What's your anonymity worth? Establishing a marketplace for the valuation and control of individuals' anonymity and personal data

Stephen Cory Robinson

Abstract

Purpose – *The viability of online anonymity is questioned in today's online environment where many technologies enable tracking and identification of individuals. In light of the shortcomings of the government, industry and consumers in protecting anonymity, it is clear that a new perspective for ensuring anonymity is needed. Where current stakeholders have failed to protect anonymity, some proponents argue that economic models exist for valuation of anonymity. By placing a monetary value on anonymity through Rawls' concept of primary goods, it is possible to create a marketplace for anonymity, therefore allowing users full control of how their personal data is used. This paper aims to explore the creation of a data marketplace, offering users the possibility of engaging with companies and other entities to sell and auction personal data. Importantly, participation in a marketplace does not sacrifice one's anonymity, as there are different levels of anonymity in online systems.*

Design/methodology/approach – *The paper uses a conceptual framework based on the abstractions of anonymity and data valuation.*

Findings – *The manuscript constructs a conceptual foundation for exploring the development and deployment of a personal data marketplace. By suggesting features allowing individuals' control of their personal data, and properly establishing monetary valuation of one's personal data, it is argued that individuals will undertake a more proactive management of personal data.*

Originality/value – *An overview of the available services and products offering increased anonymity is explored, in turn, illustrating the beginnings of a market response for anonymity as a valuable good. By placing a monetary value on individuals' anonymity, it is reasoned that individuals will more consciously protect their anonymity in ways where legislation and other practices (i.e. privacy policies, marketing opt-out) have failed.*

Keywords *Data protection, Economic value, Online anonymity, Personal data, PII*

Paper type *Conceptual paper*

Stephen Cory Robinson is Assistant Professor in Communication Design at the Department of Science and Technology, Linköping University, Norrköping, Sweden.

Introduction

Threats to remaining anonymous while online are all around us and occur with surprising frequency. Recent threats to anonymity include electronic manufacturer Vizio's smart TVs unknowingly monitoring owner's viewing habits and having their personal information sold (Goodwin, 2017), or new Google algorithms making it possible to identify individuals using severely pixelated photos (Anthony, 2017). We live in a world where the ability to easily identify individuals is posing growing threats to online anonymity.

One major threat to anonymity is the use of social networking sites. Use of the internet for socializing and communicating continues to be massively popular. Of the top 20 websites in the world, four are social networks, including LinkedIn, Facebook, Twitter and Instagram

Received 5 May 2017
Revised 5 May 2017
Accepted 1 June 2017

(Alexa.com, 2017). According to Statista.com (2017), these four networks have a combined (and probably somewhat overlapping) user population of 3.244 billion users (LinkedIn: 467 million; Facebook: 1.86 billion; Twitter: 317 million; and Instagram: 600 million).

These social networks are used by their members for many reasons, both professional and personal. The networks provide entertainment and the ability to communicate with friends (Whiting and Williams, 2013), a market for selling or purchasing of services and products (Mangold and Faulds, 2009), and job networking (Olmstead *et al.*, 2015). In addition to entertainment, social capital and purchasing of products or service, individuals also use networks to seek healthcare information and advice (Moorhead *et al.*, 2013).

While the use of these networks provides the above-mentioned benefits, their use brings with them some threats to individuals' ability to mask their identity. Through being public with the use of the internet and these social networks, individuals may be sacrificing important rights, including the ability to remain anonymous. An even bigger concern is that social networks claiming to anonymize data are easily overcome with the proper technical know-how, and ultimately, their users can be identified (Narayanan and Shmatikov, 2009).

Even as social networks continue to grow, it seems that individuals are getting more concerned about anonymity and having their online activities hidden. A recent survey found that 86 per cent of online users engage in activities to become more anonymous online (Rainie *et al.*, 2013). Growth in the adoption of anonymous texting/messaging continues to occur (Hughes and Johnson, 2016), indicating an increased interest in the ability to communicate more anonymously.

To allow social networks and online businesses to continue to flourish, while also providing opportunities for individuals to mask their online identity and maintain anonymity, the author proposes a market-based system for commodification of anonymity. Using Rawls' (2001) concept of primary goods, and building upon the idea that anonymity is a primary good (Robinson, 2015), the author will justify a system for pricing anonymity. By placing a monetary value on individuals' anonymity, it is reasoned that individuals will more consciously protect their anonymity in ways where legislation and other practices (i.e. opt-out) have failed. Several authors have explored valuation of privacy (Sidgman and Crompton, 2016; Morando *et al.*, 2014; Staiano *et al.*, 2014; Savage and Waldman, 2015); however, they have not highlighted mechanisms for controlling an individual's anonymity (a critical though different concept from privacy), specifically through a personal data marketplace – an innovative part of this manuscript.

Defining anonymity

Anonymity has been defined in varying ways in the literature as follows: "the condition of being unknown to others" (Lapidot-Lefler and Barak, 2012, p. 435), or "the state of being not identifiable" (Pfitzmann and Köhntopp, 2001, p. 2). In essence, anonymity may be explored through the concept of unidentifiable existence online. Lapidot-Lefler and Barak (2012) argue that unidentifiability is a crucial aspect of being anonymous; rather than just being nameless, the dimension of unidentifiability is broader and more significant. While anonymity and privacy are frequently used interchangeably, it is important to note that these are two distinct concepts, and this manuscript only explores anonymity. As previously stated, anonymity deals with being not identifiable. Being anonymous may also be viewed as that an individual cannot be identified by any of several identifiers, including name, location, pseudonyms that cannot be linked to name or location, patterns of behavior, social group memberships or indications of personal characteristics (Marx, 1999).

While now defined, an important notion for consideration is that different types of anonymity exist. Some have suggested two types of anonymity: technical anonymity and social anonymity (Hayne and Rice, 1997). Technical anonymity is the removal of all identifying information regarding other individuals in the material exchanged – one may remove their name or social media username from communications. Social anonymity is the perception of oneself or others being unidentifiable because of lack of cues for attributing an identity to that individual.

The individual's right to anonymity is found in both US and European law. The USA and European Union (EU) have fundamentally different perspectives on how to protect information. In the USA, the government allows industry self-regulation, whereas the European market favors formal legal regulation (Bowie and Jamal, 2006). The EU's Data Protection Directive (95/46/EC) defines personal data as any information relating to an identified or identifiable natural person or data subject (European Parliament and Council of the European Union, 1995). The notion of personal data, commonly referred to in the USA as personally identifying information (PII) (United States Government Accountability Office, 2008), is a critical component of anonymity. The availability to identify items of personal data online affects one's ability to remain anonymous, or unidentifiable, in the online realm.

Benefits and disadvantages of anonymity

The ability to not be identified can have advantages both offline and online. Anonymity can lift inhibition and lead to unusual acts of generosity or kindness (Suler, 2004). Using the protection of anonymity, people can experience lower social risk when discussing unpopular opinions and topics (Bargh *et al.*, 2002). When anonymous, individuals are able to maintain their social relations because concealing things from the public can thwart breakdowns in relationships (Schoeman, 1992). Being anonymous also provides individuals the ability to develop online personas different from those exhibited offline (Yurchisin *et al.*, 2005). Without anonymity, identification of individuals can occur, which may ultimately lead to discrimination based on identifiers (Robinson, 2015). The ability to practice anonymity online becomes a form of self-protection and self-development for all internet users.

While anonymity provides many benefits, it also has potential drawbacks. For industry, there are prospective financial losses through fake or negative product or service reviews. For instance, Amazon has intervened in cases of fraudulent product reviews (Shipley, 2015). For individuals, the disinhibition created when online can lead to misbehavior, including harsh or vulgar language, and illegal or harmful acts (Suler, 2004).

Stakeholders involved with regulating and protecting anonymity

Similar to the advertising and marketing industry in the USA, the responsibility of regulating and oversight of free speech and anonymity involve three stakeholder groups: government, industry and consumers.

National or state governments can regulate anonymity through two principal mechanisms: legislation and litigation. However, differences exist between nations in how the protection of anonymity is regulated. In the USA, government regulates industries specifically, whereas EU law is more general, requiring businesses to follow fair practices in information (Cleff, 2008).

Industry, as a second major stakeholder, may be allowed by governments to self-regulate (as is typical in the USA). Additionally, industry advocates the use of anonymized personal data in predicting trends and marketing products or services.

Consumers, as the third major stakeholder, have a responsibility to be aware of threats toward their anonymity. A proactive consumer can protect their anonymity by choosing to opt-out of services, products and websites. Consumers may also use anonymity-protecting

technologies such as a virtual private network (VPN), cookie blockers and encrypted communication tools (including internet browsers that allow anonymous internet surfing, such as Tor, and end-to-end encrypted messaging applications such as Signal).

Failures of stakeholders in protecting anonymity

Each of the three main stakeholders involved with protecting rights to anonymity have fallen short of their responsibilities. The protection of personal data through legislation and industry self-regulation is not effective (Sidgman and Crompton, 2016). In addition, consumers have a responsibility to be aware of technology trends and guard against attempts to limit anonymity or expose their sensitive data.

Personal data protection in the USA is based, in part, on the philosophy that personal data is an economic issue (Schwartz and Solove, 2014). As such, Americans treat data protection as a secondary concern, to be balanced among many others (Barnes, 2006a). Due to the conflicting philosophies of economics and individual rights, the US government tends to respond reactively rather than proactively (Border, 2012). Because technology changes so fast, and government regulation can be slow to adopt to new technological changes, state and national agencies are not nimble enough or possess the technological knowledge to properly legislate and litigate against trends to limit or weaken anonymity protections.

Like governmental organizations, industry has insufficiently addressed the issue of protection of anonymity. One attempt to lessen government regulation while appearing to protect consumers' data is displaying privacy seals on company websites; however, these privacy seals do not ensure a higher standard for protection of personal data (Pollach, 2007; Miyazaki and Krishnamurthy, 2002). Another industry standard for protecting personal data is the use of anonymized data, such as large databases of patient health records used to predict and explore health outcomes. Industry proponents argue data anonymization strips sensitive identifiers from personal data and therefore limits the chance of re-identification of individuals; but anonymizing data is not effective (Ohm, 2010) – identifiers still remain (Barbaro *et al.*, 2006) or the data can be reverse-engineered leading to re-identification of individuals (Golle, 2006; Narayanan and Shmatikov, 2008; de Montjoye *et al.*, 2015, 2013). The explosion in availability of personal data through big data technologies has given rise to data brokers, or information reselling companies (Kuempel, 2016). These data brokers can, without the authorization of the individual on whom they have collected personal data, compile detailed profiles of information from offline and online references (Anthes, 2015). A recent US Senate report from the Office of Oversight and Investigations (2013, pp. 2-3) found that data brokers "sell products that identify financially vulnerable consumers" and "operate behind a veil of secrecy"). The burgeoning data-broker industry has seen the aggregation, selling and unauthorized misuse of personal data: all of which threaten to limit or completely void one's ability to remain anonymous.

Adding to the shortcomings of the government as well as the industry in preserving individuals' anonymity, consumers also share the blame for erosion of anonymity online. For example, one common means of data protection is the use of privacy policies and user agreements. While these are standard practices online, consumers are either unaware or disinterested in reading end-user license agreements (EULAs) or privacy policies (Smith, 2014). Also, consumers are not likely to opt-out from companies they have never heard of, and ignore existing notifications (i.e. EULAs or privacy policies) where consumers agree to collection and use of personal data (Anthes, 2015). Though consumers may voice interest in safeguarding their personal information online, their online behaviors are not inhibited by these concerns (Yao *et al.*, 2007; Youn and Hall, 2008). This behavior paradox (Barnes, 2006b) may be explained by users lacking awareness of the risks of, or the methods available to, protect their personal information (Tufekci, 2008; Acquisti and Gross, 2006).

As governments are too lax or slow to regulate and litigate abuse of individuals' anonymity, industry does not properly self-regulate, and consumers have consistently shown their inability to protect their own anonymity, the author recommends a new system for ensuring individuals' anonymity. The development of a new market-based identity management and personal data system is proposed in the following sections.

Establishing anonymity has value

As mentioned earlier in the manuscript, being anonymous is the condition of not being identifiable. Being able to identify an individual either limits or lessens anonymity or creates an environment where anonymity is not possible. Information that can identify individuals and undermine anonymity includes name, date of birth, IP (Internet Protocol) address, geographic location (obtained through a cell phone's GPS tracking) and other sensitive identifiers.

The underlying sensitive personal information or data that can identify individuals has value: the capturing of personal data was valued at US$156m in 2012, or US$60 for every internet user at the time (Deighton and Johnson, 2013). Some examples in the current marketplace help illustrate the value of personal data, and in turn, the value of anonymity. One example is real-time bidding (RTB) where marketers bid to serve advertisements to a website user based on identifying information (Castelluccia *et al.*, 2014). While this advertising technology powered by users' private information is unknown to many, the revenue from RTB is slated to reach US$21bn in 2017 (Advertising Age, 2013). Further, the business models of companies like Google and Facebook rely on their users' personal data to sell advertising (Ehrenberg, 2014). The lucrative advertising industry empowered by collection of users' personal information led to a revenue of US$19bn for Google in Q2, 2016 (Johnson, 2016), and US$26bn for Facebook for the year 2016 (Facebook, 2017). Clearly, the collection, use and selling of personal information is a lucrative trade – validating the value of personal data.

As highlighted, internet search and social media companies collect user information to better target advertising to those users, ultimately collecting great sums at the expense of their users. Rather than unknowingly having their information collected for the purposes of being sold, internet users can now auction their data off. Companies such as Datacoup, Meeco and Leaflad allow individuals to sell their personal information. During Datacoup's beta phase, users were given US$8 a month if they provided the company with access to a combination of social media accounts and transactions from their credit card (Simonite, 2014). Meeco (2017, p. 1), another personal information auction platform, validates the worth of personal data by stating on their information page that "data is the new currency". Meeco also states:

> If our personal data is a currency, and we are the most accurate source of data about ourselves then how much are we worth, who is prepared to pay us and what's the going market rate? (Meeco, 2017, p. 1)

In essence, Meeco makes the argument that not only is your personal data valuable, but the company is a trustworthy broker whom users should provide their valuable personal information to.

The value of personal data has also arisen in recent corporate bankruptcies. In the examples of American corporations RadioShack (electronics retailer) and Sports Authority (sporting goods retailer), consumer data have been identified as a valuable asset. The value associated with each company's consumer databases has been a source of controversy in auction proceedings. In the case of RadioShack, the company argued that its privacy policy statement not to sell consumer information should not be enforced. Intervention from the US Federal Trade Commission (FTC) advised RadioShack to sell consumer information as a package with its retail stores (Mayfield, 2015). Another

company, Sports Authority, finalized its bankruptcy proceedings by ultimately selling its assets, including collected consumer data, to its competitor. For the competitor, Dick's Sporting Goods, the value of the consumer data was clear: opportunities abound to collect valuable consumer insights, including why consumers preferred Sports Authority over Dick's Sporting Goods, the ability to analyze regions where customers were especially loyal to Sports Authority, and ultimately to solicit customers' business (Schiffer, 2016). Personal data and consumer information has become a valuable asset in the economic operations of corporations.

As personal information is a critical component in an individual's ability to remain anonymous, and by highlighting examples in the current marketplace confirming the value of personal data, the author believes the monetary value placed on personal data should extend to anonymity itself. By overviewing the available markets and products offering increased anonymity, the author makes the case that there exists an established market and desire for the good of anonymity.

A basis for valuating anonymity in a marketplace

Explored in the previous sections, anonymity has been established as having monetary value. However, industry has also not placed enough value on personal data (Sidgman and Crompton, 2016); therefore, the appropriate valuation of data is crucial for industry to establish a credible marketplace for selling and exchanging consumer data and controlling one's online anonymity. To ensure anonymity is priced fairly, allowing consumers to afford the right of anonymity while industry fairly compensates individuals for their personal data, this section will provide recommendations for establishing proper valuation of one's anonymity.

As a starting point for considering the valuation of anonymity, it would be helpful to consider technologies that individuals would need to limit threats to or maintain their online anonymity. Popular tools for concealing one's online identity include VPNs, encrypted email and messaging services, antivirus software, and finally, temporary one-time-use disposable phone numbers (i.e. "burner" phones or numbers). Witopia, a popular VPN, charges users an annual rate of US$70 for their professional services, or US$50 for their basic services. Antivirus software, such as Intego's Content Barrier Secure X9, is priced at US$64 for a one-year subscription. For encrypted email, individuals could obtain free services from *ProtonMail*, or spend US$303 per year for premium email services. Burner, a popular one-time-use mobile number application, is free to download, but charges users a credit system depending on how many disposable, one-time-use mobile numbers are needed. The monetary costs of technology for maintaining one's anonymity online can easily exceed hundreds of dollars annually.

In addition to technologies allowing for or limiting threats to online anonymity, the value individuals place on their personal data must be considered when establishing valuation of one's anonymity. Studies have explored what information is considered the most valuable, and what price individuals are willing to pay or associate with control of their data. Savage and Waldman (2015) found that individuals were willing to pay US$5.59 for an app that concealed their browsing history, GPS location data and eliminated advertising. Another study explored what minimum value individuals would sell information to a private company for, though prices varied for different types of data (Carrascal *et al.*, 2013). And social network users are reportedly willing to pay €9.40 to migrate their profile from one social network to another (Bauer *et al.*, 2012).

Self-reported valuation of data, as in the aforementioned research articles, is one method for establishing the value of personal data, but real-world marketplaces can establish realistic values of anonymity. One such marketplace where personal data is sold is on the Dark Web (formerly home to the infamous drug trading marketplace - Silk Road). *Fullz*,– hacker terminology for a complete set of an individual's personal data that can be sold to

other criminals (Barcena *et al.*, 2014) – are commonly sold on the Dark Web. Commonly obtained fraudulently, fullz may include complete individual's identity, comprising name, address, phone, email, passwords, birthdate, national ID number, bank account and credit card number (Clarke, 2013). The more complete the fullz, the more valuable the collection of data, with prices ranging from US$25 in the USA to US$40 in Europe (Clarke, 2013).

Resell value and "shelf-life" of the personal data affects the value too. Some information has a certain shelf-life or immediacy to it. As an example, a consumer's name or date of birth remains the same and does not have an immediacy in being sold. However, an individual's media consumption or usage history can quickly change; therefore, such consumer information data and behavior have a "shelf-life" (Fang *et al.*, 2013). Media usage can change with age (Nielsen, 2015); the media viewing habits of a 25-year-old would not be applicable in determining consumer behavior for the same consumer when 40-years-old.

Regarding the resell value of personal data, the extent to which the data is used should also be considered when placing value on personal data. For example, if data from a consumer is used by a first party company, the value of the data might be lower than if the first party company resells the information to a third party, and so forth. Highlighting this, individuals reported a willingness to pay US$40-50 to disallow secondary usage of their personal data (Hann *et al.*, 2002), while another study found individuals will pay €14-17 if a social network refrains from utilizing user's personal data for personalized advertising (Krasnova *et al.*, 2009). Reselling of data in the proposed marketplace could provide additional revenue to the data owner; thus, individuals selling their personal data could receive a royalty for each additional company the information is resold to.

Economic models for selling goods can affect the value of the services or goods being offered. Mimicking the market for smartphone applications, two potential models for pricing one's personal data exist: individual's personal data may be offered to companies seeking to purchase personal data either as a one-time purchase, or a free minimal data profile with subscription add-ons for lifestyle data, fitness data, or other types of personal data can be offered. This latter model in the smartphone application market finds users spending vastly more for in-app features, rather than purchasing the app in the first place (Gartner, 2016). Another model where personal data is auctioned, like an "eBay" for personal data, may provide further opportunities to maximize profit from selling personal data. In the personal data auction model, individuals could post their sociodemographic profile, auctioning their data to the highest bidder.

Other factors affecting pricing of anonymity

An individual's perception of the value of their anonymity and personal data may be influenced by many factors (Acquisti *et al.*, 2013; Carrascal *et al.*, 2013), including, among many, the factors of age, nationality, gender, attitudes toward privacy, personality traits and culture. Gender is one factor to consider, as women are typically more protective of their personal data in online environments (Fogel and Nehmad, 2009; Hoy and Milne, 2010). The age of individuals also influences disclosure of information, such that adolescents disclose more information on Facebook (Christofides *et al.*, 2011). Individuals who consider privacy as unimportant may value their personal data and anonymity less than users who consider their privacy to be important. However, conflicting research about the affect of demographics on valuation perceptions exist, as Staiano *et al.* (2014) found behavioral differences to affect personal differences in valuations more than demographics.

Further, studies have shown that separate types of personal data have different risks associated with them (Robinson, 2017). For example, an individual's name does not have the same perceived risk as their credit card information (i.e. higher risk). With this in mind, higher risk or more sensitive personal data should hold more value. Highlighting this, a recent study found that location information (i.e. GPS information), a very sensitive item of

personal information, was the most valuable personal data item (Staiano *et al.*, 2014). These more sensitive or risky items of personal data should hold more monetary value, in turn requiring companies to pay consumers more for their use.

A proposed marketplace for anonymity

This section will provide recommendations for establishing a marketplace for anonymity-related products and services. Several authors have explored valuation of personal data (Sidgman and Crompton, 2016; Morando *et al.*, 2014; Staiano *et al.*, 2014; Savage and Waldman, 2015), however they have not highlighted mechanisms for controlling an individual's anonymity, specifically through a personal data marketplace.

As an individual would need to register for the marketplace to control and sell their data, some might argue that an individual's anonymity in the marketplace would be lessened or voided after creating a marketplace profile. If anonymity were static, being either anonymous or identifiable, it could be maintained in the marketplace by not requiring disclosure of a user's real name or other identifying information. However, anonymity is not static; rather than individuals being anonymous or not, there are levels of anonymity in online systems, from super identification (the lowest level of anonymity, not anonymous) to one being completely unidentifiable, the highest level of being anonymous, or full anonymity (Flinn and Maurer, 1996). These different levels of anonymity (Morio and Buchholz, 2009; Correa *et al.*, 2015) allow individuals in the marketplace to determine the appropriate level of anonymity they desire. For example, individuals may desire a higher level of anonymity and disclose less sensitive items of personal data (like age) rather than more sensitive, unique identifiers (like national registration number, DNA or biometrics).

The proposed marketplace focuses on the market functions of controlling and selling personal data, effectively giving individuals the right to choose their level of online anonymity. As a user's anonymity increases, communication becomes less social and more information oriented (Azechi, 2005). By eliminating the social function of disclosing personal data in the marketplace transactions, users will be able to focus on the valuation aspects of their data and anonymity, perhaps encouraging a mindset geared towards the monetary value of their personal data.

Features of an online marketplace for anonymity

In this section, the author proposes some potential features of the described personal data and identity management marketplace, including ownership of data, compensation for data, and features allowing expiration of data in transactions. Anonymity should be regulated like other market goods so that potential abuse or unauthorized access is lessened and individuals have the ability to price their data and, in turn, decide what level of disclosure to agree to.

As personal data are just that, personal, it should be owned and regulated by the rightful owner. Then and only then can anonymity be guaranteed, allowing the individual to decide whether not to identify themselves when necessary, resulting in limited anonymity or loss of anonymity. The foundation of the proposed marketplace system for anonymity and related personal data is therefore built on the premise that individuals should fully control the collection, use and selling of their personal data. Each of the forthcoming features is developed with the notion that individuals have full control of their personal information.

Research has revealed that individuals are willing to exchange personal data for certain incentives or utility gain (Krause and Horvitz, 2010). By placing a monetary value on anonymity, the author argues that individuals may, for the first time, consciously process the risks and rewards associated with online anonymity. Instead of passively disclosing personal data while consuming media on the internet, these individuals, because of the potential monetary value of their data, would have something to lose. As online users may

lack awareness of the problems or risks and methods for protecting their personal information (Acquisti and Gross, 2006; Tufekci, 2008), they will have to consciously process these risks and decide if anonymity is worthwhile. While some may not view their anonymity as worthwhile, others will acknowledge anonymity's value. If offered an easy way to manage and protect their anonymity, individuals could enjoy the benefits of communicating and shopping online while only having to take a relatively passive role in overseeing the management of their anonymity (like paying their bill every month, or reviewing an anonymity statement similar to a monthly cell phone bill).

Similar to receiving a cell phone bill, marketplace participants could receive a personal data and anonymity statement at the end of every month. The statement will allow users to conveniently overview all transactions that have occurred during the previous month. In addition, they might receive a yearly review of their marketplace activity, in essence being provided an annual anonymity audit. In the monthly statements, users would be furnished with detailed descriptions of what personal data were sold to whom, when the data agreement(s) expires and the valuation of each transaction. The statement could also score the user's online anonymity, alerting them if their anonymity score reaches a certain threshold as a result of their sharing/selling activity, and provide information on how to balance their online anonymity while still receiving monetary gain from using the marketplace.

To increase the marketplace's viability, including through creating public trust in the market and securing of personal data, government should play a vital role. As one of the underlying purposes of governments is to protect citizens, the governmental body representing the data owner should act as a non-commercially-vested broker in the commercial exchange between individual and the purchasing entity. In case of fraud or data breaches, governments should reimburse individuals whose data is stolen or accessed through unauthorized means. Ensuring the security of individuals' data and the legitimacy of the marketplace would result in higher levels of trust and lower levels of perceived risk– necessary and critical components encouraging individuals to disclose (Pavlou, 2003). Guarantee of the marketplace's solvency and information security provided by government bodies might act similar to the US government's Federal Deposit Insurance Corporation (2017), which guarantees individuals' bank accounts up to US$250,000 in the event of bank failures.

The proposed marketplace would also have a form of a "data back guarantee". What if individuals do not receive the compensation for their data they expected? If the value of the incentive for exchanging or providing personal data is not deemed valuable enough, consumers "should consider holding it back" (Klein, 2013).

Regulations should be in place limiting access to an individual's data. Similar to "disappearing" text messages made popular by social networks (Snapchat.com, 2017), or expiring emails used in encrypted email services (*ProtonMail*, 2017), individuals should be able to place an expiration date on the data sold. By using an expiration date, individuals can ensure their information is not used beyond an agreed upon time frame, in turn, guaranteeing that the purchasing company will not retain the information.

As previously noted, different types of personal data are associated with varying risk levels and, therefore, should be priced accordingly. For example, in marketing, the basic metrics necessary for completing a purchase or recommending a product or service include name, email, address and credit card number. In comparison, higher risk or more sensitive-value data would garner higher prices than lower risk items or unrelated information. Currently, data brokers and marketers segment and sell very specific categories of personal data, including geographic, demographic, psychographic (including lifestyle and personality) and behavioral variables (Kotler, 1997), necessary to target specific consumer groups. Individuals in the marketplace

could also segment and sell different packages of their personal data, including demographic or psychographic information.

Conclusion

By highlighting the shortcomings of the government, industry and consumers in protecting anonymity, it is clear that a new model for ensuring anonymity is needed. The pricing of anonymity as a good may entice industry to offer fair valuation of personal data, while providing easier anonymity management options to consumers whose online behavior continues to contradict their data protection concerns. Such a market-based system for anonymity as a valued good would require strict oversight and regulation by government bodies. Establishing a marketplace where individuals have full control over their personal data and, relatedly, their anonymity, might be difficult, but is necessary to ensure individuals' right to online anonymity. Ultimately, by valuing individuals' anonymity, we allow citizens the ability to choose their level of being identifiable or unknown on the Web. By recognizing individuals' right to anonymity online, and full control of their personal data, we can encourage fair usage of the value of personal data, which can fuel a powerful digital economy.

References

Acquisti, A. and Gross, R. (2006), "Imagined communities: awareness, information sharing, and privacy on the Facebook", in Danezis, G. and Golle, P. (Eds), *Privacy Enhancing Technologies: 6th International Workshop, PET*, Cambridge, 28-30 June, Revised Selected Papers, Springer Berlin, Heidelberg, pp. 36-58.

Acquisti, A., John, L.K. and Loewenstein, G. (2013), "What is privacy worth?", *Journal of Legal Studies*, Vol. 42 No. 2, pp. 249-274.

Advertising Age (2013), "Real-time bidding ad revenue to reach $20.8B by 2017", available at: http://adage.com/article/btob/real-time-bidding-ad-revenue-reach-20-8b-2017/290505/ (accessed 1 April 2017).

Alexa.com (2017), "The top 500 sites on the web", available at: www.alexa.com/topsites (retrieved 15 March 2017).

Anthes, G. (2015), "Data brokers are watching you", *Communications of the ACM*, Vol. 58 No. 1, pp. 28-30.

Anthony, S. (2017), "Google Brain super-resolution image tech makes "zoom, enhance!" real: Google Brain creates new image details out of thin air", available at: https://arstechnica.com/information-technology/2017/02/google-brain-super-resolution-zoom-enhance/ (accessed 17 May 2017).

Azechi, S. (2005), "Informational humidity model: explanation of dual modes of community for social intelligence design", *AI & Society*, Vol. 19 No. 1, pp. 110-122.

Barbaro, M., Zeller, T. Jr and Hansell, S. (2006), "A face is exposed for AOL searcher no. 4417749". *New York Times*, p. A1, available at: www.nytimes.com/2006/08/09/technology/09aol.html (accessed 23 March 2017).

Barcena, M.B., Wueest, C. and Lau, H. (2014), "How safe is your quantified self? Tracking, monitoring, and wearable tech", *Symantech*, available at: www.symantec.com/connect/blogs/how-safe-your-quantified-self-tracking-monitoring-and-wearable-tech (accessed 19 April 2017).

Bargh, J.A., McKenna, K.Y.A. and Fitzsimons, G.M. (2002), "Can you see the real me? Activation and expression of the "true self" on the internet", *Journal of Social Issues*, Vol. 58 No. 1, p. 33.

Barnes, M.E. (2006a), "Falling short of the mark: the United States response to the European Union's data privacy directive", *Northwestern Journal of International Law & Business*, Vol. 27 No. 1, pp. 171.

Barnes, S.B. (2006b), "A privacy paradox: social networking in the United States", *First Monday*, Vol. 11 No. 9.

Bauer, C., Korunovska, J., and Spiekermann, S. (2012), "On the value of information – what Facebook users are willing to pay", *ECIS 2012 Proceeding, Paper 197*, Barcelona.

Border, A.C. (2012), "Untangling the web: an argument for comprehensive data privacy legislation in the United States", *Suffolk Transnational Law Review*, Vol. 35, p. 363.

Bowie, N.E. and Jamal, K. (2006), "Privacy rights on the internet: self-regulation or government regulation?", *Business Ethics Quarterly*, Vol. 16 No. 3, pp. 323-342.

Carrascal, J.P., Riederer, C., Erramilli, V., Cherubini, M. and de Oliveira, R. (2013), "Your browsing behavior for a big mac: economics of personal information online", *Proceedings of the 22nd International Conference on World Wide Web ACM*, pp. 189-200.

Castelluccia, C., Olejnik, L. and Minh-Dung, T. (2014), "Selling off privacy at auction", *Network and Distributed System Security Symposium (NDSS)*, San Diego, pp. 1-15.

Christofides, E., Muise, A. and Desmarais, S. (2011), "Hey mom, what's on your Facebook? Comparing Facebook disclosure and privacy in adolescents and adults", *Social Psychological and Personality Science*, Vol. 3 No. 1, pp. 48-54.

Clarke, E. (2013), "The underground hacking economy is alive and well", available at: www.secureworks.com/blog/the-underground-hacking-economy-is-alive-and-well (assessed 23 February 2017).

Cleff, E.B. (2008), "Regulating mobile advertising in the European Union and the United States", *Computer Law & Security Review*, Vol. 24 No. 5, pp. 421-436.

Correa, D., Silva, L.A., Mondal, M., Benevenuto, F. and Gummadi, K.P. (2015), "The many shades of anonymity: characterizing anonymous social media content", *9th International AAAI Conference on Web and Social Media*, AAAI, Palo Alto, CA, pp. 71-80.

de Montjoye, Y.A., Hidalgo, C.A., Verleysen, M. and Blondel, V.D. (2013), "Unique in the crowd: the privacy bounds of human mobility", *Scientific Reports*, Vol. 3 No. 1376.

de Montjoye, Y.A., Radaelli, L., Singh, V.K. and Pentland, A. (2015), "Unique in the shopping mall: on the reidentifiability of credit card metadata", *Science*, Vol. 347 No. 6221, pp. 536-539.

Deighton, J. and Johnson, P.A. (2013), "The value of data: consequences for insight, innovation and efficiency in the US economy", *Direct Marketing Associations's Data Driven Marketing Institute*, pp. 1-105, available at: https://thedma.org/wp-content/uploads/DDMI-Summary-Analysis-Value-of-Data-Study.pdf (accessed 29 March 2017).

Ehrenberg, B. (2014), "How much is your personal data worth?", *The Guardian*, 24 April, available at: www.theguardian.com/news/datablog/2014/apr/22/how-much-is-personal-data-worth (accessed 15 March 2017).

European Parliament and Council of the European Union (1995), "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", *Official Journal of the European Communities*, available at: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (accessed 23 March 2017).

Facebook. (2017), "Facebook reports fourth quarter and full year 2016 results", available at: https://investor.fb.com/investor-news/press-release-details/2017/facebook-Reports-Fourth-Quarter-and-Full-Year-2016-Results/default.aspx (accessed 12 April 2017).

Fang, X., Sheng, O.R.L. and Goes, P. (2013), "When is the right time to refresh knowledge discovered from data?", *Operations Research*, Vol. 61 No. 1, pp. 32-44.

Federal Deposit Insurance Corporation. (2017), "Understanding deposit insurance", available at: www.fdic.gov/deposit/deposits/ (accessed 5 March 2017).

Flinn, B. and Maurer, H. (1996), "Levels of anonymity", in Maurer, H., Calude, C. and Salomaa, A. (Eds), *The Journal of Universal Computer Science: Annual Print and CD-ROM Archive Edition Volume 1*, Springer, Berlin, pp. 35-47.

Fogel, J. and Nehmad, E. (2009), "Internet social network communities: risk taking, trust, and privacy concerns", *Computers in Human Behavior*, Vol. 25 No. 1, pp. 153-160.

Gartner (2016), "Gartner mobile app survey reveals 24 percent more spending on in-app transactions than on upfront app payments", available at: www.gartner.com/newsroom/id/3331117 (accessed 12 February 2017).

Golle, P. (2006), "Revisiting the uniqueness of simple demographics in the US population", *Proceedings of the 5th ACM workshop on Privacy in electronic society*, *ACM*, *Alexandria, VA*, pp. 77-80.

Goodwin, D. (2017), "Vizio smart TVs tracked viewers around the clock without consent: manufacturer will pay $2.2 million and delete data to settle privacy-invasion charges", available at: https://arstechnica.com/tech-policy/2017/02/vizio-smart-tvs-tracked-viewers-around-the-clock-without-consent/ (accessed 12 April 2017).

Hann, I.H., Hui, K.L., Lee, T. and Png, I. (2002), "Online information privacy: measuring the cost-benefit trade-off", *Proceedings of the International Conference on Information Systems, ICIS*, *DBLP, Barcelona*.

Hayne, S.C. and Rice, R.E. (1997), "Attribution accuracy when using anonymity in group support systems", *International Journal of Human-Computer Studies*, Vol. 47 No. 3, pp. 429-452.

Hoy, M.G. and Milne, G. (2010), "Gender differences in privacy-related measures for young adult Facebook users", *Journal of Interactive Advertising*, Vol. 10 No. 2, pp. 28-45.

Hughes, S. and Johnson, J. (2016), "Encryption apps see growth after election", available at: www.marketplace.org/2016/11/15/world/encryption-app-signal-sees-400-growth-election (assessed 9 May 2017).

Johnson, L. (2016), "Google's ad revenue hits $19 billion, even as mobile continues to pose challenges", available at: www.adweek.com/digital/this-startup-is-helping-speed-up-how-publishers-and-advertisers-create-social-videos/ (accessed 2 May 2017).

Klein, J. (2013), *Reputation Economics: Why Who You Know is Worth More Than What You Have*, Palgrave Macmillan, New York, NY.

Kotler, P. (1997), *Marketing Management: Analysis, Planning, Implementation, and Control*, Prentice Hall, Upper Saddle River, NJ.

Krasnova, H., Hildebrand, T. and Guenther, O. (2009), "Investigating the value of privacy on online social networks: conjoint analysis", *13th International Conference on Information Systems, Paper 173*, AISel, Pheonix, pp. 1-18.

Krause, A. and Horvitz, E. (2010), "A utility-theoretic approach to privacy in online services", *Journal of Artificial Intelligence Research*, Vol. 39 No. 1, pp. 633-662.

Kuempel, A. (2016), "The invisible middlemen: a critique and call for reform of the data broker industry", *Northwestern Journal of International Law & Business*, Vol. 36 No. 1, pp. 207-234.

Lapidot-Lefler, N. and Barak, A. (2012), "Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition", *Computers in Human Behavior*, Vol. 28 No. 2, pp. 434-443.

Mangold, W.G. and Faulds, D.J. (2009), "Social media: the new hybrid element of the promotion mix", *Business Horizons*, Vol. 52 No. 4, pp. 357-365.

Marx, G.T. (1999), "What's in a name? Some reflections on the sociology of anonymity", *Information Society*, Vol. 15 No. 2, pp. 99-112.

Mayfield, J. (2015), "FTC requests bankruptcy court take steps to protect RadioShack consumers' personal information", Letter to Consumer Privacy Ombudsman Describes Possible Conditions on Sale of Data, Federal Trade Commission, available at: www.ftc.gov/news-events/press-releases/2015/05/ftc-requests-bankruptcy-court-take-steps-protect-radioshack (accessed 25 February 2017).

Meeco (2017), "Why Meeco", available at: https://meeco.me/why-meeco.html (accessed 12 April 2017)

Miyazaki, A.D. and Krishnamurthy, S. (2002), "Internet seals of approval: effects on online privacy policies and consumer perceptions", *Journal of Consumer Affairs*, Vol. 36 No. 1, pp. 28-49.

Moorhead, S.A., Hazlett, D.E., Harrison, L., Carroll, J.K., Irwin, A. and Hoving, C.. (2013), "A new dimension of health care: systematic review of the uses, benefits, and limitations of social media for health communication", *Journal of Medical Internet Research*, Vol. 15 No. 4, p. 16.

Morando, F., Iemma, R. and Raiteri, E. (2014), "Privacy evaluation: what empirical research on users' valuation of personal data tells us", *Internet Policy Review*, Vol. 3 No. 2, pp. 1-11.

Morio, H. and Buchholz, C. (2009), "How anonymous are you online? Examining online social behaviors from a cross-cultural perspective", *AI & Society*, Vol. 23 No. 2, pp. 297-307.

Narayanan, A. and Shmatikov, V. (2008), "Robust de-anonymization of large sparse datasets", *IEEE Symposium on Security and Privacy*, IEEE Computer Society, Washington, DC, pp. 111-125.

Narayanan, A. and Shmatikov, V. (2009), "De-anonymizing social networks", *IEEE Symposium on Security and Privacy*, IEEE Computer Society, Oakland, CA, pp. 173-187.

Nielsen (2015), "Screen wars: the battle for eye space in a TV-everywhere world", available at: www.nielsen.com/us/en/insights/reports/2015/screen-wars-the-battle-for-eye-space-in-a-tv-everywhere-world.html (accessed 11 February 2017).

Ohm, P. (2010), "Broken promises of privacy: responding to the suprising failure of anonymization", *UCLA Law Review*, Vol. 57, pp. 1701-1777.

Olmstead, K., Lampe, C. and Ellison, N.B. (2015), "Social media and the workplace: Pew Internet & American Life Project", From Pew Internet Institute, available at: www.pewinternet.org/2016/06/22/social-media-and-the-workplace/ (accessed 19 February 2017).

Pavlou, P.A.A. (2003), "Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model", *International Journal of Electronic Commerce*, Vol. 7 No. 3, pp. 69-103.

Pfitzmann, A. and Köhntopp, M. (2001), "Anonymity, unobservability, and pseudonymity: a proposal for terminology", in Federrath, H. (Ed.), *Designing Privacy Enhancing Technologies*, Springer Berlin, Heidelberg, pp. 1-9.

Pollach, I. (2007), "What's wrong with online privacy policies?", *Commununications of the ACM*, Vol. 50 No. 9, pp. 103-108.

ProtonMail (2017), "Ask your question: message expiration", available at: https://protonmail.com/support/knowledge-base/expiration/ (accessed 4 April 2017).

Rainie, L., Kiesler, S., Kang, R. and Madden, M. (2013), "Anonymity, privacy, and security online", From Pew Internet Institute, available at: www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/ (accessed 7 June 2017).

Rawls, J. (2001), *Justice as Fairness: A Restatement*, Harvard University Press, Cambridge, MA.

Robinson, S.C. (2015), "The good, the bad, and the ugly: applying rawlsian ethics in data mining marketing", *Journal of Media Ethics*, Vol. 30 No. 1, pp. 19-30.

Robinson, S.C. (2017), "Disclosure of personal data in ecommerce: a cross-national comparison of Estonia and the United States", *Telematics and Informatics*, Vol. 34 No. 2, pp. 569-582.

Savage, S. and Waldman, D. (2015), "Privacy tradeoffs in smartphone applications", *Economics Letters*, Vol. 137 No. 3, pp. 171-175.

Schiffer, A. (2016), "In sports authority bankruptcy, customer e-mail data commands hefty sum", *Los Angeles Times*, available at: www.latimes.com/business/la-fi-sports-authority-auction-20160629-snap-story.html (accessed 7 June 2017).

Schoeman, F.D. (1992), *Privacy and Social Freedom*, Cambridge University Press, Cambridge.

Schwartz, P.M. and Solove, D.J. (2014), "Reconciling personal information in the United States and European Union", *California Law Review*, Vol. 102 No. 4, pp. 877-916.

Shipley, D. (2015), "Anonymity is a threat to E-Commerce", *Bloomberg News*, 26 October, available at: www.bloomberg.com/view/articles/2015-10-26/amazon-s-case-against-fake-reviews-is-strong (accessed 9 March 2017).

Sidgman, J. and Crompton, M. (2016), "Valuing personal data to foster privacy: a thought experiment and opportunities for research", *Journal of Information Systems*, Vol. 30 No. 2, pp. 169-181.

Simonite, T. (2014), "Sell your personal data for $8 a month", *MIT Technology Review*, 12 February, available at: www.technologyreview.com/s/524621/sell-your-personal-data-for-8-a-month/ (accessed 5 January 2017).

Smith, A. (2014), "Half of online Americans don't know what a privacy policy is", Pew Internet Institute, available at: www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/ (accessed 12 March 2017).

Snapchat.com (2017), "Snapchat support: snaps", available at: https://support.snapchat.com/en-US/about/snaps (accessed 12 April 2017).

Staiano, J., Oliver, N., Lepri, B., de Oliveira, R., Caraviello, M. and Sebe, N. (2014), "Money walks: a human-centric study on the economics of personal mobile data", *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, ACM*, pp. 583-594.

Statista.com (2017), "Most famous social network sites worldwide as of April, ranked by number of active users (in millions)", available at: www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (accessed 12 May 2017).

Suler, J. (2004), "The online disinhibition effect", *Cyber Psychology & Behavior*, Vol. 7 No. 3, pp. 321-326.

Tufekci, Z. (2008), "Can you see me now? Audience and disclosure regulation in online social network sites", *Bulletin of Science, Technology & Society*, Vol. 28 No. 1, pp. 20-36.

United States Government Accountability Office (2008), "Privacy: alternatives exist for enhancing protection of personally identifiable information", available at: www.gpo.gov/fdsys/pkg/GAOREPORTS-GAO-08-536/content-detail.html (accessed 20 March 2017).

United States Senate Office of Oversight and Investigations (2013), "A review of the data broker industry: collection, use, and sale of consumer data for marketing purposes", Washington, DC, available at: www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf (accessed 9 June 2017).

Whiting, A. and Williams, D. (2013), "Why people use social media: a uses and gratifications approach", *Qualitative Market Research*, Vol. 16 No. 4, pp. 362-369.

Yao, M.Z., Rice, R.E. and Wallis, K. (2007), "Predicting user concerns about online privacy", *Journal of the American Society for Information Science & Technology*, Vol. 58 No. 5, pp. 710-722.

Youn, S. and Hall, K. (2008), "Gender and online privacy among teens: risk perception, privacy concerns, and protection behaviors", *Cyber Psychology & Behavior*, Vol. 11 No. 6, pp. 763-765.

Yurchisin, J., Watchravesringkan, K. and Brown McCabe, D. (2005), "An exploration of identity re-creation in the context of internet dating", *Social Behavior & Personality*, Vol. 33 No. 8, pp. 735-750.

Corresponding author

Stephen Cory Robinson can be contacted at: cory.robinson@liu.se