable. In fact, such case law may help to stifle the practice of prohibiting users from exerting Article 20 — especially under the disguise of a lack of technical feasibility (Turner et al., 2021). Again, regulators such as the ICO are here important. Yet, consumer rights organisations such as Which? in the UK or BEUC at the EU level, plus international digital rights advocacy groups, may drive these efforts.

5.3. Technical challenges

Undoubtedly, technical complexities and a lack of apparent return on investment make data portability a difficult thing to prioritise for organisations, which becomes a further problem when trying to overcome differences of understanding about what RtDP can, and should, achieve. This is particularly true for IoT manufacturers, given the heterogeneity of available devices (Mahmoud et al., 2015). As many interviewees stressed, exchanging data in standardised formats is unlikely to happen without significant industry-led efforts. A move towards shared protocols within the IoT sector is needed. Besides, standardisation may serve as a key means of evidence compliance with regulatory and legal obligations (Piasecki et al., 2021). That being said, direct data transmission is something that not all firms have the capacity nor appetite to build — especially securely (Swire and Lagos, 2013). This argument is often made for SMEs. Yet, it also applies to firms that introduced Internet-connectivity into existing product ranges (e.g., vendors that historically produce "offline" appliances). In this instance, a manufacturer's primary interest or expertise may sit in software development. This explains why such vendors could have limited in-house capabilities to implement or aspirations to drive data portability work (Urquhart et al., 2018). Open source APIs, such as those offered by the Data Transfer Project (n.d.), present a partial solution. Indeed, APIs have been considered in other EU Directives as a possible fix for problems arising from interoperability (De Hert et al., 2018). However, since APIs are built for specific use cases, they are unlikely to facilitate the holistic and universal application of RtDP as envisaged by Article 20.

Expert participants in the study suggested that one of the reasons RtDP may fail is a lack of impetus, given the insufficient technical guidance that GDPR provides; another key immediate reason for the tension of what may be required of manufacturers and what they may understand is possible. Recital 68[9] states the ideal outcomes of RtDP from a data subject's perspective. Although not normative, it suggests that focusing on the data subject's control of their data should encourage the tech sector to create interoperable and standardised data formats. Such uniformity has already been central to other portability efforts, including EU directives around telephone number portability (De Hert et al., 2018) and Open Banking (n.d.; n.d.). Open Banking arose from an overarching goal to provide bank account holders with the ability to switch between banks quickly and easily. A long and arduous process in the UK, beset with similar tensions and misunderstandings of the type explored here in relation to RtDP, the first step was an agreement over what data types and features would need to become interoperable. This was followed by each organisation building the required technology to ingest the agreed-upon interoperable data sets.

Interoperability can further be achieved through different forms of standardisation (De Hert et al., 2018). At one end of the spectrum, formal industry standards can set out clear requirements for implementing specific technological prerequisites. This may benefit from creating "new paths" for smaller or catch-up firms to follow (Kim et al., 2017, 1234). Nonetheless, formal industry standards — unless

[9] A recital within EU law sets out reasons behind sections of the enacted law or regulation.

mandated by a regulatory body — are voluntary in the initial phases. Hence, they rely upon "market adoption" (PE19). Furthermore, the idea of a single standard across all aspects of IoT is "naïve" (PM10) given the diversity of products. Standards for specific IoT sectors may, therefore, be more realistic and may serve as a key step in providing the type of data fluidity across systems that RtDP intends to encourage, as well as a way of evidencing compliance with the article's requirements (Piasecki et al., 2021).

Indeed, there has been some movement to improve interoperability within specific sectors of the consumer IoT market. Since 2019, the Connected Standards Alliance has published a connectivity standard and data model, along with other elements of standardised tools and controls (n.d.). Although this industry collaboration has been described as improving *connectivity* between IoT devices manufactured by different companies, it does not — at this stage — promote the exchange between various IoT vendors, which is necessary for full implementation and the reduction of uncovered uncertainties and misunderstandings around RtDP.

5.4. Where to now for RtDP?

Since the interviews were undertaken, the status quo of RtDP has not changed. However, the EU is taking further strides to regulate the digital world. This can be seen in the DMA and the proposed Data Act. The latter moves closer towards requiring IoT portability [21, Recital 31] and is intended to give users (whether natural or legal persons) more control over the use of their data.[10] Of particular interest for the present study, the Data Act builds on Article 20′s conception of RtDP. It extends the scope to non-personal data (although inferred data remains out of scope) with requirements for providing continuous, real-time data where applicable (where this may be applicable is not defined). It will also require compliance with open standards and interfaces, which will boost interoperability. Unlike the GDPR, the Data Act contains provisions within the text for the Commission to state which standards should be used (n.d.).

Whilst these developments sound positive, initial analyses of the proposed Data Act have been critical. As with GDPR's data subject rights, *in principle* the Act has the potential to be extremely powerful. However, *in practice,* it remains to be seen how the issues RtDP faces today will be addressed, and whether any changes will serve to address the tensions created by a right that neither users, manufacturers, nor policymakers seem to know how to push forward to practical use (Leistner and Antoine, 2022). In particular, the level of control that the Act envisages users to hold — namely, that they can decide *which* data can be shared or ported, and which must not — requires a level of regulatory and technical sophistication far removed from the current state of capabilities (Kerber, 2022). As such, it remains to be seen what the Data Act's impact may be — should it eventually be adopted in its current form.

6. Limitations

The current work is subject to a number of limitations: firstly, interviews were conducted in 2019. Although the ability for consumers to exercise RtDP under Article 20 has not materially changed since then, proposed amendments in the DMA and the Data Act should make the concept of data portability more widespread; secondly, since the interviews were undertaken, consumer IoT devices have become considerably more prevalent. Whilst this does not necessarily translate into users being more aware of their data subject rights, they may be more conscious of how smart devices work and how they integrate into their homes.

[10] User is the term used to describe both natural and legal persons using the product/service and providing the data to the product/service in the Data Act.

7. Conclusion

The present study examined users, experts, and policymakers' attitudes towards RtDP when applied to IoT. All interviewed groups highlighted contradictions between the intent and actual implementation of Article 20. This discrepancy between RtDP's purpose and feasibility pinpoints towards an inherent uncertainty around its significance and ultimate benefits. The findings have thrown up many fundamental questions that policy officials, as well as industry actors, must address to overcome the gaps in understanding, as shown in the interviews undertaken for this research. Particularly, the rise and malleability of the smart consumer market can hereby act as a useful incentive and speed up case law and technical advancements. It is therefore hoped that future legislative developments — including the DMA and Data Act — will result in improvements to portability by providing clearer requirements for manufacturers, even if the burden may remain on users. As authors, we are hopeful that this research may act as an impetus, which in the long run may make RtDP not only valuable *in principle* — but also *in practice*.

Funding

This research was supported by the UK Engineering and Physical Sciences Research Council and partner contributions under grant EP/N02334X/1 (Title: PETRAS Partnership Research Fund; PRF 2019). At the time of submission, Dr Leonie Maria Tanczer's salary was supported by a variety of research grants, includingMR/W009692/1 (UKRI FLF), MR/VO49879/1 (VISION), and ES/S004424/1 (VAMHN).

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that has been used is confidential.

Acknowledgements

This article and the research behind it would not have been possible without the contributions of July Galindo Quintero, Simon Turner, and Jessica Lis. They were part of the original research team that helped conduct this study as part of their "MPA Group Project" at UCL's Department for Science, Technology, Engineering and Public Policy (STEaPP). Their efforts on setting the foundation for this paper cannot go amiss. The authors are also indebted to the Open Rights Group and the PETRAS National Centre of Excellence for IoT Systems Cybersecurity for their support throughout the research process. Special thanks also 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 feedback and input, Lilly Neubauer for her editorial support on earlier paper drafts, and all those who participated in the Open Rights Group workshop. The authors would also like to express their gratitude to the editors and two anonymous referees who provided valuable suggestions on the initial manuscript.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.clsr.2023.105912.

References

Abdi N, Ramokapane KM, Such JM. More than smart speakers: security and privacy perceptions of smart home personal assistants. In: Proceedings of the Fifteenth USENIX Conference on Usable Privacy721 and Security. USENIX Association; 2019.

Article 29 Data Protection Working Party, 2017. Guidelines on the right to "data portability". Technical Report. https://ec.europa.eu/newsroom/article29/items/611233.

Baldini G, Botterman M, Neisse R, Tallacchini M. Ethical design in the internet of things. Sci Eng Ethics 2018;24.

Basaure A, Vesselkov A, Toyli J. Internet of things (IOT) platform competition: consumer switching versus provider multihoming. Technovation 2020;90.

Braun V, Clarke V. Using thematic analysis in psychology. Qual Res Psychol 2006;3.

BSI, 2021. What is a standard? Technical Report. https://www.bsigroup.com/en-GB/standards/Information-about-standards/what-is-a-standard/.

Cabral L, Haucap J, Parker G, Petropoulos G, Valletti TM, Van Alstyne MW. The eu digital markets act: a report from a panel of economic experts. Luxembourg: Publications Office of the European Union; 2021.

Castro D. Improving consumer welfare with data portability. Technical Report Info Technol Innov Found. 2021.

Chaib, I., 2018. How to regulate open banking. Technical Report. Open Bank Project.

Connectivity Standards Alliance, 2022. Connectivity standards alliance - technologies and solutions. Technical Report. https://csa-Iot.org/all-solutions/.

De Hert P, Papakonstantinou V, Malgieri G, Beslay L, Sanchez I. The right to data portability in the GDPR: towards user-centric interoperability of digital services. Comp Law Security Rev 2018;34.

Data Transfer Project, 2022. About us: data transfer project. https://datatransferproject.dev.

Deloitte, 2022. Deloitte digital consumer trends, UK edition, April - May 2022. Technical Report. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/technology-media-telecommunications/deloitte-uk-digital-consumer-trends-2022-device-usage.pdf.

Department for Business, Energy and Industrial Strategy, 2021. Business population estimates for the UK and regions 2021: statistical release. https://www.gov.uk/government/statistics/business-population-estimates-2021/business-population-estimates-for-the-uk-and-regions2021-statistical-release-html.

Department for Digital, Culture, Media and Sport 2018. code of practice for consumer IoT security https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachmentdata/file/773867/CodeofPracticeforConsumerIoTSecurityOctober2018.pdf.

Department for Digital, Media, Culture and Sport, UK Government, 2020. National data strategy. https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy.

Department for Science, Innovation and Technology, 2023. Data protection and digital information (No. 2) bill. https://bills.parliament.uk/bills/3430.

Digital Markets Act, 2022. Regulation (EU) 2022/1925 of the european parliament and of the council of 14 september 2022 on contestable and fair markets in the digital sector and amending directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

EU Data Act, 2022. Proposal for a regulation of the European Parliament and of the council on harmonised rules on fair access to and use of data (Data Act). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068.Com/2022/68final.

General Data Protection Regulation, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council (vol 59. pp 1–88).

Günther WA, Mehrizi MHR, Huysman M, Feldberg F. Debating big data: a literature review on realizing value from big data. The J Strategic Info Sys 2017;26.

Harris Interactive, 2019. Information rights strategic plan: trust and confidence. Technical Report. ICO.

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

ICO, 2022a. ICO25 Strategic Plan: objective one: safeguard and empower people. Technical Report. https://ico.org.uk/about-the-ico/our-nformation/our-strategies-and-plans/ico25-strategic-plan/how-we-will-know-if-we-have-achieved-our-objectives/1-safeguard-and-empower-people/.

ICO, 2022b. Your right to data portability. Technical *Re* port. https://ico.org.uk/for-the-public/your-right-to-data-portability/.

ICO, 2023. Preparing and submitting your subject access request. Technical Report. https://ico.org.uk/for-the-public/your-right-to-get-copies-of-your-data/preparing-and-submitting-your-subject-access-request/.

Kerber W. Governance of IoT Data: why the eu data act will not fulfill its objectives. GRUR International 2022:72.

Kim Dh, Lee H, Kwak J. Standards as a driving force that influences emerging technological trajectories in the converging world of the internet and things: an investigation of the m2m/iot patent net- work. Res Policy 2017;46.

Leistner M, Antoine L. Attention, here comes the eu data act! a critical in-depth analysis of the commission's 2022 proposal. JIPITEC 2022;13.

Mahmoud R, Yousuf T, Aloul F, Zualkernan I. Internet of things (IoT) security: current status, challenges and prospective measures. In: 2015 10th international conference for internet technology and secured transactions (ICITST). IEEE; 2015.

OECD. Risks and challenges of data access and sharing, in: En- hancing Access to and sharing of data. Organisation for Economic Co- operation and Development; 2019. chapter 5.

Open Data Institute, Fingleton, 2019. Open Banking, Preparing for lift off. Technical Report. URL: https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf.

Piasecki S, Urquhart L, McAuley D. Defence against the dark artefacts: smart home cybercrimes and cybersecurity standards. Comp Law Security Rev 2021;42.

Renaud K, Shepherd LA. How to make privacy policies both GDPR-compliant and usable. In: 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). IEEE; 2018.

Savova, D., 2022. The Data Act: a proposed new frame- workfor data access and porting within the EU. https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2022/03/the-data-act–a-proposed-new-framework-for-data-access-and-porti.html.

Swire P, Lagos Y. Why the right to data portability likely reduces consumer welfare: antitrust and privacy critique. Maryland Law Rev 2013;72.

Tanczer L, Brass I, Elsden M, Carr M, Blackstock JJ. The United Kingdom's emerging internet of things (IoT) policy landscape.(2019). In: Ellis R, Mohan & V, editors. The united kingdom's emerging internet of things (IoT) policy landscape. Rewired: Cybersecurity Governance; 2019.

Tolk A. Interoperability, composability, and their implications for distributed simulation: towards mathematical foundations of simulation interoperability. In: 2013 IEEE/ACM 17th International Symposium on Distributed Simulation and Real Time Applications. IEEE; 2013.

Turner S, Quintero JG, Turner S, Lis J, Tanczer LM. The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment. New Media Society 2021:23.

Urquhart L, Sailaja N, McAuley D. Realising the right to data portability for the domestic Internet of things. Pers Ubiquitous Comput 2018;22.

Ursic H. Unfolding the new-born right to data portability: four gateways to data subject control. SCRIPT-ed 2018:15.

Van der Auwermeulen B. How to attribute the right to data portability in Europe: a comparative analysis of legislations. Comp Law Security Rev 2017;33.

van Deursen AJAM, van der Zeeuw A, de Boer P, Jansen G, van Rompay T. Digital inequalities in the internet of things: differences in attitudes, material access, skills, and usage. Info, Comm Soc 2021:24.

Williams M, Nurse JR, Creese S. Privacy is the boring bit: user perceptions and behaviour in the internet-of-things. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST). IEEE; 2017.

Wong J, Henderson T. How portable is portable? Exercising the GDPR's right to data portability. In: Proceedings of the 2018 ACM international joint conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers; 2018.

Wong J, Henderson T. The right to data portability in practice: exploring the implications of the technologically neutral GDPR. Internat Data Privacy Law 2019;9.

Zanfir G. The right to data portability in the context of the EU data protection reform. Internatl Data Privacy Law 2012;2.

Zingales, N., 2015. Of coffee pods, videogames, and missed interoperability: reflections for EU governance of the internet of things.