Journal of the Midwest Association for Information Systems (JMWAIS)

Volume 2020
Issue 2 *Special Issue - Information Security, Privacy, and Ethics*

Article 4

2020

Advancing Technological State-of-the-Art for GDPR Compliance: Considering Technology Solutions for Data Protection Issues in the Sharing Economy

Gail L. Maunula
University of Turku, gaimau@utu.fi

Recommended Citation

Maunula, Gail L. (2020) "Advancing Technological State-of-the-Art for GDPR Compliance: Considering Technology Solutions for Data Protection Issues in the Sharing Economy," *Journal of the Midwest Association for Information Systems (JMWAIS)*: Vol. 2020 : Iss. 2 , Article 4.
DOI: 10.17705/3jmwa.000060
Available at: https://aisel.aisnet.org/jmwais/vol2020/iss2/4

Journal of the Midwest Association for Information Systems

Volume 2020 | Issue 2 Article 4

Date: 07-31-2020

Advancing Technological State-of-the-Art for GDPR Compliance: Considering Technology Solutions for Data Protection Issues in the Sharing Economy

Gail L. Maunula
University of Turku, gaimau@utu.fi

Abstract

Technology provides solutions that help create and drive growth in the Sharing Economy (SE). From the initial technologies that transformed the age-old practice of sharing into a digital disruption of traditional industries, to mobile-app technology delivering streamlined functionality to users, technology has paved the way. As the business model develops, it is no wonder the SE looks to developers to technologically capitalize on new trends and solve emerging challenges. One such challenge is the need to secure data and comply with data protection laws, such as the EU's General Data Protection Regulation (GDPR). The ongoing struggle to achieve and maintain compliance under the GDPR keeps companies reanalyzing business practices. Often, new compliance gaps emerge, as demonstrated in this research, wherein analysis of SE processing activities uncovers potential privacy, security and data protection concerns related to the platform's disclosure of personal data to end-users. This article invites those from tech fields into the inner workings of theoretical legal research, fostering a symbiotic relationship between the law, technology and industry. This research acknowledges that the path to GDPR compliance meanders through the fields of technology, and juxtaposes this reality with the results of close scrutiny of SE data processing practices to suggest future research paths.

Keywords: General Data Protection Regulation, Sharing Economy, personal data protection, legal compliance, service provider obligations

DOI: 10.17705/3jmwa.000060

1. Introduction

Personal data is at the heart of Sharing Economy (SE) business models. The growth and success of the industry are closely tied to the ability to collect copious amounts of personal data and extract the greatest value from them (Richter, 2019). Personal data allow users, facilitated by Sharing Economy Platforms (SEPs), to gain the trust needed to break down the walls of information asymmetry and non-familiarity that comes with the absence of face-to-face transactions (Seigneur, 2009). Were it not for these personal data, it would be difficult to garner the trust necessary to encourage these consumer-to-consumer interactions (Lutz et al. 2017) that predominantly involve access to physical goods and services (Dakhlia et al. 2016).

However, these personal data would be of little value without the supportive technologies that allow SEPs to collect, store and extract their value. These technologies engender the capabilities needed to fully capitalize on the benefits of personal data (Madsen 1992; Cohen and Kietzman 2014). The SE is not only built on these technological capabilities (Einav et al. 2016), but also driven by the development of new tech tools that extend these capabilities (Krivenchuk and Smutny 2019).

But technology goes a step beyond offering data capture, extraction and analysis capabilities. These technologies form the data privacy and security structures that help SEPs meet legal compliance obligations for the protection of personal data (GDPR Report). Despite the notion that technology challenges the protection of personal data (Seigneur 2009) and exacerbates the struggle to create effective data protection legal regimes (Weiner 2004), both the SE industry and data protection regulators look to technology to meet the demands of compliance, thereby looking to the exact infrastructures that create certain challenges to simultaneously solve those challenges (Room et al. 2018).

When the valuable personal data disseminated through SE transactions originate from users within the European Union (EU), the General Data Protection Regulation (GDPR) is triggered. Personal data protection under the GDPR is achieved by giving data subjects control over their personal data through a set of individual rights (GDPR, Articles 12-21) and imposing fines and penalties for non-compliance (GDPR, Article 84). The GDPR protects the personal data of those considered European data subjects in the hands of an enterprise, regardless of its location. Casting a wide net, this territorial scope places any business offering goods and services or monitoring the behavior of EU data subjects under the GDPR's purview (GDPR, Article 3).

In 2016, the GDPR entered into force as a direct response to technological developments, from the fields of information technology (IT) and information and communications technology (ICT), that challenge the privacy and security of personal data (van den Hoven et al. 2019). Many business enterprises across the globe, including popular SEPs, scrambled to achieve compliance before the GDPR applicability date of 25 May 2018, and many still struggle to achieve compliance (Irwin 2019). Indeed, balancing the affordances of available security and privacy technologies and the quest to achieve profitability (Flavián and Guinalíu 2006) is a constant process. Nevertheless, the GDPR acknowledges that modern technology is a vital pathway to data protection (Tankard 2016).

Two years on, however, there is a need for further research that focuses less on the initial compliance momentum and more on the compliance trajectory. For technology to meet the future compliance needs of any data-driven industry, it is incumbent upon legal researchers to communicate the deeper implications of the GDPR. To date, multidisciplinary research related to data privacy and security technologies, the SE industry and the GDPR focuses on meeting these initial compliance challenges (Urban et al. 2018; Lutz et al. 2017; GDPR Report 2017). These studies presume a platform positioning under the GDPR served by the present industry interpretation of the flow of data during an SE transaction and the requisite legal obligations under this interpretation. However, we are at a stage where researcher attention can be directed toward more detailed scrutiny and interpretation of implications of the GDPR in the SE. As this research shows, a GDPR-focused reinterpretation of this data flow signals the need for tools that effectively protect and secure data beyond the digital platform.

This article investigates a development at the intersection of SE business models, supportive privacy and security technologies and GDPR compliance. More directly, the article analyzes the flow of personal data inherent to SE transactions that results in a weakness in personal data protection for some end-users that may trigger a GDPR response. This data protection weakness arises when SE personal data provided to the SEP is disclosed to its service providers. Personal data disclosure to service providers is integral to the SE business model, so it is not a new function. What is new, is the analysis of weaknesses in data protection that closer scrutiny of this practice reveals and the potential obligations of service providers under the GDPR. This paper signals to tech industries that they should ready themselves for a significant shift in how SEP functions may evolve upon answering these legal questions regarding disclosure of data to service providers and offer an opportunity for technological development from

the perspective of data protection legal requirements (Room et al. 2018). The goal of this combination of theoretical legal research and practical research is to engage tech developers in the early stages of this legal discovery, to identify those technologies that will, once again, bridge the gaps toward compliance.

Following this Introduction, Section 2 explores the nature and handling of personal data in the SE and juxtaposes the industry's data processing realities with the stringent compliance demands of the GDPR. Section 2 offers a concrete example of a data privacy and security scenario that reveals the extension of data protection obligations to service providers. The Section also illuminates two critical data compliance red flags and frames the solution around the position, influence, and technological capabilities of the SEP. Section 3 analyzes the role that technology does and could play in support of the data protection compliance efforts of SE data processors, and considers the way forward for technology development in light of revelations discussed throughout this text. The paper culminates with a Conclusion and Considerations for Future Research that acknowledges the integral part privacy and security-enhancing technologies will play in achieving data protection legal compliance for the SE and other industries that similarly handle personal data. Combined, these elements provide novel research intended to spark future ICT research and achieve the data protection goals envisioned by the GDPR.

2. Sharing Economy Personal Data and its Protection

With modern technology, SEPs open a global forum for sharing that would be nearly impossible in the analog world (Codagnone and Martens 2016). SEPs leverage this technology to encourage and facilitate exchanges between individuals with an abundance of a resource, with those in temporary need of that resource (Horton and Zeckhauser 2016). The SE has social, environmental and economic benefits that have propelled its popularity, growing the industry rapidly since its emergence in 2008 (Kim et al. 2015; Heinrichs, 2013; Botsman and Rogers 2010). Already in 2015, 44% of US adults were familiar with the SE, with 25% utilizing the SE as a consumer or provider (Consumer Intelligence Series 2015). Additionally, revenues from the SE are expected to grow from $15 billion in 2015, to $335 billion in 2025 (Hawksworth and Vaughn 2014).

SEPs seek to facilitate the efficient connection between two end-user groups: service providers (offering services or resources) and end-consumers (utilizing services or resources). Both end-user groups are consumers of the SEP, which provides the technical and social infrastructure used to form their consumer-to-consumer (C2C) relationship (see Figure1). The formation of this triangular relationship requires intimate personal data (Teubner and Flath 2019) that fosters the trust necessary to conclude a transaction that occurs, in part, outside the auspices of the digital space. This unique conglomeration of digital- and physical-world contact heightens the need for reliable technical tools that collect and utilize the appropriate types and amounts of data to facilitate safe transactions efficiently.

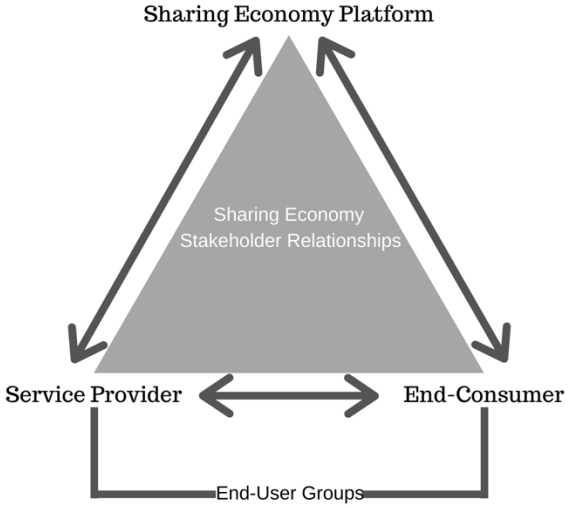

Figure 1. Sharing Economy Stakeholder Relationships

The choice to engage with a particular service provider, or the choice to offer your goods or services to a particular end-consumer, are decisions made after scrutinizing platform provided personal data collected from each user. Personal data under the GDPR is "any information relating to an identified or identifiable natural person" (GDPR, Article 4(1)).

This broad definition of personal data captures much of the data individuals provide in order to engage on SEPs. As research shows, the willingness to engage with a particular end-user depends on the richness of personal data provided (Ert, Fleischer and Magen 2016). The SEP must, therefore, espouse the technical tools necessary to assuage any hesitancy to provide this essential personal data while maintaining compliance with regulatory guidelines.

Unlike earlier peer-to-peer business models, such as eBay or Etsy, the trust between SE end-users expands beyond assurances of product quality to assurances of physical safety and responsible stewardship over another's personal property (Teubner and Flath 2019; Ranzini et al. 2017). Digitally supporting trust is challenging for any organization (Gefen et al. 2008). Still, the social exchange and real-world, physical encounter that comes along with SE transactions make trust even more vital (Williamson 1993). However, as challenging as it may be, pursuing the personal data governance mandated by the GDPR can assist in promoting the all-important trust factor necessary for successful SE interaction by demonstrating good business data practices (Zhang et al. 2020).

End-users eagerly provide their personal data supplied to the SEP, and research shows that they are more than willing to exchange their privacy for enjoying the benefits of participation in the SE (Lutz et al. 2017). Even though the choice is made to offset privacy, the duty to secure and protect personal data remains. This fact is the starting point for the remainder of this research. In Section 2.1, we go on to describe the nature of SE personal data further and track their movement to illustrate potential issues in meeting this duty to secure user personal data.

2.1 The Movement of Personal Data in the Sharing Economy

Tracking the movement of personal data is an important practice that not only allows an enterprise to clearly assess the amount and various types of personal data they govern, but also enables an accurate assessment of the appropriateness of systems used to protect this data. The GDPR recognizes the value in this process and requires some companies to keep internal records, called records of processing activities, intended "to support an analysis of the implications of any processing whether existing or planned, facilitates the factual assessment of the risk of the processing activities performed by a controller or processor on individuals' rights, and the identification and implementation of appropriate security measures to safeguard personal data" (WP29 Opinion). The information that follows is not intended to analyze the SE processing activities with the depth required of a GDPR mandated records of processing activities. Rather, the information gives a general overview of the SE personal data landscape, which still proves useful in evaluating the implications of processing activities and considering privacy and security measures.

Gateway personal data is the first necessitation for personal data in a SE transaction (Ranzani et al. 2017). This data is required to gain entry to the platform community and seek or offer goods and services. As Figure 2 depicts, the end-consumer and service provider approach the platform and provide this necessary preliminary data. Much of this data is similar for both the end-consumer and service provider; however, depending on the SEP's service offering, some of this data may be different. For example, on the Uber platform, only the service provider is required to supply data about their automobile and driving record. Some categories of gateway personal data include platform presence data (e.g., name, email address, profile information), personal property information (e.g., property address, property photos and descriptions), background and identity verification (e.g., copies of government-issued I.D.), payment information, location information (e.g., physical address, real-time GPS location) and device information (e.g., brand, battery life, and screen resolution). Gateway personal data goes a long way in shaping the trust and dual-safety SEPs attempt to digitally generate and lay the foundation for appropriate matchmaking (Ranzini et al. 2017).

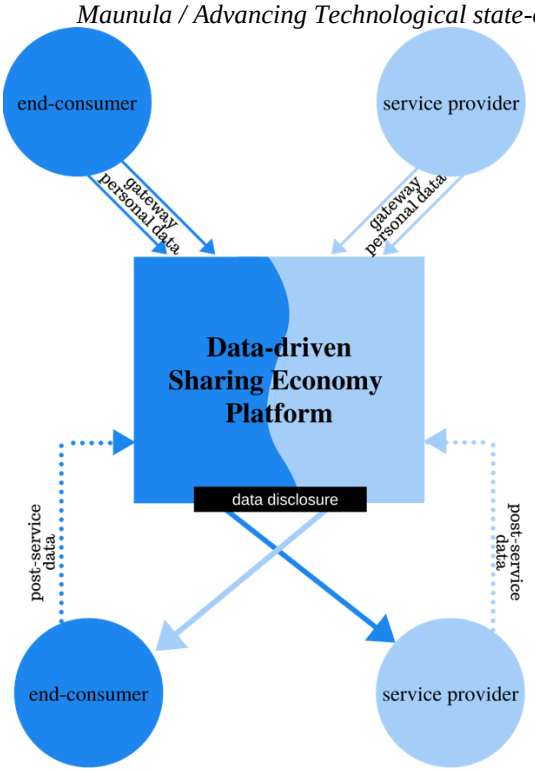

Figure 2. The flow of data in the Sharing Economy: Platform data disclosure to end-users

Figure 2 also shows that the personal data supplied to the SEP is what forms the very essence of the platform. The SEP decides which personal data is expected from each user to encourage the type of service transaction envisioned by the platform, be that on-demand travel, or lodging. The SEP assumes data controllership (Airbnb Privacy Policy), which includes the responsibilities and obligations set out by the GDPR to secure and protect this data (discussed further in section 2.3).

Once end-users supply the personal data necessary to gain access to the SEP, the next set of personal data directly contribute to the rendering of services. Here, the SEP decides which personal data it must disclose (see Figure 2), allowing the end-consumer and service provider to become transactional partners, and ultimately complete the transaction (Richter 2019). Some personal data are disclosed immediately for all platform participants to see, for example, platform presence data (as described above). Some personal data are disclosed to potential transacting partners; for example, real-time GPS location. And still, other data are disclosed to confirmed transactional partners; for example, physical addresses. SEPs do not themselves engage in the rendering of services or the provision of goods. It has been notably stated that, "Uber, the world's largest taxi company, owns no vehicles" and "Airbnb, the world's largest accommodation provider, owns no real estate" (Goodwin 2015). SEPs simply serve as matchmakers for their participants and facilitators of platform-level services, such as receiving and distributing payments.

At the time of services rendering, the utility of the data collected in an SEP's role as a matchmaker is put to the test by the end-consumer and the service provider. The proper execution of services at this point relies on the SEP identifying and passing on data already gathered for its purposes (facilitating matchmaking) to a service provider for their purposes (rendering services or providing goods).

After services are rendered, the service provider and the end-consumer return to the platform to share post-service data, as seen in Figure 2. These data include ratings and reviews and feedback data. Feedback data allows the service provider and end-consumer to rate the effectiveness of the SEP. Rating and review data, on the other hand, is personal data that enables service providers and end-consumers to evaluate the quality of the service interaction and provide future platform participants, and the SEP, with information about that interaction. Rating and reviews greatly enhance the necessary trust between service providers and end-consumers that allows participants to help one another make informed choices and steers the SEP in structuring a better platform experience for more appropriate matchmaking (Möhlmann and Geissinger 2018).

This movement of personal data is the hallmark of the SE and inherent to the business model. Users have come to expect the disclosure of their data and offset privacy concerns to receive the proven benefits of engaging through the SE (Lutz et al. 2017). However, legal compliance analysts must consider the ramifications of this data movement beyond the privacy trade-offs and scrutinize the security and protection concerns this data movement raises.

2.2 Legal Requirements for Personal Data Protection

When the personal data supplied to the SEP originate from an individual in the EU, the GDPR is triggered. In 2016, the European Commission set out to strengthen legal rules for data protection by updating the 1995 Data Protection Directive (DPD), the catalyst being the DPD's inability to address personal data protection and security in the face of emergent technologies (Room et al. 2018). The resulting GDPR has become a global gold standard in data protection with a territorial scope that captures business outside the EU, including those SEPs headquartered in the United States and elsewhere (Li and Yu, 2019; GDPR, Article 3(1-2)).

Personal data protection, as mandated by the GDPR, pivots on the designation of a data controller. The data controller determines the purpose and means - the 'why' and 'how' - for data processing (GDPR, Article 4(7)). Thus, the data controller is the entity responsible for the decisions concerning which technologies to employ for its data processing purposes. The data controller bears responsibility for compliance with the GDPR and must ensure and be able to demonstrate that all processing is done lawfully and in accordance with the provisions of the GDPR (GDPR, Article 5(2)).

Data controllers may engage competent data processors that assist in selecting appropriate technology and carrying out processing activities (GDPR, Article 28). However, this data processor can only process data by the instructions of the data controller (GDPR, Article 29) provided through a written contract known as a data processing agreement (GDPR, Article 28(3) and Article 29). As long as a data processor's actions fall within the confines of the data processing agreement, the data controller remains responsible for personal data and legally accountable for all technology choices, and any falters in security and privacy these choices bring.

This being said, a significant change from the DPD to the GDPR is that it places compliance obligations on data processors as well as data controllers. Data processors can be subject to the same hefty fines - up to 4% or 20,000,000 EUR of global annual revenue, whichever is greater (GDPR, Article 83) - for failing to meet compliance obligations applicable to the controller. While demonstrating adherence to the contractual obligations laid out in the data processing agreement can mitigate data processor penalties, the need to pay even a portion of these penalties may prove financially disastrous to some companies.

The GDPR grants individuals control over their personal data through a set of individual rights known as data subject rights (GDPR, Articles 16-21), the exercise of which should be enabled by the data controller (GDPR, Article 12(2)). Data subject rights include the rights to access, rectification, erasure, restriction of processing, data portability, and objection to processing. Data controllers must provide the transparency and tools that inform data subjects of all data collected concerning them, and the ability to access this data as envisioned by this set of rights. The data controller must provide any information pertaining to these rights in a "concise, transparent, intelligible and easily accessible form using clear and plain language…" (GDPR, Article 12(1)).

The GDPR bars any processing of personal data without establishing a legal basis to do so (GDPR, Article 6). The six lawful bases established by the GDPR include consent, the performance of a contract, compliance with a legal obligation to which the controller is subject, to protect vital interests of the data subject or other natural person, performance of a task carried out in the public interest, or legitimate interest (GDPR, Article 6(1)(a-f)). The collection, use and disclosure of personal data in the SE function primarily under the lawful bases of consent and performance of a contract (see, for example, Uber and Airbnb privacy policies).

Moreover, all processing must be done in observance of six principles. Those six principles demand that any personal data processing embrace (GDPR, Article 5(1) (a-f)):

1. lawfulness, fairness and integrity
2. a purpose limitation
3. data minimization
4. accuracy
5. storage limitations

6. with integrity and confidentiality

In the case of these principles, the data controller, once again, stands in the position of accountability and is responsible for compliance (GDPR, Article 5(2)).

Ensuring data subjects' access and control over their data, requiring a legal basis for all of their processing and demand for adherence to data processing principles are measures meant to make the GDPR a strong instrument for the protection of personal data, but also a challenge for compliance. These measures should also form the core of any technological structures to achieve compliance.

2.3 Data Protection Red Flags in the Sharing Economy Context

This Section merges the information in Section 2.1, regarding the movement of data in the SE, with the information in Section 2.2, regarding the lawful processing of personal data under the GDPR. The enmeshing of these two realities for the SE creates an entanglement that makes it easier to see irregularities that illuminate two critical GDPR compliance red flags. To deepen the understanding of the privacy and safety issues discussed, this Section begins with a real-world example of the data protection issues that can arise in the SE. Consider the following occurrence:

Denver, Colorado, USA – On 26 March 2015, Gerald Montgomery, a 51-year-old Uber driver, picked up a local woman for a trip to the airport. After successfully delivering her to the destination, Mr. Montgomery returned to her home address to burglarize the property. Mr. Montgomery was positively identified by his passenger's roommate, who was home at the time and scared him off. This identification was made possible by a screenshot the passenger took of her Uber receipt, which included his photograph.

Uber responded with the following statement: "[Uber] takes rider safety very seriously, and upon learning about this incident, we reached out [to] the rider. We immediately removed the driver's access to the Uber platform, pending an investigation. We continue to be in contact with the rider and will assist the authorities in whatever way we can." (Roberts 2015)

The data flow in the event recounted above mimics the depiction in Figure 2. The Uber rider (end-consumer) supplied her gateway personal data to the Uber platform, allowing them (through contract and consent) to use this data to efficiently match her with an available driver (service provider). The rider's personal data is protected while she is on the platform, with Uber serving as data controller. The Uber platform then disclosed necessary data to the passenger and driver, allowing them to connect to perform the service. At this stage, Uber removes itself from data controllership, as they are not involved in the service-rendering phase in any way. However, the incident shows the ease with which a service provider can use (process) personal data supplied by the platform for nefarious reasons. While banning the service provider from the platform may be appropriate business responses, what should be the proper data protection response? And, more importantly, what should be the appropriate data security support to curtail such abuses?

As Section 2.1 and the scenario above explain, personal data in the SE context is originally collected and used by the platform, who serves as the data controller (see Figure 2). The SEP then decides which data it must pass on to end-users (both service providers and end-consumers) to complete the service transaction. The reception and use of personal data by these end-users are acts of data processing. Thus, the first red flag raised by the data processing activity in the SE is the specific implication of the service provider as a data processor created by this disclosure and use of personal data.

The GDPR defines data processing 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (GDPR, Article 4(2)). Although both end-users can be described as data processors, in general, it is the processing activity of the service provider that falls under GDPR obligations. This regulatory capture is due to the fact that service providers reap an economic benefit as a result of their data processing activities. Recital 18 of the GDPR explicitly states that exclusion under Article 2(2)(c) can only be enjoyed by those "with no connection to a professional or commercial activity." Article 2(2)(c) of the GDPR provides an exclusion from GDPR provisions for those that process data "in the course of a purely personal or household activity." End-consumers that merely pay for and receive goods and services through the SE fall under this exclusion, however, service providers do not.

Now, clearly classified as data processors beholden to GDPR obligations, a threat to privacy and security arises in the fact that service providers are not considered, addressed, guided, directed, nor contracted as data processors by SEPs (see

Uber and Airbnb Privacy Policies). As described in Section 2.2, data processors must only operate under the contractual stipulations of a data processing agreement. This agreement is a vital link that maintains a connection between the data controller and the data processor, ensuring that data is processed in line with the data controller's wishes and an equivalent level of data security. However, the recognition, and thus guidance, of service providers as data processors acting upon instructions of the SEP creates a relationship counter to the SEP's business function as a mere intermediary providing a matchmaking function. The SEP reliance upon GDPR consent and contract fulfillment mechanisms do not prove adequate as a means of data protection, considering the potential of harm that could befall personal data in the hands of a service provider.

The second red flag emerges as a consequence of the first. The SEP extraction from GDPR obligations over data processed during the service rendering phase causes a break in the consistency of data protection by allowing the SEP to abandon data controllership temporarily. As Section 2.2 (and Figure 2) points out, the recursiveness of the post-service rating and review data brings end-consumer back to the platform, reigniting SEP data controllership. Rating and review data is, in fact, personal data (Golbeck 2016) subject to protection under the GDPR, and is a part of the data disclosed by the SEP. Further, rating and review data has a bearing on the digital reputation of SE users, in particular, the service provider that stands to lose the economic benefits participation brings (Hawlitschek et al. 2016). Consequently, the GDPR places special protection over data that may "give rise to… damage to the reputation" (GDPR, Recital 75). Rating and review data may fall under this special category, requiring special security measures to minimize the risks to the rights and freedoms of data subjects. The implication created by this recursivity is that the SEP re-engages as the data controller, as end-users are on the platform to provide and benefit from this valuable data.

As Figure 2 shows, the SEP is irreducibly involved in handling, management and distribution of data. As such, the SEP remains the data controller at every stage. The recursive quality of rating and review data means that the purpose for the data has not changed – to assist in the completion of the SE transaction. Thus, rating and review data strengthens the SEPs line of involvement throughout the movement of data. This has consequences on GDPR obligations and sculpts a new data controller - data processor relationship between the service provider and SEP; a relationship where the SEP must exhibit greater responsibility over the entire SE data flow.

In-depth legal analysis of the interplay between legal obligations and platform interests in the processing activities in the SE raises red flags about the security and protection of personal data. It stands to reason that this socio-technical industry would look to technology for possible solutions to strengthen privacy, security and, thus, GDPR compliance. The shift will be from considering tech tools for security and privacy from a SEP compliance perspective to a service provider as data processor perspective.

3. Technology's Supportive Role in Protecting Sharing Economy Personal Data

Although the GDPR is technology neutral, meaning that it governs manual or automated data processing (GDPR, Recital 15), throughout the text of the Regulation, it is clear that there is a focus on what technology can do for achieving compliance and the challenges of remaining compliant while instituting new technologies. For example, the GDPR is built on a concept called Privacy by Design and Default (GDPR, Article 25). This concept means that organizations must always use "appropriate technical and organizational measures" to ensure they meet GDPR requirements (GDPR, Recital 78). In other words, data protection should be integrated at every stage of product or service development, from creation to implementation (by design), while adopting the strictest privacy standards (by default) (GDPR, Article 25). Technology is the clear way to adhere to these concepts.

Article 32 and Recital 83 of the GDPR directly deal with security of processing. The GDPR requires that companies consider the current "state of the art" when determining if security measures are appropriate. Although this ambiguous statement raises many questions, it makes clear that lawmakers expect industries to devise security strategies that "continuously evolve in line with anticipated advances in technology" (ElectricIQ 2018). Further, the concepts of GDPR's privacy by default and the state-of-the-art requirement must be viewed as a unit. If simultaneously, how the technology is arranged and the state-of-the-art must be applied, it naturally leads to an understanding that technology has to be at the forefront of any discussion. The communication between data-driven industries, such as that between the SE and ICT developers about their functions and their legal compliance, becomes an ongoing conversation.

As analyses of processing activities are meant to reveal, the analysis in this research shows the type, movement and gaps in protection of personal data. Inherent in the SEP business model is the need to collect data of various types that are disclosed to service providers to complete a transaction. During the course of this transaction, new data is compiled regarding the quality of services and the technologies that enable them. This recursive flow of data implicates the service provider as a processor of data under the GDPR, and maintains the role of the SEP as controller of this data. As data

controllers, the SEP will look to the same technologies that allow this collection, disclosure, and recursive nature of data to restructure security and privacy methodologies to meet the challenges of this implication.

3.1 A Call for Customized Technology for Developing Sharing Economy Data Protection Challenges

Customizing information security technologies for these developing compliance concern in the SE requires thinking on a nuanced level. Developers must move from considering general protections of all types of information from any unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (Kissel 2013), to considering the more specific protection of information related to an identified or identifiable natural person. Additionally, the tools must move from the broader compliance support of the quite capable SEP, to the targeted compliance support of service providers under specific processing conditions (Guamán 2016).

Current tools that enable the SEP and secure its valuable data are configured with the needs and capabilities of the SEP in mind. Envisioning service providers as data processors under the direction of the SEP (the data controller) demand new or reconfigured technologies that secure personal data while on the leg of its journey that takes it through the hands of the service provider.

In the SE context, disclosure of personal data extends to intermediaries and third-party data processors, such as payment processors, background check and identity verification providers, cloud storage providers, and marketing partners (Uber Privacy Policy). These categories of data processors that process on behalf of the SEP include business that are typically better equipped to secure data. The GDPR requires that data controllers "shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of that data subject" (GDPR, Article 28(1)).

This research shows that the requirement outlined in Article 28 to only use competent data processors must now extend to the service provider. A typical SE service provider, for example an Uber driver or an Airbnb host offering a room, is not necessarily equipped to guarantee appropriate "technical and organizational measures". However, the ongoing involvement of the SEP and its ability to implement appropriate technical measures may alleviate demands placed upon an ill-equipped data processing SE service provider. Established in the EU Court of Justice Google-Spain 2013 case, the balanced approach to protecting personal data insists that parties consider where "effective and complete control" would lie. It stands to reason that in the context of the SE, the Court would draw the line of effective and complete control around the SEP and its technological capabilities and contractual positioning over the flow of data.

An adequate system of extending controls from the platform to service providers may best be delivered through mobile devices and applications. The prolific use of mobile-apps to execute SE transactions creates a significant entryway into creating new compliance strategies. Mobile technology has already perfected the SEP's capability to communicate with its users, allow users to communicate with one another, acquire consent, verify identity, collect payments and encourage the robust rating and review systems that garner trust. Adapting technologies, with their dynamic user interfaces, for the mobile app environment can efficiently extend the SEP's data controller compliance obligations through the activities of the service provider's data processing. The goal is not only to provide tools that are easy to navigate, but those that actually achieve compliance under these unique circumstances.

Currently, there are tools on the market that could be configured for this purpose. For example, a company called MangoApps has developed a screen capture program called TinyTake which can blur specific parts of a screenshot to hide certain personal data (TinyTake 2019). This could prevent users from capturing data for later, unauthorized use. But again, this requires a nuanced approach, because this personal data, in large part, is necessary. The goal would be to prevent unnecessary screenshots that may lead to nefarious behavior.

Other possible solutions could allow the platform greater control over this data. For example, many service providers using the Uber platform utilize dashcams to ensure their physical safety and protect against any false claims. However, recent violations of the use of these cameras have allowed individuals to misuse this footage, which is personal data of their riders. In a recent case in St. Louis, Missouri, a passenger using the Uber ride-sharing platform, discovered that footage taken by her driver's dashcam was being livestreamed via a paid platform. The rider was made aware of the use of the dashcam and told the driver told her it was for his personal safety and security (Heffernen 2018). The Uber passenger agreed to relinquish her privacy for that effect, but, privacy notwithstanding, the misuse of her data would constitute a violation of EU personal data protection laws. A system where the platform controls the dashcam would better protect riders in these situations. Controls at the platform level could collect the data, manage retention time and ensure proper deletion, assigning contentions over any other nefarious dashcam use to other areas of the law (e.g., criminal law, tort law).

Recent attention concerning information privacy in the SE has focused on the use of blockchain technology. Blockchain allows peer-to-peer data transmission that bypasses a centralized server (De Philippi, 2017; Tumasjan and Beutel, 2019). Blockchain is problematic in the sense that the implication of further decentralization would remove the need for an SEP altogether, robbing the business model of its function. Beyond having structural problems, the blockchain is also problematic under the GDPR. The immutability of data, a strong characteristic of blockchain technologies, does not allow the proper exercise of data subject access rights, especially the right to rectification and deletion of data. However, blockchain could be a solution if the tool is tailored for use by the platform and ensures data subject rights.

These types of tailored solutions for security and privacy may exist, but need to be re-packaged and delivered from the perspective of data protection law and the consideration of ill-equipped service providers as processors under those laws.

4. Conclusion and Considerations for Future Research

Data-driven industries, including the SE, will continue to scrutinize their business practices in light of the complexities of achieving and maintaining GDPR compliance. This requires continually balancing the goals of the business model with innovative technological affordances. It can be said that the almost paradoxical push and pull between technology and legal compliance has dramatically influenced the SEP's relationship to the GDPR. This new relationship offsets this delicate balance of business and technology. Any solution for recalibrating security and privacy systems when business model analyses raise new GDPR compliance issues must be fashioned out of the dependency on technology.

As has been argued in this paper, a fresh legal analysis of processing activities in SE business models raises two GDPR compliance red flags pulls the service provider under the compliance canopy of the GDPR. The far-reaching implications of service provider data protection obligations realigns their relationship with the SEP and the technical tools already used to achieve privacy and security in the SE. This theoretical legal research will allow the industries of internet technologies, internet communication technologies, and information systems to sculpt the perfect solution. But research such as this is essential to clearly define the issues so that these technological remedies will be appropriate. As this paper reveals, disruption may just be knocking on the door of technology with regards to the sharing economy, because the SE business model reveals weaknesses in personal data protection that are not among the pool of readily available digital tools to pull from.

The major contributions in this research are, admittedly, heavily theoretical and legal. This is not meant to diminish the multidisciplinary balance called for throughout this paper. The intent of this paper, however, is to spark the interest in IT and ICT research to enhance data privacy and security for a specific legal challenge. With this legal analysis in mind, future research should be developed in the areas of mobile application interfaces, SEP supported blockchain and features that ensure appropriate data minimization and purpose and storage limitations as personal data lies in the hands of service providers.

Placing the SEP in control of the entire SE data flow is a game changer for the relationship between all SE stakeholders: SEPs, end-users and regulators. This new relationship demands quantitative and qualitative IT and ICT. Methodologies such as business case study can support a clear vision for platform actions, and technology gap analysis alongside legal gap analysis study ensures the way forward strengthens compliance, security and protection for all involved.

5. References

"Airbnb Privacy Policy." https://www.airbnb.com/terms/privacy_policy.

Dakhila, Sami, Andrés Davila, and Barry Cumbie. "Trust, but Verify: The Role of ICTs in the Sharing Economy." *Information and Communication Technologies in Organizations and Society: Past, Present and Future Issues.* Edited by Francesca Ricciardi, and Antoine Harfouche. Springer, Switzerland, 2016.

De Filippi, Primavera. "What Blockchain Means for the Sharing Economy." *Harvard Business Review*, 2017.

ElectricIQ. *GDPR and 'State of the Art' Security.* 2018. https://medium.com/@eclecticiq/gdpr-and-state-of-the-art-security-a5c07c04aeeb.

Gefen, David, Izak Benbasat, and Paul A. Pavlou. "A Research Agenda for Trust in Online Environments." *Journal of Management Information Systems*, vol. 24, no. 4, 2008. pp. 275-286. *JSTOR*. http://www.jstor.org/stable/40398920.

Goodwin, Tom. *The Battle is for the Customer Interface,* 2015. http://social.techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/.

Guamán, Danny. *Privacy Vs. Data Protection Vs. Information Security – Software and Services Engineering,* 2016. https://blogs.upm.es/sse/2016/11/01/privacy-vs-data-protection-vs-information-security/.

Hawlitschek, F., T. Teubner, and C. Weinhardt. "Trust in the Sharing Economy ." *Die Unternehmung – Swiss Journal of Business Research and Practice*, no. 70(1), 2016. https://www.nomos-elibrary.de/10.5771/0042-059X-2016-1-26.pdf.

Heffernan, E. "Uber Evaluating Policies in Response to Story on St. Louis Driver's Secret Livestream." July 24, 2018. https://www.stltoday.com/news/local/metro/uber-evaluating-policies-in-response-to-story-on-st-louis/article_7c8e4558-ff49-54c0-8e8c-a6e79b954325.html.

Irwin, Luke. "Organisations Struggling to Meet GDPR Requirements, with Poor Planning and Lack of Awareness to Blame." 2019. https://www.itgovernance.co.uk/blog/organisations-struggling-to-meet-gdpr-requirements-with-poor-planning-and-lack-of-awareness-to-blame.

Kissel, Richard L. *Glossary of Key Information Security Terms.* 2013. https://www.nist.gov/publications/glossary-key-information-security-terms-1.

Li, He, Lu Yu, and Wu He. "The Impact of GDPR on Global Technology Development." *Journal of Global Information Technology Management*, vol. 22, no. 1, 2019. pp. 1-6. https://doi.org/10.1080/1097198X.2019.1569186, doi:10.1080/1097198X.2019.1569186.

Madsen, Wayne. *Handbook of Personal Data Protection.* Palgrave Macmillan UK. 1992. https://www.palgrave.com/gp/book/9781349128082.

Richter, Heiko, and Peter R. Slowinski. "The Data Sharing Economy: On the Emergence of New Intermediaries." *IIC - International Review of Intellectual Property and Competition Law*, vol. 50, no. 1, 2019. pp. 4-29, https://doi.org/10.1007/s40319-018-00777-7, doi:10.1007/s40319-018-00777-7.

Room, Stewart, Peter Almond, and Kayleigh Clark. *Technology's Role in Data Protection - the Missing Link in GDPR Transformation.* PwC, 2018.

Seigneur, Jean-Marc. "Social Trust of Virtual Identities." *Computing with Social Trust.* Springer London, London, 2009.

Tankard, Colin. *What the GDPR Means for Businesses.* 2016. http://www.sciencedirect.com/science/article/pii/S1353485816300563, doi:https://doi.org/10.1016/S1353-4858(16)30056-3.

TinyTake. "Best Free Windows Screen Capture & Video Recording Software." 2019, https://tinytake.com/.

"Uber Privacy Policy.", https://www.uber.com/global/en/privacy/notice/#data.

van den Hoven, Wolter, Jeroen, Blaauw, Martijn, Pieters, and Martijn Warnier. "Privacy and Information Technology." *The Stanford Encyclopedia of Philosophy.* Edited by Edward N. Zalta. Metaphysics Research Lab, Stanford University. 2019. https://plato.stanford.edu/archives/win2019/entries/it-privacy/.

Wiener, Jonathan B. *The Regulation of Technology, and the Technology of Regulation.* vol. 26. 2004.

Williamson, Oliver. "Calculativeness, Trust, and Economic Organization." *Journal of Law and Economics*, vol. 36, no. 1, 1993. pp. 453-486, https://EconPapers.repec.org/RePEc:ucp:jlawec:v:36:y:1993:i:1:p:453-86.

WP29 Opinion. *'Article 29 Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (WP 169, 16 February 2010).*

Author Biography

Gail L. Maunula is a doctoral researcher at the University of Turku Faculty of Law in Turku, Finland. Her research centers around the impact of human and fundamental rights issues on the Sharing Economy from a European socio-legal perspective, including the rights to data protection and privacy. Gail also holds a professional certification in information privacy for the European sector (CIPP/E). Gail further explores the wide range of issues arising from data protection and privacy as a member of the Digital Disruption of Industry Research Project (DDI), a multidisciplinary research consortium studying the impact of digitalization on Finnish society through the lens of industry.