Article:
Ciardiello, F. and Di Liddo, A. (2022) Privacy accountability and penalties for IoT firms. Risk Analysis: an international journal, 42 (8). pp. 1784-1805. ISSN 0272-4332

https://doi.org/10.1111/risa.13661

Risk Analysis, Vol. , No. ,

Privacy Accountability and Penalties for IoT Firms

Francesco Ciardiello*
The University of Sheffield, Sheffield, United Kingdom
Andrea Di Liddo
Department of Economics, University of Foggia, Foggia, Italy

Abstract

Internet of Things (IoT) business partnership are formed by technological partners and traditional manufacturers. IoT sensors and devices capture data from manufacturers' products. Data enforces product/service innovation thanks to data sharing among companies. However, data sharing among firms increases the risk of data breaches. The risk increase is due to two phenomena: information linkage and privacy interdependency. Data Protection Authorities (DPA) protect data users' rights and fine firms if there is an infringement of privacy laws. We present two different business scenarios: the first is where each firm is a data owner and the second is where only the manufacturer is the data owner. Data protection authorities sanction the responsible of privacy law infringement. For both scenarios we present two *fair* penalty schemes that suggest: the total amount of the fine and how to share the fine among the participants. Penalties critically vary at how innovation networks are structured in IoT industries. Our penalties provide incentives to data sharing since they redistribute firms' responsibility against data breaches. Our penalties may mitigate the risk on the manufacturer if is the unique responsible for data handling.

Keywords: Data Breach, Data Sharing, Cooperative Game Theory, Risk Mitigation, European GDPR

200-character summary for social media

We provide systems of penalties for IoT connected firms if a data breach occurs. Our penalties take into account two factors: data ownership and two types of data. Our penalties may integrate the European GDPR.

*Address correspondence to Francesco Ciardiello, Management School, University of Sheffield 1 Conduit Road, Sheffield S10 1 FL (UK), E-mail: f.ciardiello@sheffield.ac.uk.

1 Introduction

The increasing fusion of information and communication technologies has brought the so-called Industry 4.0 into the manufacturing world. Traditional manufacturers trigger new industries off by virtue of a new technological revolution: *Internet of Things* (IoT). Connections between users and devices have rapidly expanding. Technologies, such as sensors, are embedded in every day products like cars, utility meters, white goods, wearable fitness trackers or home security systems. Traditional products are equipped with sensors and devices. Devices are capable of sensing and remotely communicating among them and with products. Users' data are captured from sensors and are updated, transmitted, sorted and analysed. The latter is possible thanks to advances in digital technologies, driven largely by three fundamental economic factors: lower processing costs, cheaper storage and less expensive bandwidth (Büyüközkan & Göçer, 2018). Even though manufacturers are often data holders, they are often unable to extract business value from IoT data. Nowadays, manufacturers tend to form partnerships with technology companies, service providers and related businesses. There is an increasing trend of data-driven networks among firms in order to turn raw data in customers' services, new business models, innovation. Partners enables manufacturers to create an additional foothold with new services and manufacturers have an incentive to share IoT data with these technological partners. Conversely partners have the opportunity to face new business challenges. However, data sharing is an intricate issue for firms: coordination among firms is extended to the sharing of IoT data management infrastructures and architectures (Abu-Elkheir, Hayajneh, & Ali, 2013).

In this emerging business scenario, consumers become users and users generate data. However, users have concerns about how data are collected and shared with third parties. Data can show personal features of users' identity or behaviour. Data can be leaked, or more explicitly, exploited for non authorised purposes. The concept of data breaches embraces different contexts and angles. One of the most common definition is the following: *A data breach is a security violation in which sensitive, protected or confidential data are copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.* [1] The data processing tasks include data acquisition, fusion, aggregation and integration in IoT systems. In case of IoT ecosystems data acquired from different streams originating from various devices and subsystems undergo fusion, aggregation and integration to ensure innovation, quality of service. During data integration, attributes of data belonging to different services are correlated and integrated. At times, this reveals information or insights about users, their demographic location and activities, which lead to severe privacy concerns. In addition, with the data sharing and processing tasks possible at various levels of granularity, it becomes more complex to identify where information linkage might occur. For example, in case of IoT ecosystems, information linkage might occur not just at device/data-stream level but also while sharing statistics and analytics on the data among firms. This is why, in privacy-sensitive domains, individual data streams that potentially lead to a privacy hazard are anonymised before data handling (Porambage et al., 2016). Firms share data. However, sharing is not necessarily limited to dyadic relationships. Once data are shared with a firm, same data might be transmitted to other entities without the consent of the original source; this mechanism could be out of their own control. In such interlaced settings, the privacy of individual users is bound to be affected by the decisions of third parties and third parties' third parties and so on. The latter mechanism increase the magnitudo of negative externalities on users' privacy. This phenomenon is known as privacy interdependence and has been analysed in several data sharing contexts (Biczók & Chia, 2013), (Pu & Grossklags, 2014), (Symeonidis et al., 2018), (Olteanu, Huguenin, Humbert, & Hubaux, 2016), (Symeonidis, Shirazi, Biczók, Pérez-Solà, & Preneel, 2016). IoT Data do not have the same potential threat to users' privacy. In the current work, we make a clear distinction between two types of data having different value for users. Data, that has a higher level of users' potential information, are subject to third parties' processing, integration and analysis. We refer these data to as *private data*. Data deal with

[1] https://www.acf.hhs.gov/sites/default/files/cb/im1504.pdf. Last accessed April 30, 2020.

information on products and are analysed to improve products' features. We refer these data to as *common data*. Common data have a lower level of potential disclosure. Many privacy bodies are worldwide active and put in place laws and mechanisms to protect users' privacy rights. One of the most known regulation is the General Data Protection Regulation in the European Union (GDPR). GDPR is a regulation in EU law on data protection and privacy in the EU. According to GDPR, some key legal points are fixed: companies, who collect data, are also liable for the data processing from third parties. If a data breach happens, the supervisory body validates data that have been treated not in compliance with GDPR. The body fines the so-called data controller.

Can we suggest to Data Privacy Authorities sensible penalties for firms if a data breach happens? If not, can IoT data accountability be fairly shared among IoT firms in new business scenarios? Can those penalties mitigate the manufacturers' economic risk if the manufacturer is the unique data owner? Are potential proposed schemes congruent, integrable with the current GDPR's operational procedures and with GDPR's philosophy?

We build two penalty schemes based on a fair measurement of firms' accountabilities in IoT industries. The first penalty scheme regulates penalties if each firm is owner of private data. The second penalty scheme regulates penalties if the loss is due to a mixture of common and private data, originally collected and owned by the manufacturer. The second scenario is when the manufacturer collects data and, then, shares data with its partners. For instance, manufacturers are owners of data produced in the vehicle in the industry of smart cars.

The rest of the paper is organised as it follows. Section 2 contains literature related to our paper. Section 3 contains the description of the holistic IoT model where different economic actors are present: consumers or users, manufacturers and technological partners. To boost the formal description of the privacy model, we provide evidence of an industrial case: the industry of smart cars. In Section 4 we present our cooperative model described by transferable utility games with characteristic functions. Measurements of privacy accountability are given by Shapley values of the previous TU games. Finally, Section 5 provides penalties for privacy loss due to leaked data. Penalties are based on previous accountability measures. To boost our results in modern IoT cases, we emulate a procedural case of privacy infringement under GDPR. We show how our penalties can be used to sanction partners and how can mitigate fines' impact on the unique data controller, i.e. the manufacturer. In Conclusions, we discuss the relevance, limitations and future research of the current paper. In Appendix, proofs of main results are shown.

2 Related works

Privacy issues for sensor networks are especially related to the process of integration of data from multiple sources (Lopez, Rios, Bao, & Wang, 2017), (Madaan, Ahad, & Sastry, 2018). Privacy accountability can be somehow complex to be defined, if data ownership does not assume a clear formulation. In fact, many papers address the inadequacy of formal and ethical frameworks regulating IoT business environments and advocate for urgent actions in legal analysis and new legislation (Maras, 2015), (Weber, 2015), (Caron, Bosua, Maynard, & Ahmad, 2016), (Tzafestas, 2018). The problem of data ownership is the legal key and is widely discussed under different angles in (Janeček, 2018). In (S. Park, 2019) the author empirically argues how the growing body of privacy laws does not match with a reduction of data breaches in US. The failure is explained through the presence of unregulated economic spillovers among different firms. The complexity of the relations is specific for each business case. For instance, European regulations and data ownership in smart car industries are disentangled in (Kerber, 2018). The author argues that manufacturers use legally the so-called *extended vehicle concept*: this allows the transmission of all data produced in cars directly to servers of the manufacturers, granting them a monopolistic control of these data. Moreover, he observes that firms, within ecosystems of connected and automated mobility, could provide a wide range of

services to the cars owners and drivers, if they also have access to the in-vehicle data. As such, this recommendation suggests to transfer privacy accountability from manufacturers to partners. From the aforementioned literature, it is straightforward to see that privacy regulations are conflictual with business interests. GDPR or similar privacy regulations create friction, complexity and litigations to Internet of Things ecosystems (Seo, Kim, Park, Park, & Lee, 2018), (Shovon, Roy, Shil, & Atik, 2019). A few papers adopt an *ex post* analysis. Even if there is a growing body of literature supporting *privacy by design*, associated costs for those designs are high. In (Seo, Kim, Park, Park, & Lee, 2017), the authors examine the impacts and consequences of GDPR on a IoT industry and they perform a cost analysis. The outcome is that those costs are extremely high. The latter suggests that many firms might fail in protecting customers' privacy and they might incur in fines imposed by Data Protection Authorities. Another stream of research is related to consumers' compensation if data breaches happen. The most common practice is that firms provide product and service compensation for free (Goode, Hoehle, Venkatesh, & Brown, 2017), (Kude, Hoehle, & Sykes, 2017). Interestingly, social structure can affect consumers' perception of *fairness* for a given compensation (Kude et al., 2017).

The main concern that customers, in primis, and individuals in general, have about their data is security but also privacy (Ziegeldorf, Morchon, & Wehrle, 2014), (Díaz, Martín, & Rubio, 2016), (Lopez et al., 2017), (Kerber, 2018). Nevertheless users do not put in place mechanisms to protect privacy: such behaviour is commonly referred to as *privacy paradox* (Posner, 1981), (Acquisti, John, & Loewenstein, 2013), (Spiekermann, Acquisti, Böhme, & Hui, 2015), (Acquisti, Taylor, & Wagman, 2016). There is a stream of literature where users strategically reveal personal data at different levels in order to protect their privacy (Ioannidis & Loiseau, 2013) (Chessa, Grossklags, & Loiseau, 2015). Users may receive some benefits in giving private data away. The appropriate quantification of how much benefits users can get by releasing their data is faced in (Chessa & Loiseau, 2017). The authors propose two famous solutions from cooperative game theory: the Shapley value and the core as tools for compensating the release of personal data. The problem of economic trade-offs in data games is axiomatically faced in (Béal & Deschamps, 2016), (Béal, Deschamps, & Solal, 2016). The authors define compensation schemes, which specify how data owners should be compensated by the agents in needs of data. On the class of data games, the core, the nucleolus and the Shapley value provide relevant compensation schemes. The authors provide characterisations of the set of all (additive) compensation schemes belonging to the core, of the nucleolus, of the Shapley value for data sharing games.

3 A mathematical representation of IoT models.

A manufacturer sells a product endowed with sensors and devices. We make the following hypotheses and assumptions explicit in our holistic IoT model:

- Sensors collect data on users and on product's functioning. Data are usually stored in unstructured databases or may be captured by firms in real time (Wang et al., 2013). Data have different level of users' privacy. Most of acquired data are released on aggregate and anonymous basis and, then, is referred to as *common data*. Conversely, some data are personal and embodies users' sensible information. This data are referred to as *private data*. Data have a value since hides users' personal information somehow. This value represents a cost for users if users give away data. Such a cost increases within the associated effects in data sharing: interdependent privacy and information linkage.

- Consumers buy the product and accept privacy conditions imposed by the manufacturer. Consumers are users and generate data. Users have an incentive to give away their data (also, the most sensible ones) because they expect to receive product improvements. Consumers are aware of this process of data collection but they are less aware of further data processing from partners/third parties.

- The manufacturer forms partnerships with technological companies, service providers, IT companies in order to create business value from data. The whole set of companies in the IoT industry share and integrate data. Partnerships are innovation networks where connections are bi-directional. The relationship among innovation and inter-organisations has been deeply analysed in several and multiple environments. It is quite established result that the knowledge base of an industry has a complex behaviour when innovation is the key for the industry. The sources of innovation are found in networks, rather than in individual firms. The cooperation (more than competition) and the formation of flexible organisational links is dominant in uncertain early market (S. H. Park, 1996). Cooperation among firms to extract information from the raw data creates the so-called value chain in data-driven networks for innovation (Powell, Koput, & Smith-Doerr, 1996), (Gulati & Gargiulo, 1999), (Goes & Park, 1997). IoT systems offer a great amount of private data and innovation networks are data-driven (Abella, Ortiz-de Urbina-Criado, & De-Pablos-Heredero, 2017). Thus, new technologies are the focus of a variety of cooperative efforts that seek to reduce the inherent uncertainties associated within unexplored markets.

- Data sharing increase users' privacy value, even if data sharing is useful to product innovation. Data sharing among firms has two negative externalities for users' privacy: interdependent privacy and information linkage. The first network phenomenon can be briefly summarised as it follows: copying in same data (from a source firm to an interdependent destination firm and so on) increases users' peril of data breaches (Kamleitner & Mitchell, 2019). If destinations, i.e. firms, have own data then there is a supplementary risk to users' privacy. The second phenomenon can be briefly summarised as it follows (Madaan et al., 2018). A firm receives data from another firm. The last company might integrate received this data with their own data; in doing this, the company can gain a surplus of private information on users' private features.

We provide a mathematical formulation of the previous IoT system. As we have discussed above, partners and manufacturers form networks in order to provide innovation to products. The best way to mathematically represent this network is the mathematical concept of a graph.

- Let N be the set of n partners including the manufacturer.

- E is the set of links which represent connections from/to two different firms.

- Firms may have different number of connections with other firms. Let d_i be the degree of $i \in N$ in E. It represents the number of connections in which firm i is involved.

- $|E|$ denotes the total number of connections available in the network. Let $E_{-i} \subset E$ be the set of connections in which firm $i \in N$ is not involved. It is $|E| = |E_{-i}| + d_i$ for any $i \in N$. A network is a simple and connected mathematical graph, that is $G = (N, E)$.

- Data have a privacy value for users. The value of private data unit is $\beta_{priv} \in]0, 1]$. The value of common data unit is $\beta_{comm} \in]0, 1]$. The unitary value of private data is greater or equal than the value of common data. We normalise β_{priv} to one and set $\beta_{comm} \equiv \beta \in]0, 1[$. Both quantities of common and private data are represented by real positive numbers, since IoT data have a high volume. They can be measured in terabytes. Data can be monetized and will be measured in US $.

3.1 A real case: the industry of smart cars with a unique manufacturer

To boost our model, we discuss the case of the traditional industrial sector endowed with IoT technologies. In the last several years, the phenomenon of smart vehicles has exploded due to the technology of Internet of Things (Peters, Chun, & Lanza, 2015). In smart cars, devices are devoted

to regulate relationships between vehicles and road infrastructures, between vehicles, between vehicles and pedestrians. Most data are aimed at the safety or maintenance of cars. Collaborative technological networks are emerging in the new automotive manufacturing sector with IoT technologies (Markendahl, Lundberg, Kordas, & Movin, 2017). New technological companies entered IoT business forming partnership with traditional car manufacturers to share risk and uncertainty. For instance, the giant Apple launched a project and listed its collaboration with many car manufacturers: BMW, Ford, GM, Honda, Hyundai, Jaguar Land Rover, KIA, Mitsubishi, Nissan, PSA Peugeot Citroen, Subaru, Suzuki and Toyota. Business structures of those industrial collaborations are quite fragmented and are based on initial and flexible partnership. For instance, the Car Connectivity ConsortiumÂő (CCC) is a cross-industry organisation advancing global technologies for smartphone-to-car connectivity solutions. It includes big companies as Apple and Samsung.

Car manufacturers provide customised services to drivers. For instance, CCC is developing Digital Key, an exciting new open standard to allow smart devices, like smartphones to act as a vehicle key. Digital Key will let drivers lock and unlock their cars, and even let them start the engine and share access to friends or valets, using their phones. Mobiles are integrated in IoT data-architectures, by increasing the exposure level of users' privacy. Biometric solutions for motorised vehicles are also the source of privacy concerns since personal data could be used by insurance companies (Villa, Gofman, & Mitra, 2018), (Iqbal & Lim, 2006). For instance, Xpeng Motors in conjunction with electronics company Xiaomi, launched a car model G3 electric SUV, including facial recognition door access. In autonomous driving projects, automated GPS-based surveillance may create serious concerns for privacy and, specially, connected problems related to tracking activities and profiling, including home addresses and social and work activities (Iqbal & Lim, 2010), (Seif & Hu, 2016). There are numerous firms working in the area of autonomous vehicle: the most advanced ones include Waymo, GM Cruise and Argo AI. As such, services may pose a threat to users' privacy.

4 A cooperative approach

In this Section, our main aim is to provide fair measures of firms' accountability to privacy: these measures will be, meaningfully, used to build penalties for firms in the Section 5. To build these measures, we need two essential steps described as it follows: (1) to construct a special class of cooperative game: transferable utility games with characteristic functions; (2) to obtain measures through allocation rules of cooperative models.

4.1 A transferable utility game

Before doing this, we need to formally clarify what a transferable utility game is. A transferable utility game in characteristic form is a pair (N, ν) where N is a finite set and $\nu : P(N) \to \mathbb{R}$, where $P(N) = 2^N$ is the superset of N. [2] The quantity $\nu(T)$ represents the *quantified* degree of cooperation of players in $T \subseteq N$. Let $T \subseteq N$ be a subset of firms. Suppose that firms in T cooperate in integrating, sharing private data. It is assumed that only firms belonging to T share private data. We clarify the conceptual meaning of a fundamental quantity for our analysis.

Definition 1. *Let M^T_{priv} the sum of quantities of private data owned by firms in T. The Privacy Value for a coalition T is the value of private data M^T_{priv}, after some data being shared among firms in T or/and integrated with data from different IoT sources. If $T = N$, we simply call it privacy value.*

In order to understand how privacy values are structured, we can make assumptions on the effect of data sharing and integration on data value. In particular, we define coefficients which regulate the increase from the original value of M^T_{priv} to the privacy value within a coalition T. It is given for granted that firms in T might use links in the whole E for the sake of data transmission.

[2] $v(\emptyset) = 0$.

[3] After a clarification on what cooperation means in our settings, we define coefficients that shape the increase of privacy values.

Definition 2. *Let N the set of players (firms) and E a set of links between players. We represent the unitary increase rate of value of M^T_{priv}, through a function*

$$\lambda^E : P(N) \to \mathbb{R}^+,$$

which satisfies the following axioms:

- $\lambda^E(T) = 0$ *if T contains isolated firms in T, i.e. $E_{|T} = \emptyset$.*
- *If $T_1 \subseteq T_2 \subseteq N$, then $\lambda^E(T_1) \leq \lambda^E(T_2)$.*
- *Let $T \subseteq N$ and E, E' be two sets of links between palyers such that $E \subseteq E'$. Then $\lambda^E(T) \leq \lambda^{E'}(T)$.*

If $\lambda^E(T) = 0$, then private data sharing do not increase users' value of private data. The first axiom says that the rate is 0, if firms in T are not neighbours. The second axiom says the following: the rate increases if we add some players to the coalition T. The third axiom says that the rate increases if the number of internal links in T increases.

In the following, for simplicity and whenever this does not create confusion, we will simply indicate λ^E as λ.

Among coefficients satisfying those axioms, the simplest expression is the following:

$$\lambda_a(T) = 2|E_{|T}|.$$

A normalised readjusting term, which takes into account the size of the coalition, multiplies the previous coefficient, as it follows

$$\lambda_f(T) = 2\frac{|T|}{n}|E_{|T}|.$$

Privacy values depend on how private data are originally distributed among firms, after their collections. In other words, privacy values depend on data ownership before being shared and integrated among them. It is also reasonable to assume that privacy values decrease if data are scattered among different firms. The more data ownership is spread among firms, the less the privacy value becomes. To better formalise, we say that an ownership distribution of private data in N is a function $s : N \to \mathbb{R}^+$, which assign to firms the quantity of private data possessed by firms. The support of data distribution is the following integer: $supp(s) = |\{i \in N | s_i \neq 0\}|$. The worth of a coalition $\nu(T)$ will be the privacy value for coalition T divided by the support of the restricted data distribution function $s_{|T} : N \to \mathbb{R}^+$.

4.2 The Shapley value

To find fair measures of accountability against privacy value is the next step. The technique used here is to build these accountability measures, as an outcome of allocation rules for transferable utility games. Before proceeding further, we specify the allocation rule used throughout this paper: the Shapley value. The Shapley value addresses an aggregation question: How to summarise information from TU games into single payoffs assigned to each of the players? Shapley proposes a solution to this question, which is based on the simple fact of defining an axiomatic *value* for each participant involved in the game. Such an individual value is the so-called Shapley value. Shapley

[3] The cooperation among firms in T does not embody the classical "connectedness" of T, i.e., the capability of transmitting data between firms in T, only through links in $E_{|T}$. The graph induced on E by T is $E_{|T}$. To cover this aspect through a cooperative approach, we should take into consideration only connected coalitions. Differently in the current paper, we take into consideration only firms' contributions to share and/or integrate data on networks.

succeeded in providing four conditions on the transformation from a TU-game into an allocation that can be fairly said to be natural. The first is the symmetry axiom: if two participants equally contribute to the worth of any coalition, i.e. $\nu(T)$, then they must have the same Shapley value. The second is the efficiency axiom: the sum of individual Shapley values must be equal to the worth of the whole grand coalition. The third is the dummy-player axiom. A participant who does not contribute to any coalition must have a null value. A fourth axiom is the additivity axiom (the most debated one). Let us have two TU games on the same set of players. For each TU game, each player has a Shapley value. Let us construct the sum-game of the previous two games. Then, individual Shapley values of sum game are equal to the sum of the two initial Shapley values. Actually, some of those axioms can be considered quite compelling, from the point of view of the standard interpretation of cooperative games. Such a value is unique and can be formulated for a TU game (N, ν) as it follows:

$$Sh_i(N,\nu) = \sum_{T \subseteq N \setminus \{i\}} W(|T|, n) \left(\nu(T \cup \{i\}) - \nu(T)\right),$$

where

$$W(\tau, n) = \frac{\tau!(n-\tau-1)!}{n!}.$$

In (Moretti & Patrone, 2008), the authors describe how wide is the scientific domain that has been investigated using the Shapley value and related refinements: cost allocation, social networks, water-focused issues, biology, reliability theory, belief formation, centrality theory.

4.3 Results

We have clarified the cooperative approach to the model and we have clarified the role of the Shapley value as a fair individual measure for privacy accountability. We are ready to apply our conceptual scheme to two business scenarios. The two scenarios differ because of a key issue in IoT ecosystems: data ownership. Our scenarios are similar to the ones described in (**?**): a vertical and a horizontal models for IoT business models.

4.4 Scenario A.

Each firm collects private data from different sensors and devices. This data are different. The data collected potentially contain sensitive consumer data and can be classified as private data. The amount of private data collected from each firm is $m_{priv} \geq 0$. The ownership distribution of private data is the function: $s(i) = m_{priv}$, with $supp(s) = N$. The quantity of private data within coalition T is equal to $|T|m_{priv}$. The increase of original value is $\lambda(T, s)|T|m_{priv}$. The privacy value for T is the sum of the two previous terms. It is straightforward to see that $s|_T(i) = m_{priv}$ and $supp(s|_T) = |T|$. We define our characteristic function as the ratio of privacy values and the support of data distribution on T. The TU game (N, ν) is represented as it follows:

$$\nu(T) = \begin{cases} \dfrac{[1+\lambda(T)]\, m_{priv}|T|}{supp(s_{|T})} & \text{if } T \neq \emptyset, \\ \\ 0 & \text{if } T = \emptyset. \end{cases} \tag{1}$$

We build two transferable utility games by replacing the rate $\lambda(T)$ with λ_a, λ_f, respectively.

Theorem 1. *Let $\nu = \nu_a$, where*

$$\nu_a(T) = \begin{cases} \left[1 + 2|E_{|T}|\right] m_{priv} & \text{if } T \neq \emptyset, \\ \\ 0 & \text{if } T = \emptyset. \end{cases} \tag{2}$$

Then

$$Sh_i(N, \nu_a) = \left(d_i + \frac{1}{n}\right) m_{priv}. \tag{3}$$

Theorem 2. *Let $\nu = \nu_f$, where*

$$\nu_f(T) = \begin{cases} \left[1 + 2\dfrac{|T||E_{|T}|}{n}\right] m_{priv} & \text{if } T \neq \emptyset, \\ 0 & \text{if } T = \emptyset. \end{cases} \tag{4}$$

Then

$$Sh_i(N, \nu_f) = \left(\frac{2}{3}d_i + \frac{2}{3n}|E| + \frac{1}{n}\right) m_{priv}. \tag{5}$$

4.5 Scenario B

The manufacturer collects private and common data provided by a set C of consumers. The

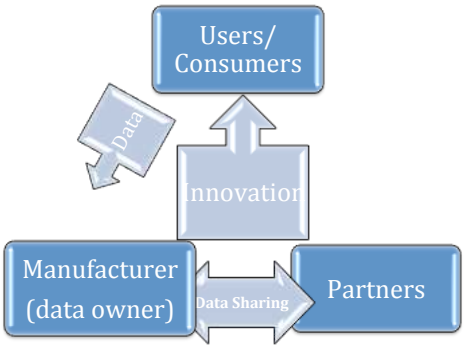

Figure 1. Scenario B. Three actors are present in IoT business ecosystems. The manufacturer collects data from users. The manufacturer with its technological partners provide innovation to users. Users give away their data to the manufacturer. Scenario B describes the case of data ownership in the industry of smart cars.

special relationship of the manufacturers with the remaining actors is illustrated in Fig.1. For the sake of simplicity, the manufacturer is the firm denoted by $i = 1$. The amount of private information collected by $i = 1$ is $m_{priv} \geq 0$. The ownership distribution of private data is, then, $s(i) = m_{priv}$ for $i = 1$; 0 otherwise. Its support is 1. The amount of public information, collected by $i = 1$, is $M_{comm} \geq 0$. If the manufacturer does not share data with peers in the network, the privacy values thus collected are

$$\nu(\{1\}) = m_{priv} + \beta M_{comm}, \quad \nu(\{i\}) = 0$$

where $0 \leq \beta < 1$, $i \neq 1$. The manufacturer shares collected data with some or all components of the network. Let $T \subseteq N$. If $1 \notin T$ then the companies that are in T have no data from C. If $1 \in T$ then firms that are in T acquire both private and public data from the manufacturer. In particular, each firm in T acquire the quantity of m_{priv}. Data values for coalition T increase by the rate $\lambda(T)$. We define the worth of a coalition T as the ratio between privacy values and supports of data distribution on T. Then, the worth of coalition T becomes equal to

$$\nu(T) = \frac{m_{priv} + \lambda(T) m_{priv}}{supp(s|_T)} + \beta M_{comm}.$$

Summing up those considerations, we define the TU cooperative game (N, ν) where the characteristic function ν is defined by

$$\nu(T) = \begin{cases} [1 + \lambda(T)]\, m_{priv} + \beta M_{comm} & \text{if } 1 \in T, \\ 0 & \text{if } 1 \notin T. \end{cases} \tag{6}$$

Let $C_1 = \{i \in N | (1, i) \in E \; i = 2, ..., n\}$ be the subset of firms connected to the manufacturer.

Theorem 3. *Let $\nu = \nu_a$, where*

$$\nu_a(T) = \begin{cases} \left(1 + 2|E_{|T}|\right) m_{priv} + \beta M_{comm} & \text{if } 1 \in T, \\ 0 & \text{if } 1 \notin T. \end{cases} \tag{7}$$

It is

$$Sh_1(N, \nu_a) = \left(1 + \frac{1}{3} d_1 + \frac{2}{3}|E|\right) m_{priv} + \beta M_{comm}. \tag{8}$$

Let $k \in N$ with $k \neq 1$. If $k \in C_1$, then

$$Sh_k(N, \nu_a) = \left(\frac{2}{3} d_k + \frac{1}{3}\right) m_{priv}. \tag{9}$$

Let $k \in N$ with $k \neq 1$. If $k \notin C_1$, then

$$Sh_k(N, \nu_a) = \frac{2}{3} d_k m_{priv}. \tag{10}$$

Theorem 4. *Let $\nu = \nu_f$, where*

$$\nu_f(T) = \begin{cases} \left[1 + 2\dfrac{|T||E_{|T}|}{n}\right] m_{priv} + \beta M_{comm} & \text{if } 1 \in T, \\ 0 & \text{if } 1 \notin T. \end{cases} \tag{11}$$

It is

$$Sh_1(N, \nu_f) = \left(\frac{n+1}{6n} d_1 + \frac{n+1}{2n}|E| + 1\right) m_{priv} + \beta M_{comm}. \tag{12}$$

Let $k \in N$ con $k \neq 1$. If $k \in C_1$, then

$$Sh_k(N, \nu_f) = \left(\frac{1}{6n} d_1 + \frac{1}{2} d_k + \frac{1}{2n}|E| + \frac{1}{6}\right) m_{priv}. \tag{13}$$

Let $k \in N$ with $k \neq 1$. If $k \notin C_1$, then

$$Sh_k(N, \nu_f) = \left(\frac{1}{6n} d_1 + \frac{1}{2} d_k + \frac{1}{2n}|E|\right) m_{priv}. \tag{14}$$

5 Penalties

IoT companies may be involved in cases of privacy infringement. A data breach is a disruptive event in which part of data are stolen, or used for not authorised purposes. Data, that have been affected by a breach, somehow, are referred to as *leaked data*. We adopt EU as legal authority and GDPR for infringement of privacy. Investigations by Data Protection Authorities may find the infringement of privacy regulations. Since data (originally in the hands of a specific data controller) may be in possess of any firm (after data sharing), then each firm can be found guilty of privacy laws' infringements. However, EU Data Protection Authorities fine only data controllers if there is an infringement.[4] Data controllers are the firms who, after collecting users' data, are also responsible of data processing from third parties. Therefore, our penalties establish the total amount of the fine. Our penalties enforce a corporate spirit of responsibility for data breaches and divides the fine among the whole set of firms. How to divide the whole fine among firms? Each firm is sanctioned proportionally to its fair measure against the privacy value. These proportional fair measures are given by firms' Shapley values. In addition, Shapley values and, then, individual penalties change if networks have specific topologies.

Innovation networks involve the interchange of people, ideas and organizations to create new, technologically and commercially feasible products, and organizational structures. The complexity of such interactions among IoT firms might be framed into a general framework for innovation proposed in (Ahrweiler & Keane, 2013). However, empirical results show differences in the topology of networks formed by firms in knowledge-intensive sectors (Salavisa, Sousa, & Fontes, 2012). For instance, scaling behavior exhibited by US patent networks is consistent with a preferential attachment mechanism(Valverde, Solé, Bedau, & Packard, 2007). It is challenging to a priori define stereotypical topologies for innovation networks, especially in emerging IoT business models. On the top of these considerations, Data Protection Authorities may find cumbersome to access to the knowledge of IoT ecosystems and, within realistic assumptions, may have a partial knowledge of these technological infrastructures. For the sake of showing examples of our penalties, we limit our attention to some regular networks. From now onwards, we select linear, circular and star-shaped networks for our analysis. A linear network is characterised by the following topology: $d_1 = d_n = 1$, $d_2 = ..., d_{n-1} = 2$ and $|E| = n - 1$ for n firms. Firm 1 is the manufacturer in the linear model. In star-shaped networks, the manufacturer is connected to any firm. The topological parameters are the the following: $d_1 = n-1$, $d_i = 1$ for $i = 2, ..., n$ and $|E| = n-1$. A circular network assumes the geometrical shape of a circle and its topological parameters are the following: $d_i = 2$ for $i = 1, ..., n$ and $|E| = n$. However, some supporting considerations on the selected topologies can be underlined. Linear networks are classic in the literature of supply chains; a mixture of strong and weak ties in the shape of star-shaped networks show reinforcing properties for some Italian innovation networks with a leading firm (Capaldo, 2007); circular networks are emergent in the field of a new production paradigm, the so-called circular economy.

In scenario A, each firm collects private data and, then, is the data controller of his own private data. We define the following penalties if breaches involve a certain quantity of private data.

Definition 3. *Assume M_{priv}^{leak} being leaked. We define the function*

$$\nu^{leak} : x \in [0, M_{priv}] \to [1 + 2|E|]\, x.$$

A vector $\mathbf{x} \in R^n$ is a penalty scheme if

$$\mathbf{x} = \frac{\nu^{leak}(M_{priv}^{leak})}{\nu(N)}\mathbf{y}$$

[4] EU Commission includes a proposal for consumer organisations to bring collective class-style actions on behalf of users. Fines are decided by the privacy authority on case-by-case basis. Fines can be reckoned according to the negative impact on users. Users may claim that data collected have been treated not in compliance with GDPR. The following website https://www.enforcementtracker.com/ contains a list and overview of fines which Data Protection Authorities have imposed under EU General Data Protection Regulation.

where $y_i = Sh_i(N, \nu)$.

Here, we deduce the specific formulations of Shapley values, if business scenario A is the adopted one for IoT data ownership.

Corollary 1 (Scenario A)**.**

– *A linear network.*

$$\begin{aligned} Sh_i(N,\nu_a) &= \left(1+\frac{1}{n}\right) m_{priv} \quad \text{if } i = 1, n; \\ Sh_i(N,\nu_a) &= \left(2+\frac{1}{n}\right) m_{priv} \quad \text{if } i = 2, ..., n-1; \end{aligned}$$

$$\begin{aligned} Sh_i(N,\nu_f) &= \left(\frac{4}{3}+\frac{1}{3n}\right) m_{priv} \quad \text{if } i = 1, n; \\ Sh_i(N,\nu_f) &= \left(2+\frac{1}{3n}\right) m_{priv} \quad \text{if } i = 2, ..., n-1; \end{aligned}$$

– *A circular network.*

$$Sh_i(N,\nu_a) = Sh_i(N,\nu_f) = 2+\frac{1}{n}, \quad i = 1, n;$$

– *A star-shaped network.*

$$\begin{aligned} Sh_1(N,\nu_a) &= \left(n-1+\frac{1}{n}\right) m_{priv}; \\ Sh_k(N,\nu_a) &= \left(1+\frac{1}{n}\right) m_{priv}; \qquad \text{if } k = 2, ..., n. \\ Sh_1(N,\nu_f) &= \left(\frac{2n}{3}+\frac{1}{3n}\right) m_{priv}; \\ Sh_k(N,\nu_f) &= \left(\frac{4}{3}+\frac{1}{3n}\right) m_{priv}; \quad \text{if } k = 2, ..., n. \end{aligned}$$

We show a potential example for business scenario A.

Example 1. *Each firm collects* $m_{priv} = 300,000$ *from users. Its value is* $300,000$\$. *Assume that the amount of leaked private data is* $400,000$. (N, E) *is a linear network with* $n = 5$. *We assume that the characteristic function used to compute the Shapley values is* ν_a*, which has been defined in (2). The Shapley values are*

$$\begin{aligned} Sh_i(N,\nu_a) &= 360,000; \quad i = 1, 5 \\ Sh_i(N,\nu_a) &= 660,000 \quad i = 2, 3, 4. \end{aligned}$$

The penalty is equal to $3,600,000$ *\$. It is shared among the firms as it follows:*

$$x_1 = x_5 = 480,000\$ \quad x_2 = x_3 = x_4 = 880,000\$$$

We assume that the characteristic function used to compute the Shapley values is ν_f, which has been defined in (4). The penalty is equal to $3,600,000$ *\$.*

$$\begin{aligned} Sh_i(N,\nu_f) &= \tfrac{7}{5}\, m_{priv} \quad i=1,5; \\ Sh_i(N,\nu_f) &= \tfrac{31}{15}\, m_{priv} \quad i=2,3,4; \end{aligned}$$

It is shared among the firms as it follows:

$$x_1 = x_5 = 560,000\$; \quad x_2 = x_3 = x_4 = 826,666.66\$.$$

The manufacturer collects data from users in scenario B. The data controller/data holder is the manufacturer within General Data Protection Regulation (GDPR). The manufacturer is, then, the responsible of data handling. If data are a mixture of common and private data, then we say that data are mixed. Assume that leaked data are mixed, then we have the following definition of penalties.

Definition 4. *We define the function*

$$\nu^{leak} : (x,y) \in [0, m_{priv}] \times [0, M_{comm}] \to [1 + 2|E|]\, x + \beta y.$$

Assume that the quantity $M^{leak}_{priv} + M^{leak}_{comm}$ has been leaked. A vector $\mathbf{x} \in R^n$ is a penalty scheme if

$$\mathbf{x} = \frac{\nu^{leak}(m^{leak}_{priv}, M^{leak}_{comm})}{\nu(N)}\mathbf{y}$$

where $y_i = Sh_i(N,\nu)$.

Here, we formulate the expressions of Shapley values if the business scenario B is the adopted one for IoT data ownership.

Corollary 2 (Scenario B)**.**

– *A linear network. $n \geq 3$*

$$\begin{aligned} Sh_1(N,\nu_a) &= \left(\frac{2n}{3} + \frac{2}{3}\right) m_{priv} + \beta M_{comm}; \\ Sh_2(N,\nu_a) &= \frac{5}{3} m_{priv}; \\ Sh_k(N,\nu_a) &= \frac{4}{3} m_{priv}; \qquad\qquad \text{if } k = 3, ..., n-1; \\ Sh_n(N,\nu_a) &= \frac{2}{3} m_{priv}. \end{aligned}$$

$$
\begin{aligned}
Sh_1(N,\nu_f) &= \left(\frac{n}{2}+\frac{7}{6}-\frac{1}{3n}\right)m_{priv}+\beta M_{comm};\\
Sh_2(N,\nu_f) &= \left(\frac{5}{3}-\frac{1}{3n}\right)m_{priv};\\
Sh_k(N,\nu_f) &= \left(\frac{3}{2}-\frac{1}{3n}\right)m_{priv}; \qquad\qquad \text{if } k=3,...,n-1;\\
Sh_n(N,\nu_f) &= \left(1-\frac{1}{3n}\right)m_{priv}.
\end{aligned}
$$

– *A circular network.*

$$
\begin{aligned}
Sh_1(N,\nu_a) &= \left(\frac{2n}{3}+\frac{5}{3}\right)m_{priv}+\beta M_{comm};\\
Sh_k(N,\nu_a) &= \frac{5}{3}m_{priv}; \qquad\qquad \text{if } k=2,n;\\
Sh_k(N,\nu_a) &= \frac{4}{3}m_{priv}; \qquad\qquad \text{if } k=3,...,n-1.
\end{aligned}
$$

$$
\begin{aligned}
Sh_1(N,\nu_f) &= \left(\frac{n}{2}+\frac{11}{6}+\frac{1}{3n}\right)m_{priv}+\beta M_{comm};\\
Sh_k(N,\nu_f) &= \left(\frac{5}{3}+\frac{1}{3n}\right)m_{priv}; \qquad\qquad \text{if } k=2,n;\\
Sh_k(N,\nu_f) &= \left(\frac{3}{2}+\frac{1}{3n}\right)m_{priv}; \qquad\qquad \text{if } k=3,...,n-1.
\end{aligned}
$$

– *A star-shaped network.*

$$
\begin{aligned}
Sh_1(N,\nu_a) &= nm_{priv}+\beta M_{comm};\\
Sh_k(N,\nu_a) &= m_{priv}; \qquad\qquad \text{if } k=2,...,n.\\
Sh_1(N,\nu_f) &= \left(\frac{2n}{3}+1-\frac{2}{3n}\right)m_{priv}+\beta M_{comm};\\
Sh_k(N,\nu_f) &= \left(\frac{4}{3}-\frac{2}{3n}\right)m_{priv}; \qquad\qquad \text{if } k=2,...,n.
\end{aligned}
$$

In scenario B, our penalties are useful since other firms contribute to fines and mitigate the risk sustained by a single firm, e.g. the manufacturer. We show a potential example of infringement of privacy laws for the scenario B.

Example 2. *Assume that only the manufacturer collects data and shares them with the remaining firms. Assume that* (N,E) *is a circular network and* $n=5$*. Common and private data are* $M_{comm}=1,000,000$ *and* $m_{priv}=300,000$*, respectively. The whole quantity of common and private data are*

leaked. The total cost of common and private data is $800,000$\$ *since* $\beta = 0.5$. *Assume that the characteristic function is* ν_a *defined in (7). It is* $\nu^{leak}(m^{leak}_{priv}, M^{leak}_{comm}) = 3,800,000$. *According to GDPR, the manufacturer is fined the amount* $3,800,000$ *\$. However, our penalties try to mitigate the fine's impact on the manufacturer. Our penalties prescribe the following payments for the whole set of firms:*

$$\begin{aligned} x_1 = Sh_1(N, \nu_a) &= 2,000,000\$; \\ x_2 = x_5 = Sh_2(N, \nu_a) = Sh_5(N, \nu_a) &= 500,000\$; \\ x_3 = x_4 = Sh_3(N, \nu_a) = Sh_4(N, \nu_a) &= 400,000\$. \end{aligned}$$

Conversely, we assume that the characteristic function is ν_f. Then, our penalties prescribe the following payments:

$$\begin{aligned} x_1 = Sh_1(N, \nu_f) &= 1,820,000\$; \\ x_2 = x_5 = Sh_2(N, \nu_f) = Sh_5(N, \nu_f) &= 520,000\$; \\ x_3 = x_4 = Sh_3(N, \nu_f) = Sh_4(N, \nu_f) &= 470,000\$. \end{aligned}$$

Conclusions and Future research

Firms in IoT industries must be accountable for handling data. Some IoT data are common and associated privacy is hidden; some data are more explicit about private or personal details. We propose two penalty schemes to be applied on firms. Penalties can be applied if there is an infringement or violation of privacy rights. Penalties are fair and take into account different privacy value of data. Our penalties redistribute fines' monetary amount among partners, including the manufacturer. In case the manufacturer is the unique data owner, our penalty schemes represent an incentive for the manufacturer to share data with its partners. In this case, the manufacturer mitigate its individual risk for a potential data breach. Penalty schemes represent an incentive for partners to protect data since they become accountable for potential data breaches.

Future privacy models might take into account asymmetric endowments of data for firms in IoT ecosystems. However, this may bring in severe difficulties to compute penalties. A simulation approach to the computation of Shapley values is needed for such investigation. Penalties might incorporate a feedback from consumers's side if data breaches happen. For example, DPA might impose penalties taking into account users' evaluation of product innovation, lastly provided by the manufacturer. The latter should determine the lowering of penalties for firms. Cooperative game theory might suggest different allocation rules, in order to study penalties. The Shapley value gained its reputation for its fairness. However, the nucleolus, that takes into account objections and counter-objections, might prevent firms' data breach litigations.

Acknowledgements

The authors thank two anonymous referees who helped us to improve the current paper. The authors thank Antonio Capaldo, Andrea Genovese, Diego Ruiz-Hernandez, Ines Macho-Stadler, Antonino Sgalambro and Philippe Solal for discussions across multiple disciplines: hazard/risk evaluation, innovation networks, production systems/supply chains and, of course, cooperative game theory.

Conflict of Interests

The authors declare that there are no conflict of interest.

Appendix

Proof of Theorem 1

Proof. It straightforwardly follows from Theorem 1 in (Deng & Papadimitriou, 1994). □

Note that $\nu = \nu_1 + \nu_2$, where ν is defined in (1) and

$$\nu_1(T) = \begin{cases} \lambda(T, E_{|T}) m_{priv} & \text{if } T \neq \emptyset, \\ 0 & \text{if } T = \emptyset. \end{cases} \tag{A. 1}$$

$$\nu_2(T) = \begin{cases} m_{priv} & \text{if } T \neq \emptyset, \\ 0 & \text{if } T = \emptyset. \end{cases} \tag{A. 2}$$

For the additivity property of the Shapley value, it is

$$Sh_i(N; \nu) = Sh_i(N; \nu_1) + Sh_i(N; \nu_2); \quad i = 1, ..., n.$$

Lemma 1. *It is*

$$Sh_i(N; \nu_2) = \frac{m_{priv}}{n}. \tag{A. 3}$$

Proof. Let $T \subseteq N$ such that $i \notin T$. If $T \neq \emptyset$, then $\nu_2(T \cup \{i\}) - \nu_2(T) = 0$. If $T = \emptyset$ then $\nu_2(T \cup \{i\}) - \nu_2(T) = m_{priv}$. It is

$$Sh_i(N; \nu_2) = W(0, n) m_{priv} = \frac{m_{priv}}{n}.$$

□

Lemma 2. *Let*

$$\lambda(T, E_{|T}) = 2\frac{|T||E_{|T}|}{n}.$$

Then

$$Sh_i(N; \nu_1) = \frac{2}{3} m_{priv} d_i + \gamma |E|, \tag{A. 4}$$

where

$$\gamma := \frac{2 m_{priv}}{3n}.$$

Proof. Let us consider $e \in E$ connecting agents i and j. We say that $e \in g(T)$ if $i \in T$ and $j \in T$, where $T \subseteq N$. We define the following function $\nu_e : 2^N \to \mathbb{R}$,

$$\nu_e(T) = \begin{cases} 2\,\frac{|T|\, m_{priv}}{n} & \text{if } e \in g(T); \\ 0 & \text{if } e \notin g(T). \end{cases} \tag{A. 5}$$

Let $G_e = (N, v_e)$ the finite family of TU-games on N with characteristic function ν_e.
Let $T \subseteq N$. It is

$$\sum_{e \in E} \nu_e(T) = \sum_{e \in g(T)} \frac{2|T|}{n}\, m_{priv} = \frac{2|E_{|T}||T|}{n} m_{priv} = \nu_1(T),$$

where ν_1 is defined by (A. 1).
Therefore, it is

$$\sum_{e \in E} \nu_e = \nu_1.$$

1. Let us consider the game $G_e = (N, v_e)$, where $e = (i, j)$, $i, j \in N$.

   (a) Nodes i and j are symmetric with respect to the game G_e.
   In fact, suppose that a coalition T does not include i, j. By definition of ν_e, it follows $v_e(T \cup \{i\}) = v_e(T \cup \{j\}) = 0$.

   (b) Let $s, t \in N \setminus \{i, j\}$. Suppose that a coalition T does not include s, t. By definition of ν_e, the following is true.

   - If $e \in g(T)$ then $e \in g(T \cup \{s\})$ and $e \in g(T \cup \{t\})$. Moreover $|T \cup \{s\}| = |T \cup \{t\}| = |T| + 1$. Hence

   $$v_e(T \cup \{s\}) = v_e(T \cup \{t\}) = 2\,\frac{(|T|+1)\,m_{priv}}{n}.$$

   - If $e \notin g(T)$ then $e \notin g(T \cup \{s\})$ and $e \notin g(T \cup \{t\})$. Hence $v_e(T \cup \{s\}) = v_e(T \cup \{t\}) = 0$.

   It follows that players s and t are symmetric.

   Since the Shapley value satisfies the symmetry properties, we have

   $$Sh_i(N, \nu_e) = Sh_j(N, \nu_e) := \rho_e \quad Sh_s(N, \nu_e) = \gamma_e \qquad \forall s \in N,\ s \neq i,\ s \neq j.$$

2. Here, we compute the Shapley value of each game $G_e = (N, v_e)$, $e = (i, j) \in E$ for players different from i and j.

   Let $k \in N$, $k \neq i$, $k \neq j$. By definition, it is

   $$\gamma_e = Sh_k(N, \nu_e) = \sum_{T \subseteq N \setminus \{k\}} W(|T|, n)\,[\nu_e(T \cup \{k\}) - \nu_e(T)]\,, \tag{A. 6}$$

   where

   $$W(|T|, n) = \frac{|T|!(n - |T| - 1)!}{n!}.$$

   It is

   $$\gamma_e = W(n-1, n)\,[\nu_e(N) - \nu_e(N \setminus \{k\})] + \overline{\gamma}_e,$$

   where [5]

   $$\overline{\gamma}_e = \sum_{\substack{|T|=2 \\ T \subseteq N \setminus \{k\}}}^{n-2} W(|T|, n)\,[\nu_e(T \cup \{k\}) - \nu_e(T)]\,.$$

   It is

   $$W(n-1, n)\,[\nu_e(N) - \nu_e(N \setminus \{k\})] = \frac{1}{n}\,[\nu_e(N) - \nu_e(N \setminus \{k\})] = \frac{2}{n^2} m_{priv}.$$

   Let T be a coalition such that $2 \leq |T| \leq n - 2$ and $k \notin T$.

   - If $e = (i, j) \in g(T)$, then

   $$[\nu_e(T \cup \{k\}) - \nu_e(T)] = 2\,\frac{(|T|+1)\,m_{priv}}{n} - 2\,\frac{(|T|)\,m_{priv}}{n} = \frac{2\,m_{priv}}{n}.$$

   - If $e = (i, j) \notin g(T)$, then

   $$[\nu_e(T \cup \{k\}) - \nu_e(T)] = 0.$$

[5] Note that if T is a single player coalition, then $e \notin g(T)$ and $e \notin g(T \cup k)$. It follows that $\nu_e(T) = \nu_e(T \cup \{k\}) = 0$. Consequently, the contribution of single player coalition in the sum (A. 6) is null.

It follows that

$$\overline{\gamma}_e = \sum_{\substack{|T|=2 \\ k\notin T;\ e\in g(T)}}^{n-2} W(|T|,n)\left[\nu_e(T\cup\{k\}) - \nu_e(T)\right] = \sum_{\substack{|T|=2 \\ k\notin T;\ e\in g(T)}}^{n-2} W(|T|,n)\frac{2\,m_{priv}}{n},$$

so that

$$\overline{\gamma}_e = \frac{2\,m_{priv}}{n} \sum_{\substack{|T|=2 \\ k\notin T;\ e\in g(T)}}^{n-2} W(|T|,n).$$

The number of coalitions T such that $|T|=\tau$, $k\notin T; i\in T; j\in T$ is $\binom{n-3}{\tau-2}$. Consequently

$$\overline{\gamma}_e = \frac{2\,m_{priv}}{n}\sum_{\tau=2}^{n-2}\binom{n-3}{\tau-2}W(\tau,n),$$

or

$$\overline{\gamma}_e = \frac{2\,m_{priv}}{n}\sum_{\tau=2}^{n-2}\frac{(n-3)!}{(\tau-2)!(n-\tau-1)!}\frac{\tau!(n-\tau-1)!}{n!}.$$

It is

$$\sum_{\tau=2}^{n-2}\frac{(n-3)!}{(\tau-2)!(n-\tau-1)!}\frac{\tau!(n-\tau-1)!}{n!} = \frac{1}{n(n-1)(n-2)}\sum_{\tau=2}^{n-2}\tau(\tau-1) = \frac{n-3}{3n}.$$

Then, it is

$$\overline{\gamma}_e = \frac{2(n-3)}{3n^2}m_{priv}.$$

We conclude that

$$\gamma_e = \frac{2}{n^2}m_{priv} + \frac{2(n-3)}{3n^2}m_{priv},$$

or

$$\gamma_e = \frac{2}{3n}m_{priv}.$$

Note that γ_e does not depend on the specific edge e, hence definitively we set $\gamma = \gamma_e$.

3. Let $k\in N$. Let $E_k = \{e\in E | k \text{ is an endpoint of e}\}$. It is $|E_k| = d_k$. By additivity of the Shapley value, we have

$$Sh_k(N,\nu_1) = \sum_{e\in E} Sh_k(N,\nu_e) = \sum_{e\in E_k} Sh_k(N,\nu_e) + \sum_{e\in E\setminus E_k} Sh_k(N,\nu_e);$$

that is

$$Sh_k(N,\nu_1) = \sum_{e\in E_k}\rho_e + \sum_{e\in E\setminus E_k}\gamma = \sum_{e\in E_k}\rho_e + \gamma(|E|-d_k).$$

It is easy to verify that ρ_e does not depend on the specific edge e. We set $\rho := \rho_e$. It follows that

$$Sh_k(N,\nu_1) = d_k\rho + (|E|-d_k)\gamma.$$

The efficiency property of the Shapley value implies

$$\nu_1(N) = \sum_{k\in N} Sh_k(N,\nu) = \rho\sum_{k\in N} d_k + \left(|N||E| - \sum_{k\in N} d_k\right)\gamma.$$

Let us remember that $\sum_{k\in N} d_k = 2|E|$. It follows that

$$\nu_1(N) = 2|E|\rho + (n|E| - 2|E|)\,\gamma. \tag{A. 7}$$

Since $\nu_1(N) = 2|E|\ m_{priv}$ and $\gamma = \frac{2}{3n} m_{priv}$, substituting in (A. 7), we obtain

$$\rho = \frac{2(n+1)}{3n} m_{priv}.$$

It follows that

$$Sh_k(N,\nu_1) = d_k\rho + (|E| - d_k)\gamma = (\rho - \gamma)d_k + \gamma|E| = \frac{2}{3} m_{priv} + \gamma|E|.$$

□

Proof of Theorem 2

Proof. It follows from Lemma 1 and Lemma 2. □

Lemma 3.

$$Sh_1(N;\nu_2) = m_{priv} + \beta M_{comm},\ Sh_j(N;\nu_2) = 0 \ se\ j \neq 1. \tag{A. 8}$$

Proof. The proof is trivial. □

Lemma 4. *Let*

$$\nu_1(T) = \begin{cases} \lambda(T, E_{|T}) m_{priv} & \text{if } 1 \in T, \\ 0 & \text{if } 1 \notin T, \end{cases}$$

where

$$\lambda(T, E_{|T}) = 2|E_{|T}|.$$

In other words

$$\nu_1(T) = \begin{cases} 2|E_{|T}| m_{priv} & \text{if } 1 \in T, \\ 0 & \text{if } 1 \notin T. \end{cases}$$

Let

$$C_1 = \{k \in N | (1,k) \in E\}.$$

It is $\#(C_1) = d_1$. *Moreover*

- $$Sh_1(N;\nu_1) = \left(\frac{1}{3} d_1 + \frac{2}{3}|E|\right) m_{priv}. \tag{A. 9}$$
- *Let* $k \in N$ *and* $k \neq 1$. *If* $k \in C_1$, *then*

$$Sh_k(N;\nu_1) = \left(\frac{2}{3} d_k + + \frac{1}{3}\right) m_{priv}. \tag{A. 10}$$

- *Let $k \in N$ and $k \neq 1$. If $k \notin C_1$, then*

$$Sh_k(N;\nu_1) = \frac{2}{3} d_k m_{priv}. \tag{A. 11}$$

Proof. 1. Let us consider $e = (i,j) \in E$ an edge connecting agents i and j. We say that $e \in g(T)$ if $i \in T$ and $j \in T$, where $T \subseteq N$. We define the following function $\nu_e : 2^N \to \mathbb{R}$

$$\nu_e(T) = \begin{cases} 2m_{priv} & \text{if } e \in g(T) \text{ and } 1 \in T; \\ \\ 0 & \text{otherwise.} \end{cases} \tag{A. 12}$$

Let $G_e = (N, v_e)$ the finite family of TU-games on N with characteristic function ν_e.
Let $T \subseteq N$.

- Let $1 \in T$. Then

$$\sum_{e \in E} \nu_e(T) = \sum_{e \in g(T)} 2\ m_{priv} = 2|E_{|T}| m_{priv} = \nu_1(T).$$

- Let $1 \notin T$. Then

$$\sum_{e \in E} \nu_e(T) = 0 = \nu_1(T),$$

Therefore, it is

$$\sum_{e \in E} \nu_e = \nu_1.$$

2. (Computation of $Sh_1(\nu_e)$).

$$Sh_1(N, \nu_e) = \sum_{T \subseteq N \setminus \{1\}} W(|T|, n) \left[\nu_e(T \cup \{1\}) - \nu_e(T)\right], \tag{A. 13}$$

where

$$W(|T|, n) = \frac{|T|!(n - |T| - 1)!}{n!}.$$

Since $1 \notin T$ implies $\nu_e(T) = 0$, we have

$$Sh_1(N, \nu_e) = \sum_{T \subseteq N \setminus \{1\}} W(|T|, n) \nu_e(T \cup \{1\}).$$

(a) Let $e = (i,j)$ with $i \neq 1$ and $j \neq 1$. It is

$$e \in g(T \cup \{1\}) \iff e \in g(T).$$

If $e \in g(T)$, then

$$\nu_e(T \cup \{1\}) = 2m_{priv}.$$

Hence

$$Sh_1(N, \nu_e) = \sum_{T \subseteq N \setminus \{1\};\ i \in T;\ j \in T} W(|T|, n) 2m_{priv}.$$

Let $|T| = \tau$, $\tau = 2, ..., n-1$.

$$\#\left\{T \subseteq N | i \in T;\ j \in T;\ 1 \notin T; |T| = \tau\right\} = \binom{n-3}{\tau - 2}.$$

It follows that

$$Sh_1(N,\nu_e)=\sum_{\tau=2}^{n}W\tau,n)2\binom{n-3}{\tau-2}m_{priv},$$

that is

$$Sh_1(N,\nu_e)=\frac{2}{3}m_{priv}. \tag{A. 14}$$

(b) Let $e=(1,j)$ with $j\neq 1$.
Let $T\subseteq N$ with $1\notin T$.

- If $j\in T$ then

$$e\notin g(T);\quad e\in g(T\cup\{1\}),$$

so that

$$\nu_e(T\cup\{1\})=2m_{priv};\quad \nu_e(T)=0.$$

- If $j\notin T$ then

$$e\notin g(T);\quad e\notin g(T\cup\{1\}),$$

so that

$$\nu_e(T\cup\{1\})=\nu_e(T)=0.$$

Hence

$$Sh_1(N,\nu_e)=\sum_{T\subseteq N\setminus\{1\};\ j\in T}W(|T|,n)2m_{priv}.$$

Let $|T|=\tau$, $\tau=1,...,n-1$.

$$\#\{T\subseteq N|j\in T;\ 1\notin T;|T|=\tau\}=\binom{n-2}{\tau-1}.$$

It follows that

$$Sh_1(N,\nu_e)=\sum_{\tau=1}^{n-1}W\tau,n)2\binom{n-2}{\tau-1}m_{priv},$$

that is

$$Sh_1(N,\nu_e)=m_{priv}. \tag{A. 15}$$

3. (Computation of $Sh_1(\nu_1)$).
It is

$$Sh_1(N,\nu_1)=\sum_{e\in E}Sh_1(\nu_e)=\sum_{e=(i,j)\in E|i\neq 1;\ j\neq 1}Sh_1(\nu_e)+\sum_{e=(1,j)\in E|j\neq 1}Sh_1(\nu_e).$$

$$\#\{e=(i,j)\in E|i\neq 1;\ j\neq 1\}=|E|-d_1;\quad \#\{e=(1,j)\in E|j\neq 1\}=d_1.$$

From (A. 14) and (A. 15), it follows that

$$Sh_1(N,\nu_1)=(|E|-d_1)\frac{2}{3}m_{priv}+d_1m_{priv},$$

or

$$Sh_1(N;\nu_1)=\left(\frac{1}{3}d_1+\frac{2}{3}|E|\right)m_{priv}.$$

4. (Computation of $Sh_k(\nu_e);\ k \neq 1$).

$$Sh_k(N,\nu_e) = \sum_{T \subseteq N \setminus \{k\}} W(|T|,n)\left[\nu_e(T \cup \{k\}) - \nu_e(T)\right], \tag{A. 16}$$

where

$$W(|T|,n) = \frac{|T|!(n-|T|-1)!}{n!}.$$

If $1 \notin T$ then $1 \notin T \cup k$, so that

$$\nu_e(T \cup \{k\}) = \nu_e(T) = 0.$$

Hence

$$Sh_k(N,\nu_e) = \sum_{T \subseteq N \setminus \{k\};\ 1 \in T;\ e \in g(T)} W(|T|,n)\left[\nu_e(T \cup \{k\}) - \nu_e(T)\right],$$

(a) Let $e = (i,j)$ with $i \neq 1;\ j \neq 1;\ i \neq k;\ j \neq k$. It is

$$e \in g(T \cup \{k\}) \iff e \in g(T).$$

If $1 \in T$ and $e \in g(T)$, then

$$\nu_e(T \cup \{k\}) - \nu_e(T) = 2m_{priv} - 2m_{priv} = 0.$$

Hence

$$Sh_k(N,\nu_e) = 0.$$

(b) Let $e = (1,j)$ with $j \neq 1;\ j \neq k$.
It is

$$e \in g(T \cup \{k\}) \iff e \in g(T).$$

If $1 \in T$ and $e \in g(T)$, then

$$\nu_e(T \cup \{k\}) - \nu_e(T) = 2m_{priv} - 2m_{priv} = 0.$$

Hence

$$Sh_k(N,\nu_e) = 0.$$

(c) Let $e = (k,j)$ with $j \neq 1;\ j \neq k$. Remember that

$$Sh_k(N,\nu_e) = \sum_{T \subseteq N \setminus \{k\};\ 1 \in T;\ e \in g(T)} W(|T|,n)\left[\nu_e(T \cup \{k\}) - \nu_e(T)\right],$$

that is

$$Sh_k(N,\nu_e) = \sum_{T \subseteq N \setminus \{k\};\ 1 \in T;\ j \in T} W(|T|,n)\left[\nu_e(T \cup \{k\}) - \nu_e(T)\right],$$

Let $T \subseteq N$ such that $k \notin T;\ 1 \in T;\ j \in T;\ j \neq k$ It is $e \notin g(T)$ and $e \in g(T \cup \{k\})$.
Hence

$$Sh_k(N,\nu_e) = \sum_{T \subseteq N \setminus \{k\};\ 1 \in T;\ j \in T;\ j \neq k} W(|T|,n) 2m_{priv},$$

Let $|T| = \tau$, $\tau = 2, ..., n-1$.

$$\#\left\{T \subseteq N |\ j \in T;\ 1 \in T;\ k \notin T;\ |T| = \tau\right\} = \binom{n-3}{\tau-2}.$$

It follows that

$$Sh_k(N,\nu_e)=\sum_{\tau=2}^{n-1}W\tau,n)2\binom{n-3}{\tau-2}m_{priv},$$

that is

$$Sh_k(N,\nu_e)=\frac{2}{3}m_{priv}. \tag{A. 17}$$

(d) Let $e=(1,k)$ with $k\neq 1$. Remember that

$$Sh_k(N,\nu_e)=\sum_{T\subseteq N\setminus\{k\};\ 1\in T;\ e\in g(T)}W(|T|,n)\left[\nu_e(T\cup\{k\})-\nu_e(T)\right],$$

Let $T\subseteq N$ such that $k\notin T;\ 1\in T;\ 1\neq k$ It is $e\notin g(T)$ and $e\in g(T\cup\{k\})$. Hence

$$Sh_k(N,\nu_e)=\sum_{T\subseteq N\setminus\{k\};\ 1\in T;\ 1\neq k}W(|T|,n)2m_{priv},$$

Let $|T|=\tau$, $\tau=1,...,n-1$.

$$\#\left\{T\subseteq N|\ 1\in T;\ k\notin T;\ |T|=\tau\right\}=\binom{n-2}{\tau-1}.$$

It follows that

$$Sh_k(N,\nu_e)=\sum_{\tau=1}^{n-1}W(\tau,n)2\binom{n-2}{\tau-1}m_{priv},$$

that is

$$Sh_k(N,\nu_e)=m_{priv}. \tag{A. 18}$$

5. (Comutation of $Sh_k(N,\nu_1);\ k\neq 1$).

It is

$$Sh_k(N,\nu_1)=\sum_{e\in E_1}Sh_k(N,\nu_e)+\sum_{e\in E_2}Sh_k(N,\nu_e)+\sum_{e\in E_3}Sh_k(N,\nu_e)+\sum_{e\in E_4}Sh_k(N,\nu_e),$$

where

$$E_1=\{e\in E|e=(i,j);\ i\neq 1;\ j\neq 1;\ i\neq k;\ j\neq k\},$$
$$E_2=\{e\in E|e=(1,j);\ j\neq 1;j\neq k\},$$
$$E_3=\{e\in E|e=(k,j);\ j\neq 1;\ j\neq k\},$$
$$E_4=\{e\in E|e=(1,k)\}.$$

Then

$$Sh_k(N,\nu_1)=m_{priv}\left(0\#(E_1)+0\#(E_2)+\frac{2}{3}\#(E_3)+1\#(E_4)\right).$$

We distinguish two cases:

(a) $(1,k)\in E$.

$$\#(E_4)=1;\ \#(E_2)=d_1-1;\ \#(E_3)=d_k-1;$$
$$\#(E_1)=|E|-\#(E_2)-\#(E_3)-\#(E_4)=|E|-d_1-d_k+1.$$

It is

$$Sh_k(N,\nu_1)=m_{priv}\left(\frac{2}{3}(d_k-1)+1\right),$$

or

$$Sh_k(N,\nu_1)=m_{priv}\left(\frac{2}{3}d_k+\frac{1}{3}\right).$$

(b) $(1,k) \notin E$.

$$\#(E_4) = 0;\ \#(E_2) = d_1;\ \#(E_3) = d_k;$$
$$\#(E_1) = |E| - \#(E_2) - \#(E_3) - \#(E_4) = |E| - d_1 - d_k.$$

It is

$$Sh_k(N,\nu_1) = \frac{2}{3} d_k m_{priv}.$$

□

Remark 1. *It is worthwhile to prove the efficiency of our formulas. The sum of the Shapley values should be equal to $\nu_1(N)$. The authors are aware that this property should be already guaranteed by our formulas. However, we prove that this property is satisfied. Remember that $Sh_1(N;\nu_1) = \left(\frac{1}{3}d_1 + \frac{2}{3}|E|\right) m_{priv}$. Let $Sh_k^{yes}(N;\nu_1) = m_{priv}\left(\frac{2}{3}d_k + \frac{1}{3}\right)$, $Sh_k^{no}(N;\nu_1) = \frac{2}{3}d_k m_{priv}$. Note that*

$$\sum_{k=1}^{n} Sh_k(N,\nu_1) = Sh_1(N,\nu_1) + \sum_{k\neq 1;\ (1,k)\in E} Sh_k^{yes}(N,\nu_1) + \sum_{k\neq 1;\ (1,k)\notin E} Sh_k^{no}(N,\nu_1).$$

$$\#\{k \in N | k \neq 1;\ (1,k) \in E\} = d_1; \quad \#\{k \in N | k \neq 1;\ (1,k) \notin E\} = n - 1 - d_1.$$

$$\sum_{k\neq 1;\ (1,k)\in E} Sh_k^{yes}(N,\nu_1) = m_{priv}\left[\frac{1}{3}d_1 + \sum_{k\neq 1;\ (1,k)\in E} \frac{2}{3} d_k\right]$$

$$\sum_{k\neq 1;\ (1,k)\notin E} Sh_k^{no}(N,\nu_1) = m_{priv} \sum_{k\neq 1;\ (1,k)\notin E} \frac{2}{3} d_k$$

$$\sum_{k\neq 1;\ (1,k)\in E} Sh_k^{yes}(N,\nu_1) + \sum_{k\neq 1;\ (1,k)\notin E} Sh_k^{no}(N,\nu_1) = m_{priv}\left(\frac{1}{3}d_1 + \sum_{k\neq 1} \frac{2}{3} d_k\right).$$

$$\sum_{k\neq 1} \frac{2}{3} d_k = \frac{2}{3}\sum_{k\neq 1} d_k = \frac{2}{3}(2|E| - d_1) = \frac{4}{3}|E| - \frac{2}{3}d_1.$$

$$\begin{aligned}
\textstyle\sum_{k\neq 1;\ (1,k)\in E} Sh_k^{yes}(N,\nu_1) + \sum_{k\neq 1;\ (1,k)\notin E} Sh_k^{no}(N,\nu_1) &= \\
&= m_{priv}\left(\frac{1}{3}d_1 + \frac{4}{3}|E| - \frac{2}{3}d_1\right) \\
&= m_{priv}\left(\frac{4}{3}|E| - \frac{1}{3}d_1\right).
\end{aligned}$$

$$\sum_{k=1}^{n} Sh_k(N,\nu_1) = Sh_1(N,\nu_1) + m_{priv}\left(\frac{4}{3}|E| - \frac{1}{3}d_1\right).$$

$$\sum_{k=1}^{n} Sh_k(N,\nu_1) = m_{priv}\left(\frac{1}{3}d_1 + \frac{2}{3}|E| + \frac{4}{3}|E| - \frac{1}{3}d_1\right).$$

$$\sum_{k=1}^{n} Sh_k(N,\nu_1) = 2|E| m_{priv}.$$

Then

$$\sum_{k=1}^{n} Sh_k(\nu_1) = \nu_a(N)$$

as expected.

Proof of Theorem 3

Proof. It follows from Lemma 3 and Lemma 4. □

Lemma 5. *Let*

$$\nu_1(T) = \begin{cases} \lambda(T, E_{|T})m_{priv} & \text{if } 1 \in T, \\ 0 & \text{if } 1 \notin T, \end{cases}$$

where

$$\lambda(T, E_{|T}) = 2\frac{|T||E_{|T}|}{n}.$$

In other words

$$\nu_1(T) = \begin{cases} 2\frac{|T||E_{|T}|}{n}m_{priv} & \text{if } 1 \in T, \\ 0 & \text{if } 1 \notin T, \end{cases}$$

Let

$$C_1 = \{k \in N | (1, k) \in E\}.$$

It is $|C_1| = d_1$.
Moreover

-

$$Sh_1(N; \nu_1) = \left(\frac{n+1}{6n}d_1 + \frac{n+1}{2n}|E|\right) m_{priv}. \tag{A. 19}$$

- *Let* $k \in N$ *and* $k \neq 1$. *If* $k \in C_1$, *we have*

$$Sh_k(N; \nu_1) = \left(\frac{1}{6n}d_1 + 1\frac{1}{2}d_k + \frac{1}{2n}|E| + \frac{1}{6}\right) m_{priv}. \tag{A. 20}$$

- *Let* $k \in N$ *and* $k \neq 1$. *If* $k \notin C_1$, *we have*

$$Sh_k(N; \nu_1) = \left(\frac{1}{6n}d_1 + \frac{1}{2}d_k + \frac{1}{2n}|E|\right) m_{priv}. \tag{A. 21}$$

Proof. 1. Let us consider $e = (i, j) \in E$ an edge connecting agents i and j. We say that $e \in g(T)$ if $i \in T$ and $j \in T$, where $T \subseteq N$. We define the following function $\nu_e : 2^N \to \mathbb{R}$

$$\nu_e(T) = \begin{cases} 2\ \frac{|T|\ m_{priv}}{n} & \text{if } e \in g(T) \text{ and } 1 \in T; \\ 0 & \text{otherwise.} \end{cases} \tag{A. 22}$$

Let $G_e = (N, v_e)$ the finite family of TU-games on N with characteristic function ν_e.
Let $T \subseteq N$.

- Let $1 \in T$. Then

$$\sum_{e \in E} \nu_e(T) = \sum_{e \in g(T)} \frac{2|T|}{n}\, m_{priv} = \frac{2|E_{|T}||T|}{n} m_{priv} = \nu_1(T),$$

- Let $1 \notin T$. Then

$$\sum_{e \in E} \nu_e(T) = 0 = \nu_1(T),$$

Therefore, it is

$$\sum_{e \in E} \nu_e = \nu_1.$$

2. (Computation of $Sh_1(N, \nu_e)$).

$$Sh_1(N, \nu_e) = \sum_{T \subseteq N \setminus \{1\}} W(|T|, n) \left[\nu_e(T \cup \{1\}) - \nu_e(T)\right], \tag{A. 23}$$

where

$$W(|T|, n) = \frac{|T|!(n - |T| - 1)!}{n!}.$$

Since $1 \notin T$ implies $\nu_e(T) = 0$, we have

$$Sh_1(N, \nu_e) = \sum_{T \subseteq N \setminus \{1\}} W(|T|, n) \nu_e(T \cup \{1\}).$$

(a) Let $e = (i, j)$ with $i \neq 1$ and $j \neq 1$. It is

$$e \in g(T \cup \{1\}) \iff e \in g(T).$$

If $e \in g(T)$, then

$$\nu_e(T \cup \{1\}) = \frac{2(|T| + 1)}{n} m_{priv}.$$

Hence

$$Sh_1(N, \nu_e) = \sum_{T \subseteq N \setminus \{1\};\, i \in T;\, j \in T} W(|T|, n) \frac{2(|T| + 1)}{n} m_{priv}.$$

Let $|T| = \tau$, $\tau = 2, ..., n - 1$. It is[6]

$$\#\left\{T \subseteq N | i \in T;\ j \in T;\ 1 \notin T; |T| = \tau\right\} = \binom{n-3}{\tau-2}.$$

It follows that

$$Sh_1(N, \nu_e) = \sum_{\tau=2}^{n} W\tau, n) \frac{2(\tau + 1)}{n - 1} \binom{n-3}{\tau-2} m_{priv},$$

that is

$$Sh_1(N, \nu_e) = \frac{n + 1}{2n} m_{priv}. \tag{A. 24}$$

(b) Let $e = (1, j)$ with $j \neq 1$. Let $T \subseteq N$ with $1 \notin T$.

[6] $\#(S)$ denotes the number of elements of S.

- If $j \in T$ then

$$e \notin g(T); \quad e \in g(T \cup \{1\}),$$

so that

$$\nu_e(T \cup \{1\}) = \frac{2(|T|+1)}{n} m_{priv}; \quad \nu_e(T) = 0.$$

- If $j \notin T$ then

$$e \notin g(T); \quad e \notin g(T \cup \{1\}),$$

so that

$$\nu_e(T \cup \{1\}) = \nu_e(T) = 0.$$

Hence

$$Sh_1(N, \nu_e) = \sum_{T \subseteq N \setminus \{1\};\, j \in T} W(|T|, n) \frac{2(|T|+1)}{n} m_{priv}.$$

Let $|T| = \tau$, $\tau = 1, ..., n-1$.

$$\#\{T \subseteq N | j \in T;\ 1 \notin T; |T| = \tau\} = \binom{n-2}{\tau - 1}.$$

It follows that

$$Sh_1(N, \nu_e) = \sum_{\tau=1}^{n-1} W\tau, n) \frac{2(\tau+1)}{n-1} \binom{n-2}{\tau-1} m_{priv},$$

that is

$$Sh_1(N, \nu_e) = \frac{2(n+1)}{3n} m_{priv}. \tag{A. 25}$$

3. (Computation of $Sh_1(N, \nu_1)$).
It is

$$Sh_1(N, \nu_1) = \sum_{e \in E} Sh_1(N, \nu_e) = \sum_{e=(i,j) \in E | i \neq 1;\, j \neq 1} Sh_1(N, \nu_e) + \sum_{e=(1,j) \in E | j \neq 1} Sh_1(N; \nu_e).$$

$$\#\{e = (i,j) \in E | i \neq 1;\ j \neq 1\} = |E| - d_1; \quad \#\{e = (1,j) \in E | j \neq 1\} = d_1.$$

From (A. 24) and (A. 25), it follows that

$$Sh_1(N, \nu_1) = (|E| - d_1) \frac{n+1}{2n} m_{priv} + d_1 \frac{2(n+1)}{3n} m_{priv},$$

or

$$Sh_1(N, \nu_1) = \left(\frac{n+1}{6n} d_1 + \frac{n+1}{2n} |E| \right) m_{priv}.$$

4. (Computation of $Sh_k(N, \nu_e);\ k \neq 1$).

$$Sh_k(N, \nu_e) = \sum_{T \subseteq N \setminus \{k\}} W(|T|, n) \left[\nu_e(T \cup \{k\}) - \nu_e(T) \right], \tag{A. 26}$$

where

$$W(|T|, n) = \frac{|T|!(n - |T| - 1)!}{n!}.$$

If $1 \notin T$ then $1 \notin T \cup k$, so that

$$\nu_e(T \cup \{k\}) = \nu_e(T) = 0.$$

Hence

$$Sh_k(N, \nu_e) = \sum_{T \subseteq N \setminus \{k\};\, 1 \in T;\, e \in g(T)} W(|T|, n) \left[\nu_e(T \cup \{k\}) - \nu_e(T) \right],$$

(a) Let $e=(i,j)$ with $i\neq 1;\ j\neq 1;\ i\neq k;\ j\neq k$. It is

$$e\in g(T\cup\{k\})\iff e\in g(T).$$

If $1\in T$ and $e\in g(T)$, then

$$\nu_e(T\cup\{k\})-\nu_e(T)=\frac{2(|T|+1)}{n}m_{priv}-\frac{2|T|}{n}m_{priv}=\frac{2}{n}m_{priv}.$$

Hence

$$Sh_k(N,\nu_e)=\sum_{T\subseteq N\setminus\{k\};\ 1\in T;\ i\in T;\ j\in T}W(|T|,n)\frac{2}{n}m_{priv},$$

Let $|T|=\tau$, $\tau=3,...,n-1$.

$$\#\left\{T\subseteq N|i\in T;\ j\in T;\ 1\in T;\ k\notin T;\ |T|=\tau\right\}=\binom{n-4}{\tau-3}.$$

It follows that

$$Sh_k(N,\nu_e)=\sum_{\tau=3}^{n-1}W\tau,n)\frac{2}{n}\binom{n-4}{\tau-3}m_{priv},$$

that is

$$Sh_k(N,\nu_e)=\frac{1}{2n}m_{priv}. \tag{A. 27}$$

(b) Let $e=(1,j)$ with $j\neq 1;\ j\neq k$.
It is

$$e\in g(T\cup\{k\})\iff e\in g(T).$$

If $1\in T$ and $e\in g(T)$, then

$$\nu_e(T\cup\{k\})-\nu_e(T)=\frac{2(|T|+1)}{n}m_{priv}-\frac{2|T|}{n}m_{priv}=\frac{2}{n}m_{priv}.$$

Hence

$$Sh_k(N,\nu_e)=\sum_{T\subseteq N\setminus\{k\};\ 1\in T;\ j\in T;\ j\neq k}W(|T|,n)\frac{2}{n}m_{priv},$$

Let $|T|=\tau$, $\tau=2,...,n-1$.

$$\#\left\{T\subseteq N|\ j\in T;\ 1\in T;\ k\notin T;\ |T|=\tau\right\}=\binom{n-3}{\tau-2}.$$

It follows that

$$Sh_k(N,\nu_e)=\sum_{\tau=2}^{n-1}W\tau,n)\frac{2}{n}\binom{n-3}{\tau-2}m_{priv},$$

that is

$$Sh_k(N,\nu_e)=\frac{2}{3n}m_{priv}. \tag{A. 28}$$

(c) Let $e=(k,j)$ with $j\neq 1;\ j\neq k$. Remember that

$$Sh_k(N,\nu_e)=\sum_{T\subseteq N\setminus\{k\};\ 1\in T;\ e\in g(T)}W(|T|,n)\left[\nu_e(T\cup\{k\})-\nu_e(T)\right],$$

that is

$$Sh_k(N,\nu_e) = \sum_{T\subseteq N\setminus\{k\};\ 1\in T;\ j\in T} W(|T|,n)\left[\nu_e(T\cup\{k\}) - \nu_e(T)\right],$$

Let $T \subseteq N$ such that $k \notin T;\ 1 \in T;\ j \in T;\ j \neq k$ It is $e \notin g(T)$ and $e \in g(T \cup \{k\})$. Hence

$$Sh_k(N,\nu_e) = \sum_{T\subseteq N\setminus\{k\};\ 1\in T;\ j\in T;\ j\neq k} W(|T|,n)\frac{2(|T|+1)}{n} m_{priv},$$

Let $|T| = \tau$, $\tau = 2, ..., n-1$.

$$\#\left\{T \subseteq N |\ j \in T;\ 1 \in T;\ k \notin T;\ |T| = \tau\right\} = \binom{n-3}{\tau-2}.$$

It follows that

$$Sh_k(N,\nu_e) = \sum_{\tau=2}^{n-1} W\tau, n)\frac{2(\tau+1)}{n}\binom{n-3}{\tau-2} m_{priv},$$

that is

$$Sh_k(N,\nu_e) = \frac{n+1}{2n} m_{priv}. \tag{A. 29}$$

(d) Let $e = (1, k)$ with $k \neq 1$. Recall that

$$Sh_k(N,\nu_e) = \sum_{T\subseteq N\setminus\{k\};\ 1\in T;\ e\in g(T)} W(|T|,n)\left[\nu_e(T\cup\{k\}) - \nu_e(T)\right],$$

Let $T \subseteq N$ such that $k \notin T;\ 1 \in T;\ 1 \neq k$ It is $e \notin g(T)$ and $e \in g(T \cup \{k\})$. Hence

$$Sh_k(N,\nu_e) = \sum_{T\subseteq N\setminus\{k\};\ 1\in T;\ 1\neq k} W(|T|,n)\frac{2(|T|+1)}{n} m_{priv},$$

Let $|T| = \tau$, $\tau = 1, ..., n-1$.

$$\#\left\{T \subseteq N |\ 1 \in T;\ k \notin T;\ |T| = \tau\right\} = \binom{n-2}{\tau-1}.$$

It follows that

$$Sh_k(N,\nu_e) = \sum_{\tau=1}^{n-1} W\tau, n)\frac{2(\tau+1)}{n}\binom{n-2}{\tau-1} m_{priv},$$

that is

$$Sh_k(N,\nu_e) = \frac{2(n+1)}{3n} m_{priv}. \tag{A. 30}$$

5. (Computation of $Sh_k(N,\nu_1);\ k \neq 1$).

It is

$$Sh_k(N,\nu_1) = \sum_{e\in E_1} Sh_k(N,\nu_e) + \sum_{e\in E_2} Sh_k(N,\nu_e) + \sum_{e\in E_3} Sh_k(N,\nu_e) + \sum_{e\in E_4} Sh_k(N,\nu_e),$$

where

$$E_1 = \{e \in E | e = (i, j);\ i \neq 1;\ j \neq 1;\ i \neq k;\ j \neq k\},$$
$$E_2 = \{e \in E | e = (1, j);\ j \neq 1; j \neq k\},$$

$$E_3 = \{e \in E | e = (k, j);\ j \neq 1;\ j \neq k\},$$
$$E_4 = \{e \in E | e = (1, k)\}.$$

Then

$$Sh_k(N, \nu_1) = m_{priv}\left(\frac{1}{2n}\#(E_1) + \frac{2}{3n}\#(E_2) + \frac{n+1}{2n}\#(E_3) + \frac{2(n+1)}{3n}\#(E_4)\right).$$

We distinguish two cases:

(a) $(1, k) \in E$.

$$\#(E_4) = 1;\ \#(E_2) = d_1 - 1;\ \#(E_3) = d_k - 1;$$
$$\#(E_1) = |E| - \#(E_2) - \#(E_3) - \#(E_4) = |E| - d_1 - d_k + 1.$$

It is

$$Sh_k(N, \nu_1) = m_{priv}\left(\frac{1}{2n}(|E| - d_1 - d_k + 1) + \frac{2}{3n}(d_1 - 1) + \frac{n+1}{2n}(d_k - 1) + \frac{2(n+1)}{3n}\right),$$

or

$$Sh_k(N, \nu_1) = m_{priv}\left(\frac{1}{6n}d_1 + \frac{1}{2}d_k + \frac{1}{2n}|E| + \frac{1}{6}\right).$$

6. $(1, k) \notin E$.

$$\#(E_4) = 0;\ \#(E_2) = d_1;\ \#(E_3) = d_k;$$
$$\#(E_1) = |E| - \#(E_2) - \#(E_3) - \#(E_4) = |E| - d_1 - d_k.$$

It is

$$Sh_k(N, \nu_1) = m_{priv}\left(\frac{1}{2n}(|E| - d_1 - d_k) + \frac{2}{3n}d_1 + \frac{n+1}{2n}d_k\right),$$

or

$$Sh_k(N, \nu_1) = m_{priv}\left(\frac{1}{6n}d_1 + \frac{1}{2}d_k + \frac{1}{2n}|E|\right).$$

□

Remark 2. *It is worthwhile to prove the efficiency of our formulas. The sum of the Shapley values should be equal to* $\nu_1(N)$. *The authors are aware that this property should be already guaranteed by our formulas. However, we prove that this property is satisfied. Recall that* $Sh_1(N, \nu_1) = \left(\frac{n+1}{6n}d_1 + \frac{n+1}{2n}|E|\right)m_{priv}$. *Let* $Sh_k^{yes}(N, \nu_1) = \left(\frac{1}{6n}d_1 + \frac{1}{2}d_k + \frac{1}{2n}|E| + \frac{1}{6}\right)m_{priv}$, $Sh_k^{no}(N, \nu_1) = \left(\frac{1}{6n}d_1 + \frac{1}{2}d_k + \frac{1}{2n}|E|\right)m_{priv}$. *Note that*

$$\sum_{k=1}^{n} Sh_k(N, \nu_1) = Sh_1(N, \nu_1) + \sum_{k\neq 1;\ (1,k)\in E} Sh_k^{yes}(N, \nu_1) + \sum_{k\neq 1;\ (1,k)\notin E} Sh_k^{no}(N, \nu_1).$$

$$\#\{k \in N | k \neq 1;\ (1, k) \in E\} = d_1; \quad \#\{k \in N | k \neq 1;\ (1, k) \notin E\} = n - 1 - d_1.$$

$$\sum_{k\neq 1;\ (1,k)\in E} Sh_k^{yes}(N, \nu_1) = m_{priv}\left[d_1\left(\frac{1}{6n}d_1 + \frac{1}{2n}|E| + \frac{1}{6}\right) + \sum_{k\neq 1;\ (1,k)\in E}\frac{1}{2}d_k\right]$$

$$\sum_{k\neq 1;\ (1,k)\notin E} Sh_k^{no}(N,\nu_1) = m_{priv}\left[(n-1-d_1)\left(\frac{1}{6n}d_1+\frac{1}{2n}|E|\right)+\sum_{k\neq 1;\ (1,k)\notin E}\frac{1}{2}d_k\right]$$

It is

$$d_1\left(\frac{1}{6n}d_1+\frac{1}{2n}|E|+\frac{1}{6}\right)+(n-1-d_1)\left(\frac{1}{6n}d_1+\frac{1}{2n}|E|\right)=\frac{2n-1}{6n}d_1+\frac{n-1}{2n}|E|.$$

$$\sum_{k\neq 1;\ (1,k)\in E} Sh_k^{yes}(N,\nu_1)+\sum_{k\neq 1;\ (1,k)\notin E} Sh_k^{no}(N,\nu_1) = m_{priv}\left(\frac{2n-1}{6n}d_1+\frac{n-1}{2n}|E|+\sum_{k\neq 1}\frac{1}{2}d_k\right).$$

$$\sum_{k\neq 1}\frac{1}{2}d_k=\frac{1}{2}\sum_{k\neq 1}d_k=\frac{1}{2}(2|E|-d_1)=|E|-\frac{1}{2}d_1.$$

$$\sum_{k\neq 1;\ (1,k)\in E} Sh_k^{yes}(N,\nu_1)+\sum_{k\neq 1;\ (1,k)\notin E} Sh_k^{no}(N,\nu_1) = m_{priv}\left(\frac{2n-1}{6n}d_1+\frac{n-1}{2n}|E|+|E|-\frac{1}{2}d_1\right).$$

$$\sum_{k\neq 1;\ (1,k)\in E} Sh_k^{yes}(N,\nu_1)+\sum_{k\neq 1;\ (1,k)\notin E} Sh_k^{no}(N,\nu_1) = m_{priv}\left(\frac{2n-1}{6n}d_1+\frac{3n-1}{2n}|E|-\frac{1}{2}d_1\right).$$

$$\sum_{k=1}^{n} Sh_k(N,\nu_1) = Sh_1(N,\nu_1)+m_{priv}\left(\frac{3n-1}{2n}|E|-\frac{n+1}{6n}d_1\right).$$

$$\sum_{k=1}^{n} Sh_k(N,\nu_1) = m_{priv}\left(\frac{n+1}{6n}d_1+\frac{n+1}{2n}|E|+\frac{3n-1}{2n}|E|-\frac{n+1}{6n}d_1\right).$$

$$\sum_{k=1}^{n} Sh_k(N,\nu_1) = 2|E|m_{priv}=\nu_1(N)$$

as it is expected.

Proof of Theorem 4

Proof. It follows from Lemma 3 and Lemma 5. □

6 References

Abella, A., Ortiz-de Urbina-Criado, M., & De-Pablos-Heredero, C. (2017). A model for the analysis of data-driven innovation and value generation in smart cities' ecosystems. *Cities*, *64*, 47–53.

Abu-Elkheir, M., Hayajneh, M., & Ali, N. A. (2013). Data management for the internet of things: Design primitives and solution. *Sensors*, *13*(11), 15582–15612.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies*, *42*(2), 249–274.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, *54*(2), 442–92.

Ahrweiler, P., & Keane, M. T. (2013). Innovation networks. *Mind & Society*, *12*(1), 73–90.

Béal, S., & Deschamps, M. (2016). On compensation schemes for data sharing within the european reach legislation. *European Journal of Law and Economics*, *41*(1), 157–181.

Béal, S., Deschamps, M., & Solal, P. (2016). Comparable axiomatizations of two allocation rules for cooperative games with transferable utility and their subclass of data games. *Journal of Public Economic Theory*, *18*(6), 992–1004.

Biczók, G., & Chia, P. H. (2013). Interdependent privacy: Let me share your data. In *International conference on financial cryptography and data security* (pp. 338–353).

Büyüközkan, G., & Göçer, F. (2018). Digital supply chain: Literature review and a proposed framework for future research. *Computers in Industry*, *97*, 157–177.

Capaldo, A. (2007). Network structure and innovation: The leveraging of a dual network as a distinctive relational capability. *Strategic management journal*, *28*(6), 585–608.

Caron, X., Bosua, R., Maynard, S. B., & Ahmad, A. (2016). The internet of things (iot) and its impact on individual privacy: An australian perspective. *Computer Law & Security Review*, *32*(1), 4–15.

Chessa, M., Grossklags, J., & Loiseau, P. (2015). A game-theoretic study on non-monetary incentives in data analytics projects with privacy implications. In *2015 ieee 28th computer security foundations symposium* (pp. 90–104).

Chessa, M., & Loiseau, P. (2017). A cooperative game-theoretic approach to quantify the value of personal data in networks. In *Proceedings of the 12th workshop on the economics of networks, systems and computation* (pp. 1–1).

Deng, X., & Papadimitriou, C. H. (1994). On the complexity of cooperative solution concepts. *Mathematics of Operations Research*, *19*(2), 257–266.

Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing. *Journal of Network and Computer Applications*, *67*, 99–117.

Goes, J. B., & Park, S. H. (1997). Interorganizational links and innovation: The case of hospital services. *Academy of Management Journal*, *40*(3), 673–696.

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the sony playstation network breach. *MIS Quarterly*, *41*(3), 703–727.

Gulati, R., & Gargiulo, M. (1999). Where do interorganizational networks come from? *American Journal of Sociology*, *104*(5), 1439–1493.

Ioannidis, S., & Loiseau, P. (2013). Linear regression as a non-cooperative game. In *International conference on web and internet economics* (pp. 277–290).

Iqbal, M. U., & Lim, S. (2006). A privacy preserving gps-based pay-as-you-drive insurance scheme. In *Symposium on gps/gnss (ignss2006)* (pp. 17–21).

Iqbal, M. U., & Lim, S. (2010). Privacy implications of automated gps tracking and profiling. *IEEE Technology and Society Magazine*, *29*(2), 39–46.

Janeček, V. (2018). Ownership of personal data in the internet of things. *Computer law & Security Review*, *34*(5), 1039–1052.

Kamleitner, B., & Mitchell, V. (2019). Your data is my data: A framework for addressing interdependent privacy infringements. *Journal of Public Policy & Marketing*, *38*(4), 433–450.

Kerber, W. (2018). Data governance in connected cars: The problem of access to in-vehicle data. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, *9*, 310.

Kude, T., Hoehle, H., & Sykes, T. A. (2017). Big data breaches and customer compensation strategies: Personality traits and social influence as antecedents of perceived compensation. *International Journal of Operations & Production Management*, *37*(1), 56–74.

Lopez, J., Rios, R., Bao, F., & Wang, G. (2017). Evolving privacy: From sensors to the internet of things.

Future Generation Computer Systems, *75*, 46–57.

Madaan, N., Ahad, M. A., & Sastry, S. M. (2018). Data integration in iot ecosystem: Information linkage as a privacy threat. *Computer Law & Security Review*, *34*(1), 125–133.

Maras, M.-H. (2015). Internet of things: security and privacy implications. *International Data Privacy Law*, *5*(2), 99.

Markendahl, J., Lundberg, S., Kordas, O., & Movin, S. (2017). On the role and potential of iot in different industries: Analysis of actor cooperation and challenges for introduction of new technology. In *2017 internet of things business models, users, and networks* (pp. 1–8).

Moretti, S., & Patrone, F. (2008). Transversality of the Shapley value. *Topologica*, *16*(1), 1–41.

Nedeltcheva, G. N., & Shoikova, E. (2017). Models for innovative iot ecosystems. In *Proceedings of the international conference on big data and internet of thing* (pp. 164–168).

Olteanu, A. M., Huguenin, K., Humbert, M., & Hubaux, J.-P. (2016). *The sharing game: Benefits and privacy implications of (co)-location sharing with interdependences* (Tech. Rep.). EPFL, research report, 2016.[Online]. Available: https://infoscience. epfl ....

Park, S. (2019). Why information security law has been ineffective in addressing security vulnerabilities: Evidence from california data breach notifications and relevant court and government records. *International Review of Law and Economics*, *58*, 132–145.

Park, S. H. (1996). Managing an interorganizational network: a framework of the institutional mechanism for network control. *Organization Studies*, *17*(5), 795–824.

Peters, S., Chun, J.-H., & Lanza, G. (2015). Digitalization of automotive industry–scenarios for future manufacturing. *Manufacturing Review*, *3*.

Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A., & Vasilakos, A. V. (2016). The quest for privacy in the internet of things. *IEEE Cloud Computing*, *3*(2), 36–45.

Posner, R. A. (1981). The economics of privacy. *The American Economic Review*, *71*(2), 405–409.

Powell, W. W., Koput, K. W., & Smith-Doerr, L. (1996). Interorganizational collaboration and the locus of innovation: Networks of learning in biotechnology. *Administrative Science Quarterly*, 116–145.

Pu, Y., & Grossklags, J. (2014). An economic model and simulation results of app adoption decisions on networks with interdependent privacy consequences. In *International conference on decision and game theory for security* (pp. 246–265).

Salavisa, I., Sousa, C., & Fontes, M. (2012). Topologies of innovation networks in knowledge-intensive sectors: Sectoral differences in the access to knowledge and complementary assets through formal and informal ties. *Technovation*, *32*(6), 380–399.

Seif, H. G., & Hu, X. (2016). Autonomous driving in the icity—hd maps as a key challenge of the automotive industry. *Engineering*, *2*(2), 159–162.

Seo, J., Kim, K., Park, M., Park, M., & Lee, K. (2017). An analysis of economic impact on iot under gdpr. In *2017 international conference on information and communication technology convergence (ictc)* (pp. 879–881).

Seo, J., Kim, K., Park, M., Park, M., & Lee, K. (2018). An analysis of economic impact on iot industry under gdpr. *Mobile Information Systems*, *2018*.

Shovon, A. R., Roy, S., Shil, A. K., & Atik, T. (2019). Gdpr compliance: Implementation use cases for user data privacy in news media industry. In *2019 1st international conference on advances in science, engineering and robotics technology (icasert)* (pp. 1–6).

Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K.-L. (2015). The challenges of personal data markets and privacy. *Electronic Markets*, *25*(2), 161–167.

Symeonidis, I., Biczók, G., Shirazi, F., Pérez-Solà, C., Schroers, J., & Preneel, B. (2018). Collateral damage of facebook third-party applications: a comprehensive study. *Computers & Security*, *77*, 179–208.

Symeonidis, I., Shirazi, F., Biczók, G., Pérez-Solà, C., & Preneel, B. (2016). Collateral damage of facebook apps: Friends, providers, and privacy interdependence. In *IFIP international conference on ict systems security and privacy protection* (pp. 194–208).

Tzafestas, S. G. (2018). Ethics and law in the internet of things world. *Smart Cities*, *1*(1), 98–120.

Valverde, S., Solé, R. V., Bedau, M. A., & Packard, N. (2007). Topology and evolution of technology innovation networks. *Physical Review E*, *76*(5), 056118.

Villa, M., Gofman, M., & Mitra, S. (2018). Survey of biometric techniques for automotive applications. In *Information technology-new generations* (pp. 475–481). Springer.

Wang, C., Daneshmand, M., Dohler, M., Mao, X., Hu, R. Q., & Wang, H. (2013). Guest editorial-special

issue on internet of things (iot): Architecture, protocols and services. *IEEE Sensors Journal*, *13*(10), 3505–3510.

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review*, *31*(5), 618–627.

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the internet of things: threats and challenges. *Security and Communication Networks*, *7*(12), 2728–2742.