DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

Mexican Law Review
New Series
VOLUME XII
Number 2

LEGAL RECOGNITION OF THE DIGITAL TRADE IN PERSONAL DATA

Itzayana TLACUILO FUENTES*

ABSTRACT: *In the digital world, millions of consumers transfer their personal data to access and use new Internet technologies every day. The technology industry is making immense profits from this data. It is a social and economic fact that peoples' personal data is used as an asset in the digital economy. Should consumers be compensated for the value of their personal data? This article argues that it is time to legally recognize the trade in personal data. As a response to increasing cross-border flows, governments protect personal data with privacy frameworks. However, it remains the decision of the consumer to give consent for the transfer of their data. This article proposes that an international framework that recognizes the trade of personal data could generate proper protection for the digital trade, while incentivizing free cross-border data flows and allowing the market to determine the value of the personal data. Moreover, consumers could share in the profits made from their personal information and will personally control their information and privacy. The use of personal data as an asset is a reality that can no longer be avoided. It is necessary to create legal standards to make trade of personal data more transparent, efficient and fair. This article aims to explore the idea of trading in one's personal data is not a surrealistic scenario, rather, in practice this trade already exists.*

KEYWORDS: *Digital Trade, Personal Data, Cross-border Data Flows, Digital Economy, Privacy Framework, Consumer, and Ownership Rights.*

RESUMEN: *En el mundo digital, cada día millones de consumidores transfieren sus datos personales con el objetivo de acceder y utilizar las nuevas tecnologías en Internet. La industria tecnológica obtiene una enorme ganancia de estos datos. Es un factor social y económico que los datos personales se utilizan como un activo en la economía digital. ¿Deberá el consumidor ser compensado por el valor de sus datos personales? Este artículo argumenta que es tiempo de reconocer legalmente el comercio de datos personales. Como respuesta al creci-*

* Master of Laws (LL.M.) in the University of Melbourne, Australia. Trained as a lawyer at the National Autonomous University of Mexico (UNAM), Mexico; Bachelor's Degree with Honors. Email: *itzayana.tlacuilo@gmail.com*.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

miento del flujo de datos transfronterizos, algunos gobiernos protegen los datos personales con marcos de privacidad. Sin embargo, el consumidor puede dar su consentimiento para la transferencia de sus datos. Este artículo sostiene que un marco internacional que reconozca el comercio de datos personales generará una protección adecuada para el comercio digital, incentivará los flujos de datos transfronterizos libres y permitirá que el mercado determine el valor de los datos personales. Adicionalmente, el consumidor compartirá la ganancia obtenida por su información personal y controlará sus datos y privacidad. El uso de datos personales como un bien es una realidad que no puede seguir en negación. Es necesario crear estandares legales para comercializar con datos personales en una forma transparence, eficaz y justa. Este artículo tiene como objetivo comunicar al lector que la idea de comercializar con los datos personales para nada es surrealista ya que en práctica existe.

Palabras Clave: *Comercio Digital, Datos Personales, Flujo de Datos Transfronterizos, Economía Digital, Marco de Privacidad, Consumidor y Derecho de Propiedad.*

Table of Contents

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

I. Introduction

Every day consumers input their personal data to access and use websites, social media, Internet of Things (IoT), and different available technologies. In this regard, cross-border data flows have exponentially increased in the digital world. Personal data has become an asset used by technology companies for profit. However, consumers are not adequately compensated for the value of their data.

Personal data flows are a social and economic reality that can no longer be avoided. This article argues that the trade of personal data should be legally recognized in an international context. The legal status given to such data will incentivise digital trade since cross-border data flows will not be restricted, and a new market will be legalised and protected. Moreover, consumers would share the profits generated by their own data.

The response of governments to the evolution of digital trade has been the creation of privacy policies to protect personal data. One main concern is the risk of misuse of personal data when transferred across borders, at the same time, there is concern that overprotection of this data might harm trade. If personal data were to be considered a tradable asset, trade regulations would have to cope with a privacy framework. This article argues that privacy law is ancillary protection to the consumer, as through consent the trade is possible. Is it time to legally accept personal data as a tradable good?

There are three main reasons for recognizing personal data as a tradable asset. First, the data subject, the consumers that are active on the Internet, should share the profit made out of their personal information and should be the one controlling their own information and privacy. Second, companies are legally protected if the data subject/owner consents to the use of personal data. Third, digital trade could benefit as data trading becomes recognized by the law, cross-border data flows would become more free and responsive to the market, leading to enhanced competitiveness and innovation in the data economy,[1] as the value of personal data is freely determined by unrestricted supply and demand.

This article does not discuss whether personal data should be treated as a good rather than a service, this distinction is a matter best left to research.[2]

[1] European Commission, Building a European Data Economy, COM (2017) 9 final (2017).

[2] For practical reasons, this article will name the trade of personal data as a good.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

The important thing here is that personal data is considered a tradable asset. This study emphasises the benefits and needs for individual's personal data to be regulated as an object of trade. It is structured in four substantive parts. Part I introduces the reader in the subject matter of this article. Part II gives a general overview of personal data, its use and cross-border transfer. Part III examines profits generated from cross-border data flows. Part IV outlines the possible constraints a legal framework that accepts personal data as a tradable asset might face. This article concludes that personal data is an asset in the digital economy, and posits that recognising the right to trade with it will contribute to freeing digital trade.

II. Personal Data

In the digital era, everyday users of the Internet, IoT, and new technologies input personal data to access websites, smartphones, GPS, apps, social media, e-commerce, and a massive array of options that new technologies have to offer. High tech companies are collecting this personal information to make a profit out of it. This article argues that the users should enjoy compensation for the use of their personal data.

This section gives background on essential aspects of the transfer of personal data, defining the type of personal data that the article will refer to. The use of personal data will then be examined, to understand how the companies collect personal data. Finally, this section will look at the fact that data is exchanged through the Internet, causing cross-border data flows and generating legal and commercial consequences.

1. *Defining Personal Data*

There is a range of definitions of personal data. These definitions depend on whether the data is related to an identifiable natural person, and the strength of that link. The differentiation between 'personal data' and 'non-personal data' remains in force.[3] In the broadest sense, 'personal data' could be considered the DNA of a person, which would thus be subject to human rights. However, 'non-personal' data, which is included in personal data, is data produced by the person, it is this 'non-personal data' that is the subject of this article, however, it will be referred to as personal data.

To clarify which type of data is included in this definition, this section includes an analysis of the researcher Václav Janeček, who divides personal data between extrinsically and intrinsically private. Janeček's classification fol-

[3] *See* Nadezhda Purtova, *Do Property Rights in Personal Data Make Sense after the Big Data Turn?: Individual Control and Transparency*, 10(2) Journal of Law and Economic Regulation, Tilburg Law School 27 (2017).

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

lows the traditional contrast between personal and non-personal data.[4] According to Janeček, intrinsically personal data contain "intrinsically private information",[5] controlling it is like controlling one's identity. However, not all personal data are intrinsically personal, as regards for example GPS data, IP addresses, or data held in personal task managers. Janeček argues that this type of data is personal only extrinsically and therefore does not face the same conceptual, ethical, and legal issues as intrinsically private data.[6] Thus extrinsically private data can be the object of transactions.

Whether it is called extrinsically private or non-personal data, it is clear that there is a type of personal data produced by the users of the Internet, especially consumers, that is used to create economic value. International law has to be revolutionary and legally recognize personal data is an asset subject to ownership and to trade. This article proposes that the trade of personal data is only possible for extrinsically private personal data, since this does not attempt against the privacy of the individual, as he or she can consent (or veto) the exchange of this type of information.

2. *Use of Personal Data*

This section examines how online consumers use data to interact on the Web. At the same time data is used by the subject, it is collected by third parties, for example, by websites. Given the full range of possibilities for collecting personal data, individuals use their data to interact. For example, through blog accounts, social media, e-commerce, gadgets known as IoT and even by interacting with government bureaus such as health, tax, or finance.

The Privacy Guidelines of the organization for Economic Co-operation and Development (OECD) considers personal data the following type of information:[7]

- User-generated content: blogs, commentaries, photos and videos;
- Activity or behavioural data: what people search for, what they buy online and the methods of payment;
- Social data: for instance, social networking sites;
- Locational data: residential addresses, GPS and geo-location and IP address;
- Demographic data: age, gender, race, income, sexual preferences, and political affiliation;

[4] *See* Václav Janeček, *Ownership of Personal Data in the Internet of Things*, 34(5) Computer Law & Security Review 1039–1502 (2018).

[5] *Id.*

[6] *Id.*

[7] OECD Privacy Guidelines *(2013)*, Jul. 11, 2013, OECD (2013).

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

- Data of an official nature: financial information, account numbers, health information, national health or social security numbers, and police records.[8]

The data is created by and about people. The World Economic Forum divides personal data in three: (a) volunteered data, which is created and explicitly shared by individuals, for example in social network profiles; (b) observed data, captured by recording the actions of individuals, for example through IoT; and, (c) inferred data about individuals based on the analysis of observed information, for example by the purchase history.[9]

Statistics show that on an average day, users send around 47 billion emails and submit 95 million "tweets" on Twitter[10]. Each month, users share about 30 billion pieces of content on Facebook. [11] According to the International Data Corporation, in 2010 individuals' actions generated about 70 percent of digital data. This data is created by activities such as sending emails, taking digital pictures, turning on mobile phones or posting content online.[12]

These statistics demonstrate how personal data is required to interact in the digital society. Hence, individuals become creators and users of their data, and become the subject and the object of their data. From the individual perspective, one must use data to cope with the demands of everyday modern life.[13]

3. *Cross-Border Data Flows*

The data that is uploaded to the Internet technically does not face border barriers because physical jurisdictions do not restrict the Internet and the digital space. It is well known that the Internet enables the possibility of people interacting with one another across the globe. The same case applies to consumers using Websites from different parts of the world. "Cross-border

---

[8] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers 220 (Apr. 2, 2013) *https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.*

[9] *See* The World Economic Forum, *Personal Data: The Emergence of a New Asset Class,* The World Economic Forum 40 (2011).

[10] *See* Kevin Thau, *Twitter + Ping = Discovering More Music*, Twitter Blog, Nov. 11 2010, *https://blog.twitter.com/en_us/a/2010/twitter-ping-discovering-more-music.html.*

[11] The World Economic Forum, *supra* note 9.

[12] *Id.*

[13] The generalisation applies to the people that have access to the Internet and IoT. Statista measured that in July 2018, over 4.1 billion people were active internet users and 3.3 billion were social media users.

See also Statista, *Global Digital Population as of July 2018 (in Millions),* Statista, Jul. 2018, *https://www.statista.com/statistics/617136/digital-population-worldwide/.*

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

data flow refers to the movement of personal information (or data) across national borders".[14]

The use of the Internet facilitates the exchange of personal data without border restrictions. Huge corporations enable the movement of personal data within different jurisdictions, for example, Facebook, Google, Amazon and Twitter.

Today, international businesses are handling customer data in many areas. These cross-border data flows have raised concerns for governments in different countries. One key worry is that personal information may be at risk. For example, in 2005, undercover reporters from the Australian Broadcasting Corporation "were allegedly offered for sale personal data of 1,000 Australians for around US$10 per person."[15] Governments argue that data is more secure if it is locally stored since they are in a better position to enforce privacy regulations. [16]

As privacy protection is on the agenda of several countries, there is an increasing tendency to regulate cross-border data flows. These changes in the global policy include administrative requirements such as consumer consent, the right to be forgotten, and sanctions for non-compliance.[17]

On the contrary, some academics and businesspeople argue that too much data regulation may block trade. The OECD issued a report that compares the nexus between policy motivations and cost considerations. It stated: "While there are legitimate policy concerns associated with cross-border data flows, there is a growing sense of danger in the business community that these measures are being put in place without a proper analysis of their trade-inhibiting effects and with little guarantee that privacy concerns will be addressed."[18]

While it is crucial that policy barriers address issues cross-border data flows may face, the focus of this article is not the actions that governments have taken to protect personal data. Rather, the concern is connected to the legal rights that consumers should have concerning their data and how that is related to the trade. The privacy issue is a secondary aspect that will be addressed later on, but only as it relates to available protection to the consumer, not as compensation for consumer data.

In this sense, the importance of the cross-border data flows to this article is that the data has value across borders and industries. The following sec-

---

[14] *APEC Privacy Framework (2015),* APEC#217-CT-01.9 (Reports) 8493, (2015).

[15] *See* Australian Law Reform Commission, *Cross-Border Data Flows,* Australian Government (Aug. 16, 2010), *https://www.alrc.gov.au/publications/31.%20Cross-border%20Data%20Flows%20/introduction*.

[16] *See* OECD, *Working Party of the Trade and Agriculture Directorate,* 56, *Emerging Policy Issues: Localisation Barriers to Trade*, TAD/TC/WP (2014)17/FINAL (May 12, 2015).

[17] *See* L. Lee Tuthill, *Cross-Border Data Flows: What Role for Trade Rules?*, in Research Handbook on Trade in Services 357 (Pierre Sauvé and Martin Roy eds., 2016).

[18] OECD, *supra* note 7.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

tion will delve more extensively into the implications these flows have on the digital trade.

III. Profit and Cross-Border Data Flows

Trade today is associated with data crossing borders in at least some element of the transaction or as the product itself. [19] It is recognized that data has value across borders and industries. However, the value is different from the one attributed to physical commodities such as oil.[20] According to the Swedish National Board of Trade, "companies need to transfer data to trade." [21]

Personal data is used by corporations and governments as a means to make a profit. Increasingly, consumers are seeking a share of that profit; however, it is still unclear how they are to be compensated for the transfer of their data. This article proposes that the trade in personal data should be legally recognized and organized by a legal framework. The data flow would then be more free and responsive to market supply and market demand. Furthermore, the legal recognition of trade of personal data would ensure the exchange of personal data on the Internet is transparent.

This section analyses the value in the personal data itself, subject to the transaction, as well as the value that corporations, government and consumers secure from this data. Studies show that consumers can obtain a profit from their personal data.

1. *The Value of Personal Data*

Personal data is an essential asset in today's digital society. There have been several studies to estimate the economic value of personal data, this value is of interest to corporations, governments, and consumers (who themselves are the source of the data).

In 2012, the Boston Consulting Group published a report called *The Value of Our Digital Identity*. It shows that the value of personal data can be massive. The report projects to the year 2020. Data is estimated to be worth €1 trillion in Europe, and for European businesses and governments, the use of personal data will deliver an annual benefit of €330 billion. It is the public sector and health care that are expected to profit the most, totalling 40 per cent of their total organizational revenues. For the data of individuals, the value will be €670 billion.[22] The consumer value is generated via reduced

[19] OECD, *supra* note 7.

[20] *See* Michael Mandel, *The Economic Impact of Data: Why Data Is Not Like Oil*, Progressive Policy Institute 20 (2017).

[21] Tuthill, *supra* note 17.

[22] *See* John Rose, Olaf Rehse and Björn Röber, *The Value of Our Digital Identity,* The Boston

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

prices, time savings through self-service transactions, and the valuation of free online services.[23]

A World Economic Forum study published in 2010 highlighted the relevance of personal data as an economic asset that could be perceived as the new "oil."[24] It classifies the use of personal data as a product in itself and as a primary component of varied economic activities.[25]

US based Data Driven Marketing Institute published a report on the role of Individual-Level Consumer Data (ILCD). In providing marketing services, the value was around $156 Billion in 2012. According to this study, the most substantial contribution to the economic value of data-driven market economies is the exchange of ILCDs between firms.[26]

The OECD carried out a study which identifies the monetary value of personal data to a firm. The value can be calculated by the stock value, by the revenues or by the price of data records on the market. Alternatively, it can be calculated by the costs of a data breach and through the price of personal data on an illegal market.[27] In addition, *The Financial Times* published an interactive sheet calculating market prices for specific sorts of data, such as demographic data, family and health data, property, leisure activities, and consumer data.[28]

These studies show that personal data is being used as an asset by corporations and even by governments. The questions that this article raises are: which is the value associated to the consumers for their own data, and how they should be compensated? In this article data subjects are generalised as consumers because they give their information in exchange for a free service; while interacting through e-commerce, surveys, or other activities that involve economic values such as a good or a service.

The Boston Consulting Group found that consumers, with an awareness of how their data is used, require 26 per cent more benefit in return for sharing their data. [29] Consumers that can manage their privacy are up to 52

Consulting Group, Nov. 20, 2012, *https://www.bcg.com/publications/2012/digital-economy-consumer-insight-value-of-our-digital-identity.aspx*.

[23] *See* Marc Van Lieshout, *The Value of Personal Data*, in Privacy and Identity Management for the Future Internet in the Age of Globalisation 26 (Jan Camenisch, Simone Fischer-Hubner and Marit Hansen eds., 2015).

[24] The World Economic Forum, *supra* note 10.

[25] Van Lieshout, *supra* note 23.

[26] Van Lieshout, *supra* note 23.

[27] *See* OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value* (OECD Digital Economy Papers No 220, OECD, 2 April 2013) *https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en* ('*Exploring the Economics of Personal Data*').

[28] *See* Emily Steel et al., *How Much Is Your Personal Data Worth?*, Financial Times, June 13, 2013.

[29] Rose, Rehse and Röber, *supra* note 22.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

per cent more willing to share information against those who are not able to manage their privacy. Thus, privacy controls and sufficient benefits, mean consumers are more willing to share their data.[30] The Boston Consulting Group's study reflects that consumers need to perceive the benefits of sharing their data in order to ensure the flow of data in the digital market. As an additional argument, privacy would be secured if the consumer is involved directly in the control of their information.

Mainly the corporations and the governments make profit out of the value of the personal data. Since consumers are the source of the data, they should share the economic benefit from it. The previous studies show that personal data can produce value for the consumer. The remaining question is how the consumer will receive the benefits of such an asset.

2. *The Market*

Access to the Internet has given rise to a number of data-sharing practices. Through different platforms, people share details about their location, their mood and their activities. They leave traces with their smartphones and devices, or through their click behaviour. The value of this information is well understood by marketers, who collect as much data about personal behaviours and preferences as possible. More data allows these marketers to follow purchasing habits and strategies, and make targeted offers to consumers.[31]

The highest economic value of the new tech companies is their access to data. We live in a multidirectional trade market where within the Internet everyone trades with everyone; and data is the product and the service. The global integration of business has become dependent on Information Technology (IT) and data.[32] Similarly, governments are making a profit out of data collection and its use within public services. This section analyses the current market with regards to personal data.

A. *Corporations*

The exponential growth of tech companies was spurred by collecting, aggregating, analysing and monetising personal data. Innovative businesses are built on the economics of personal data, as is the case with Google, Facebook and Instagram.[33] Besides using personal data in social media companies or tech companies, a market of personal data brokers has emerged, in this market, data is the product. Data brokers are entities that collect information

30 Rose, Rehse and Röber, *supra* note 22.

31 Van Lieshout, *supra* note 23.

32 Tuthill, *supra* note 17.

33 The World Economic Forum, *supra* note 10.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

about consumers and sell it to other data brokers, companies, and individuals. They can be divided into three categories: sites for finding persons, data brokers that focus on marketing, and data brokers who offer risk mitigation products to verify identities and help detect fraud.[34]

There is a cluster of major data brokers in the marketing field. The first is Acxiom. In the early 1980s, Acxiom pioneered the business model of collecting data on people, segmenting that data and selling it to be used in marketing. It is described as "the biggest company you have never heard of" by Bernard Marr.[35] Currently, Acxiom's data is said to be used to make 12 percent of direct marketing sales in the US.[36] The second is Nielsen. It has been in the market since 1923 and has established itself as a leader in market research and ratings. Nielsen is active in gathering data on consumers from 100 different countries.[37]

The third is Experian. This company combined credit scoring with database and marketing expertise to offer its services, initially to financial industries and then to all sectors. It also sells data directly to consumers by offering insights into their creditworthiness. In 2011, Experian reported total revenues of US$4.2 billion realised over 600 million individual records and 60 million business data records. [38]

Large service providers such as Google and Apple have also become personal data brokers. Today, Google owns brokers such as AdMob and Double Click. Apple has its own ad-broker with iAd. The ad-broker sector is growing. For example, BlueKai[39] offers a data exchange platform that captures more than 30,000 attributes over 300 million users. [40]

Besides their role as data brokers, multinational corporations such as Facebook, Google and Twitter are monitoring everything we do. They probably know as much, or more, about us. Apparently these companies offer their services for free; however, their economic profit comes from the users' data.

The famous Cambridge Analytic Scandal led Mark Zuckerberg to admit that Facebook not only provides data to advertisers but works for them. Face-

---

[34] *See* Yael Grauer, *What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?,* Motherboard, Mar. 28, 2018, *https://motherboard.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection*.

[35] *See* Bernard Marr, *Where Can You Buy Big Data? Here Are The Biggest Consumer Data Brokers,* Forbes 1, September 7, 2017.

[36] *Id.*

[37] *Id.*

[38] Marr, *supra* note 35.

[39] *Cf.* BlueKai is a cloud-based big data platform that enables companies to personalise online, offline, and mobile marketing campaigns.

Oracle, *Oracle Buys BlueKai*, Oracle and Bluekai (Feb. 24, 2014), *https://www.oracle.com/corporate/acquisitions/bluekai/*.

[40] Van Lieshout, *supra* note 23.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

book makes its money through advertising.[41] In 2017, Facebook made US$40 billion in revenue from which 39.9 billion came from digital advertisements,[42] primarily Facebook Ads, which target user profiles.

Google is well known for its famous search engine, email service, web browser, as well as a host of online tools we use daily. Its revenue in 2017 was of US$110.8 Billion, gained mainly from its proprietary advertising service, Google AdWords. It works in the following way: when one uses Google to search for anything, one is given a list of search results generated by Google's algorithm. This algorithm provides the most relevant results, accompanied by related suggested pages from an AdWords advertiser. Advertisers pay Google each time a visitor clicks on their advertisement.[43]

The economic profit from personal data for corporations is in the realm of billions of dollars, mainly in the advertisement business and in data analytics. Hence, the importance of gathering, controlling, analysing and selling data is massive. It isn't only advertising companies, but also specific companies like data brokers and social media corporations, use personal data as their main asset.

B. *Government*

An increasing tendency is for governments and public sector institutions to use data as a public utility. E-governance initiatives can improve the efficiency and effectiveness of communication among public organizations and with citizens.[44] Governments gather personal information through different portals. For instance, the government of Mexico collects official tax declarations through its online portal.[45]

Government agencies also use personal data to deliver a range of services, including health, education, welfare and law enforcement.[46] Moreover, government demands for data held by the private sector have increased. This is called systematic access, and is divided into two types: direct access by the government to private-sector databases or networks, and government access to data mediated by the company that maintains the database or network.[47]

---

41 *Cf.* Ben Gilbert, *How Facebook Makes Money from Your Data, in Mark Zuckerberg's Words,* Business Insider Australia, April 12, 2018.

42 *Cf.* Rakesh Sharma, *How Does Facebook Make Money?*, Investopedia, Jul. 25, 2018, *https://www.investopedia.com/ask/answers/120114/how-does-facebook-fb-make-money.asp.*

43 *Cf.* Eric Rosenberg, *How Google Makes Money,* Investopedia, Oct. 9, 2018, *https://www.investopedia.com/articles/investing/020515/business-google.asp.*

44 The World Economic Forum, *supra* note 9.

45 *E.g,.* 'Portal de Trámites y Servicios - SAT', *https://www.sat.gob.mx/personas*.

46 The World Economic Forum, supra note 9.

47 *See* Ira S. Rubinstein et al., *Systematic Government Access to Personal Data: A Comparative Analysis*, 4(2) International Data Privacy Law 96 (2014).

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

In 2014, the *Harvard Business Review* published an article titled "How Cities Are Using Analytics to Improve Public Health." Two examples in which personal data was used were described. In one, the Chicago Department of Public Health (CDPH) in association with the Department of Innovation and Technology, identified data related to food establishments and their locations. Using this data, they constructed models that calculated a score for every food establishment, "with higher scores correlating with an increased risk of critical public health violations." [48] In the other, the city of Chicago partnered with the Eric & Wendy Schmidt Data Science for Social Good Fellowship at the University of Chicago (DSSG) to develop a model to better predict which homes are more likely to have lead-based paints (lead presents a severe health risk, particularly for children who are exposed to it). The DSSG used the data from home inspection records, assessor value, history of blood lead level testing, census data and other factors.[49]

The public sector uses personal data and analytics of that data to improve their services. Governments are starting to be aware of the use they can give to all this big data. Furthermore, while implementing e-governance, governments collect sensitive data, including financial information, which generates economic value even if a privacy framework protects it.

3. *The Consumer's Perspective*

While the market of personal data is apparent in the private sector and visible in the public sector, the value of this data to the individuals themselves is unclear. This section examines different cases to demonstrate how individual users have attempted to make a profit out of their personal data.

A. *Personal Data For Sale*

In 2014, Shawn Buckles set up an online auction to sell his personal data to the highest bidder. He offered a one-year subscription to his profile, his location tracking records, his train tracking records, his calendar, his email conversations, his online conversations, his consumer preferences, his browsing history, as well as his thoughts to the firm that offered the highest price. The winner was The Next Web who paid €350 for it.[50]

---

[48] *Cf.* Keck School of Medicine, University of Southern California, *Big Data and Public Health*, Master of Public Health Online (Online), 2018, *https://mphdegree.usc.edu/resources/articles/big-data-and-public-health/*.

[49] *Id.*

[50] *Cf.* Shawn Buckles, *For $ale Personal Data*, Personal Data: I will sell you my soul, Apr. 12, 2014, *http://shawnbuckles.nl/dataforsale/*.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

As part of his project, Shawn Buckles made a pamphlet to raise awareness about the commercialisation of personal data and the consequences for privacy. He showed that people could attribute a specific monetary value to their personal data.

This case was an individual project, which showed that personal data can be publicly commercialized. The importance of this project was not the monetary amount Shawn Buckles won, but rather it was the demonstration that an individual has the possibility of making a profit out of their own data, which in any case is already being collected by major corporations or governments. What would have happened if instead of Shawn Buckles acting alone, the offer to sell personal data was drawn up by a group of people?

Data clearly has a value, but it is up to every person to claim it. Instead of being benefited by the use of free services, such as Facebook or Google, consumers should enjoy economic compensation for the data they introduce into the Internet. The case of Shawn Buckles proves it is possible.

B. *Surveys and Apps*

The Internet is full of new ideas and ways to make money. The advertising market has reached a point where they pay consumers for responding to surveys. Even more innovative is the release of apps that pay for personal data. The impressive fact is that consumers accept and use these websites and apps to make money out of their data.

Paid surveys are a revolutionary market that has not been properly addressed. It is becoming a trend to respond to surveys in exchange for reward cards, and consumers make a profit from their data. The British newspaper *The Telegraph* printed an article where it disclosed the ten most profitable survey sites. The pay depends on the time invested, the terms and the effort involved.[51] Two of those survey sites are examined below.

The first one is MySurvey. Here, the user earns points by completing online surveys via PC, Laptop, Tablet or Mobile Phone. The points are exchanged for a variety of products, gift cards, e-certificates and vouchers. The rewards include PayPal and Amazon vouchers. A typical survey might reward a user with around 100 points. They can get a £3 PayPal payment for 345 points, or a £5 Argos voucher for 550 points. The average time needed to complete a survey is between 15 to 20 minutes.[52]

---

[51] *Cf.* Sophie Christie, *Five-Minute Guide to Making Easy Money with Online Surveys*, The Telegraph (Online), Jul. 3, 2018, *https://www.telegraph.co.uk/money/consumer-affairs/five-minute-guide-making-easy-money-online-surveys/*.

[52] *Cf.* My Survey UK, *How Do Paid Surveys Work?*, MySurvey UK (2018), *https://uk.mysurvey.com.*

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

The second one is Crowdology which "offers paid online surveys that fit in with your day".[53] The surveys can be completed in between 2 and 15 minutes. Responses are anonymous and are used by brands and companies to improve their products and services. The user will earn cash paid into a PayPal account. The price is around 40p to £10 per survey. One can argue that Crowdology is buying personal data in a commercial context. In exchange for a service or good, depending on how it is to be classified as the input of personal data, the website pays users with money.[54]

Another new market is the release of apps that have as the object the collection of data. *The New York Times* published an article called "4 Free Apps that Can Earn You Extra Cash". This article states that there are a few cell phone apps designed to earn money, in the form of cards and even cash. In return, the app will track some of the user's data. Commonly, the collection of this personal data is for marketing purposes. Apps collect information about the websites visited, real-time locations, online purchases and the use of other apps as well as the user's contact list and search queries.[55]

These examples support the argument that personal data is subject to commercialisation. Privacy policies have not prevented the making of profit through the use of personal data. Consumers could be the ones using technological innovations to make a profit out of their personal data, instead of giving it away it in exchange for free services, such as Facebook or Google. Instead, this data could be traded with companies that openly and directly collect their data.

The question that remains is: Is it time to legally regulate personal data as a tradable good? The next section briefly examines the perspective of consumers with regards to disclosing their data in order for it to be traded.

C. *The Opposite Direction: Privacy*

So far this article has studied the possibility that data be considered an asset. In doing so, it is crucial to address the opinion of consumers, to see whether they are indeed open to trading their data or would instead prefer to protect their privacy. This section addresses two studies in this direction. The first one was carried out by Acxiom and it studies the population of the UK with regards to perspectives on data privacy. The second study focuses on consumer willingness to buy their personal data that is already in the cloud.

In February 2018, Acxiom published a study titled "What the consumer thinks," which looked at data privacy. It found that three-quarters of people

53 *Cf.* Crowdology, *Take Paid Surveys Online | Get Cash for Your Opinions*, Crowdology (2016), *https://crowdology.com/uk/surveys/*.

54 *Id.*

55 *See* Kristin Wong, *4 Free Apps That Can Earn You Extra Cash*, The New York Times, February 13, 2018, at B5.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

surveyed are either unconcerned or pragmatic about the data they share with organizations. The pragmatic group, which represents 50 per cent of the total of the surveyed population, seeks a clear reward or value in exchange for their data. Consumers increasingly regard their personal data as an asset and the concern about privacy has decreased.[56]

The study reveals that in 2017, the number of people in the UK who claim to be concerned about online privacy was 75 per cent while in 2012 it had been 84%. In 2017, among 18 to 24-year-old consumers it was just 58 per cent. Furthermore, 61% of 18-24-year-olds view data exchange as vital to modern society. [57] Survey respondents stated that considerations for engaging in the data economy include trust and transparency in organizations or businesses, as well as the possibility of sharing the benefits.[58] Finally, 48 percent of consumers surveyed in the UK believe they should have ultimate responsibility for their data security, while only 10 per cent believed that the government should bear the responsibility. At the same time, 41 per cent of consumers are happy for government departments to share personal information in order to enhance the efficiency of public services.[59]Acxiom's study revealed that often, consumers are open to exchanging their data, as long as they benefit from it, either monetarily or through the provision of public services. Privacy concerns are reducing, but in exchange, the consumer wants to have control of their data. They feel that it is their responsibility, not the government's.

In a separate study named 'Psychology of Ownership and Asset Defense: Why People Value Their Personal Information Beyond Privacy'[60], Spiekermann investigated what people are willing to pay to keep private their data previously left on Facebook. [61] The experiment was performed with over 1,500 Facebook participants. It offered three hypothetical scenarios:[62]

a) Mark Zuckerberg retires from Facebook. He offers users to either repurchase their information or have it destroyed.
b) A third party takes over Facebook. Participants can leave their data on the platform or repurchase their data.
c) Participants are offered a share in the revenues of the third party that took over Facebook.

---

56 *See* Foresight Factory et al., *Data Privacy: What the Consumer Really Thinks*, The Direct Marketing Association *29* (2018).

57 Factory, *supra* note 57.

58 *Id.*

59 *Id.*

60 *See* Sarah Spiekermann, Jana Korunovska & Christine Bauer, *Psychology of Ownership and Asset Defense*, in Thirty Third International Conference on Information Systems (2012).

61 Van Lieshout, *supra* note 24.

62 *Id.*

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

The results showed that the willingness to pay/protect was lowest in the first option, valued at €16; the option to pay/protect for preventing the data to be sold to a third party was valued at €54; and in the third option of sharing in the revenues, the data was valued at €507. Spiekermann thus concludes that ownership is more relevant to consumers than privacy concerns.[63]

These studies reveal that the consumers have an interest in sharing their personal data in exchange for compensation. The protection of their privacy is of minor concern. However, it seems that privacy is weighed against the benefit that the consumer receives by releasing their information. Nonetheless, the first study showed that the consumer is aware of privacy protection and they feel that it is their responsibility to protect it. This article dares to suggest that the personal data belongs to the consumer, both in terms of the benefits it can create, and in terms of privacy rights.

Cross-border flows of personal data remain an area of development. For that reason, the transfer of personal data should be regulated to set the necessary legal provision to control, enforce and establish the parameters by which such transfer is done, and through creating a legal framework for the trading of personal data.

This would help to create a trade relationship between the consumer and technology companies: rather than being a mere user, the consumer will have bargaining power. It would also protect companies against claims made by consumers, since consumers consented to the transfer and obtained a remuneration, rather than only accepting terms and conditions.

The digital trade will benefit, as cross-border data flows will be consented to and accepted by the subject of the data. Further, the trade of personal data will represent another innovation in the digital economy.

IV. Challenges of Data as a Tradable Good

Personal data is collected and purchased by the marketing industry; consumers exchange their data for free services, reward cards or for money. In other words, personal data is an asset in the digital trade. A consumer might be aware or unaware of the use given to their data, but the law should be at the forefront of its regulation.

The privacy protections of personal data are on the agenda of many governments. The key concern is the risk of misuse of personal data when transferred across borders, at the same time there is a concern about over protection, which could harm trade. There is a general acceptance that at the end it is the consumer or data subject that bears the right to consent the use of his or her own data.

63 Van Lieshout, *supra* note 24.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

International treaties should thus focus on creating a legal framework that regulates the consent, control, and transaction of the personal data. This framework would incentivise digital trade by not restricting the personal data flows and will legalize and protect the new market.

The answer to the social issues noted in the previous section should be a legal framework that recognizes and regulates the sale of personal data *as a good*. This section analyses the legal structure necessary to recognize personal data as an asset and finalizes with a proposal on how this could be achieved.

1. *Protection of Personal Data*

The response of governments to the evolution of digital trade was to protect personal data with privacy policies. If personal data were to be considered a tradable good, the trade regulations would have to cope with the privacy framework. This section briefly addresses the importance of privacy policies to personal data.

The regulatory phenomenon has its origin in the potential infringement of "internal" or "external" peace.[64] According to Polcak and Svantesson, two sorts of risks, direct and indirect, are associated with the presence of information footprints. The infringement of individual sovereignty, internal peace and the right to be let alone constitutes a direct risk. Indirect infringement means individual data has untraceable effects of group manipulation or social engineering. This data is used to control the environment, with no significant or provable individual effects. It is difficult to protect this data, because it is impossible to find any aspect of being let alone in the processing of personal data.[65]

The international community has issued legislation on this matter. This section will briefly study the privacy framework of the OECD and the Asia-Pacific Economic Cooperation (APEC), as well as the position of the free trade agreement Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the General Agreement on Trade in Services (GATS) related to the privacy protection of the personal data.

The EU recently issued the General Data Protection Regulation in 2018, which is a leading legal mechanism in the matter. However, this article will not make further reference to it. The scope of application is the EU, and though it does have effects on countries outside the EU, privacy protection is a complementary matter to this article.

---

64 *See* Radim Polcak & Dan JB Svantesson, *Private Information Sovereignty*, in Private information sovereignty: Data Privacy, Sovereign Powers and the Rule of Law 81 (Radim Polcak and Dan JB Svantesson eds, 2017).

65 Polcak & Svantesson, *supra* note 64.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

A. *The OECD Privacy Guidelines*

The organization for Economic Co-operation and Development adapted the OECD Privacy Guidelines in 2013 to meet the demands of the new digital trade era. These guidelines include principles that are of paramount importance in the protection of the privacy of the data subject. The Privacy Guidelines suggest that governments should not over-restrict the cross-border data flows.

The OECD promotes respect for privacy as a fundamental value and a condition for the free flow of personal data across borders.[66] Their concern is that a growing number of online entities collect vast amounts of personal data. To harmonize privacy regulation among its members, the Privacy Guidelines develop basic principles for national application. A summary of the principles included in the OECD Privacy Guidelines is further developed.

The collection of personal data has limits and should be obtained by lawful means with the knowledge or consent of the data subject. [67] The purpose should be specified and the subsequent use limited to the fulfilment of those purposes or not incompatible them. [68] As a limitation, personal data should not be disclosed, made available or otherwise used for purposes other than those specified except with the consent of the data subject or by the authority of law. [69] Finally, "personal data should be protected by security safeguards against the risks of loss or unauthorised access, destruction, use, modification or disclosure of data". [70]

The OECD Privacy Guidelines address the relationship between individuals and the data controller. The individuals have the right to obtain from a data controller "confirmation of whether or not the data controller has data relating to them and communication of the data related to them". [71] In the case of denial, the individual has the right to challenge such denial and if they are successful, to have the data erased, rectified, completed or amended. [72]

Finally, "the data controller should be accountable for complying with measures that give effect to the previous principles". [73] They are also accountable for personal data under their control, without regard to the location of the data, hence cross-border data.

The OECD Privacy Guidelines provide that member countries should not enact laws that unnecessarily create obstacles to cross-border flows of per-

66 *OECD Privacy Guidelines (2013)*.

67 *Id*, art. 7.

68 *OECD Privacy Guidelines (2013)*, art. 9.

69 *Id*, art. 10.

70 *Id*, art. 11.

71 *Id*, art. 13 § a.

72 *Id*, art. 13.

73 *Id*, art. 14.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

sonal data.[74] The Council recognizes that 'Member countries have a common interest in promoting and protecting the fundamental values of privacy, individual liberties and the global free flow of information'.[75] A nationally coordinated strategy is needed to achieve the right balance between the social and economic benefits of data and analytics.[76]

B. *The APEC Privacy Framework*

The APEC Privacy Framework was created in 2015 to promote electronic commerce throughout the Asia-Pacific region. It is consistent with the 2013 OECD Privacy Guidelines.[77] This framework includes principles to protect personal data. However, it gives more freedom for the transfer of data than the OECD Guidelines.

APEC Members consider that "the information flows are vital to conducting business in a global economy. They realise the enormous potential of electronic commerce to expand business opportunities, reduce costs, increase efficiency, improve the quality of life, and facilitate the greater participation of small business in global commerce." [78] Thus, a framework that enables local data transfers will benefit consumers, businesses, and governments. The APEC Privacy Framework "promotes that Members should avoid the creation of unnecessary barriers to information flows".[79]

The Framework includes principles for privacy protection. Due to the similarities with the OECD Guidelines, it is not necessary to repeat all of them; however, it is essential to enhance the fact that the APEC gives freedom to the individual concerning their personal information.[80] Two articles are of relevance, Article 9 and 19, which are developed below.

APEC Principle 9 is essential. It says that "accountability should follow the data."[81] According to Crompton and Ford, "this principle is the most important difference between the APEC Framework and the EU Directive on border controls".[82] In the Framework, once an organization has collected personal information, it remains accountable for the data "whether domestically or internationally".[83] This principle is important because it relies upon

---

74 Australian Law Reform Commission, *supra* note 16.

75 *OECD Privacy Guidelines (2013)*.

76 *Id.*

77 *APEC Privacy Framework (2015)*.

78 *Id.*

79 *Id.*

80 *Id.*

81 *Malcolm Crompton and Peter Ford, Implementing the APEC Privacy Framework: A New Approach*, International Association of Privacy Professionals, December 01, 2005.

82 *Id.*

83 *APEC Privacy Framework (2015), principle 9.*

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

the protection in the data itself and the parties to it, the person itself and the collector. The Framework does not create a cross-border barrier to the transfer of personal data.

Within Principle 3, the Framework requires that "the collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned." [84] The exception to this rule is found in Principle 4 which allows the collection of personal data through "the consent of the individual whose personal information is collected, when necessary to provide a service or product requested by the individual; or, required by law". [85] Furthermore, Principle 5 states that individuals have the right to "exercise choice about the collection, use and disclosure of their personal information… However, it may not be the case in publicly available information".[86]

The APEC Privacy Framework encourages cross-border cooperation between members. These may include mechanisms to assist in investigations and identify and prioritise cases for cooperation in severe cases of privacy infringement.[87]

There have been some arguments against this Framework, calling it too weak in the protection of privacy. For instance, Professor Graham Greenleaf argues that it has a bias toward the free flow of personal information. [88] The requirement of accountability, coupled with a requirement either of consent or that the disclosed takes reasonable steps to protect the information is said to be very soft compared to the EU Directive.[89]

On the other hand, the APEC Privacy Framework responds to the social factor behind personal data. That fact is required to protect the individual once they have traded with their data because it gives protection to the data subject but allows the data flow.

C. *The CPTPP*

The CPTPP is a free trade agreement involving 11 countries in the Pacific region, including Australia, Mexico, and Canada. It is an example of how free trade agreements protect personal data but at the same time require their members to allow cross-border data flows in order to promote trade. Accord-

84 *Id, principle 3.*

85 *Id, principle 4.*

86 *Id, principle 5.*

87 *Id.*

88 Australian Law Reform Commission, *supra* note 16.

89 *Id.*

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

ing to Deborah Elms of the Asian Trade Centre, the CPTPP it the "most important trade agreement we've had in two decades."[90]

The CPTPP includes a chapter related to electronic commerce in which in Article 14.8 of the TPP protects personal information. Within it, "the Parties recognize the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce."[91]

Article 14 requires each party to maintain a legal framework that protects the personal information of the users of electronic commerce. They should take into account principles and guidelines related to privacy protection. It also requires "each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks."[92]

The other relevant article is the 14.11 for the cross-border transfer of information by electronic means. Even though each Party may have its regulatory requirements, they "shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person".[93]

D. *The GATS*

The General Agreement on Trade in Services includes a safeguard for individual privacy. The GATS is a leading mechanism for digital transactions. It contains the World Trade Organization (WTO) rules that affect data flows.[94] Hence it is essential to make a brief reference to its provisions regarding privacy protection.

Within the General Exceptions, in Article XIV, the Governments have to take measures for the protection of the privacy of individuals about the processing and dissemination of personal data. Privacy, morals, public order, health, and the prevention of fraud, which are among the reasons to control data flows, are referenced in the provisions as policy objectives.[95]

---

90 *See* A. F., *What on Earth Is the CPTPP? - The Economist Explains*, The Economist, May 12, 2018.

91 Foreign Affairs Trade and Development Canada, *Chapter 14–Electronic Commerce*, in Consolidated TPP Text (Government of Canada, 2016).

92 *Id.*

93 *Id.*

94 *See* Aditya Mattoo and Joshua P Meltzer, 'International Data Flows and Privacy' (2018) Policy Research Working Paper (8431) *World Bank* 30.

95 Tuthill, *supra* note 17.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

The principle of data flow or, at least its fundamental trade objective, can be found in the GATS. According to Tuthill, the movement of capital can be compared to data flows. If that is the case, the GATS are recognizing that data is an essential part of the service itself. The cross-border movement of capital is found in a footnote to Article XVI on market access. [96] It states: "If a Member undertakes a market-access commitment concerning the supply of a service through the mode of supply referred to in subparagraph 2(a) of Article I[97]And *if the cross-border movement of capital is an essential part of the service itself, that Member is thereby committed to allowing such movement of capital.* If a Member undertakes a market-access commitment in relation to the supply of a service through the mode of supply referred to in subparagraph 2(c) of Article I[98], it is thereby committed to allowing related transfers of capital into its territory"[99] [emphasis added].

Accordingly, Members allow cross-border data flows. However, one remains with the uncertainty of why can the data be recognized as the capital which is the essential part of the service and yet cannot be recognized as the service itself. Meaning that data might as well be recognized as the service subject to trade.

Businesses that visit the WTO have suggested that in some countries there is a lack of transparency regarding the data flow regulations, this can become a serious challenge to doing day-to-day business and trading around the world.[100]

International treaties should focus on creating a legal framework that regulates the trade of personal data. The international community should incentivise digital trade by not restricting the personal data flows but rather should create a legal framework that legalises and protects the market.

Privacy frameworks will remain available to the individual, as protection that can be exercised at all times. The difference will be that the right to keep the information private will be upon the individual. The principle of *volenti non fit injuria* applies in this case. The law limits the protection to the extent that corresponds to the will of those who are entitled to it. In the matter of personal data, consent makes lawful conduct that otherwise would be a violation.[101]

---

96 *Id.*

97 Section 2 (a) of Article I: '(a) from the territory of one Member into the territory of any other Member;'

98 Section 2 (c) of Article I 'c) by a service supplier of one Member, through commercial presence in the territory of any other Member;'

99 GATS 1994: General Agreement on Trade in Services 1994, signed Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 UNTS 183 (1994).

100 Tuthill, *supra* note 17.

101 Polcak & Svantesson, *supra* note 64.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

2. *Trade Aspects*

This study argues that personal data will eventually be recognized as an asset subject to trade. To achieve this, a whole new series of regulations have to be created. An international framework is needed in order to allow cross-border data flows and trade regulations must be harmonized within different jurisdictions. Due to the fact that the Internet erases the physical borders, it is of paramount importance to create global recognition of the trade of personal data.

In order to trade in personal data, the ownership of personal data should be allocated. The data subject has the right to make a profit from their data, thus, they should be the ones bearing the right of ownership. Once the allocation of ownership is done, a legal framework should be created that specifies the characteristics of the sale of personal data. However, some may argue against such practice which leads this article to make reference to such counterarguments. This section addresses the regulation of ownership, its counterarguments and makes a proposal regarding the trade of personal data.

A. *Ownership*

The question ownership of personal data is still to be resolved. It is essential to recognize ownership if personal data is to be legally considered subject to trade. For instance, as a first step in the data strategy of the European Union, in 2015, Commissioner Günther Oettinger announced: "We need a virtual and digital law of property that includes data." [102] He stated that the creation of a legal basis clarifying who owns data is needed. [103]

Janeček, the postdoctoral researcher at the Oxford Internet Institute, proposed that four elements have to exist to recognize the ownership of personal data: control, protection, valuation and allocation. Those four elements are essential. This article uses these four elements to develop further the characteristics of the ownership of personal data.

First, control is necessary because through it the owner can fully use personal data by accessing, storing, sharing, selling, or processing it. It also allows the owner to destroy or abandon the data.[104] As an example, the General Data Protection Regulation framework is based on control and certainty. Recital 7 states that "Natural persons should have control of their own personal

[102] *See* Andreas Wiebe, *Protection of Non-Personal Data: A New Legal Framework for Data Ownership?*, in Value of Information: Intellectual Property, Privacy and Big Data 9–27 (Maciej Barczewski ed., 2018).

[103] *Id.*

[104] Janeček, *supra* note 4.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

data".[105] According to Andreas Wiebe, this regulation tries to put the data subject in control of their personal data through ownership. He rationalises this as follows: "if my data belongs to me, then I should have control over it and decide who should have access to it and what is done with it."[106]

Second, protection excludes third parties from controlling personal data and makes available a legal remedy for infringement of data. The protection is for the ownership right as an object, not for the personal information. The privacy regulation would protect the latter.

The protection of the ownership of personal data could be achieved through control and access to information. New technologies might make this possible, for instance, one project proposed a platform that protects personal data through blockchain. It relied on a blockchain that recognizes the users as the owners of their data, codifying services as guests with delegated permissions. Each user has complete transparency over what data is being collected and how it is accessed, and at any time they may alter the set of permissions and revoke access to previously collected data.[107]

A new company named Wibson, launched in 2018, offers a blockchain-based decentralized marketplace for consumers. It allows consumers to make a profit from selling their personal data.[108] Mat Travizano, the CEO of Wibson says "Wibson will change an opaque, buyer-dominated ecosystem into a transparent and fair market where consumers are compensated for their data based on their personal preferences and comfort level." [109] He affirms that "Individuals own their data," and he remarks "Now, Wibson allows them to profit from it as well."[110]

The company assumes the subject of the data as the owner of personal data and aims to change the marketplace of personal data. This is a practical example of how fast the market is evolving. Wibson did not wait until the law allocated the ownership of personal data to the consumer to allow trade of personal data, but went ahead and created a platform that makes it possible. The company targets fairness, transparency and control over personal data through their product.

Third, the valuation is a key element. As noted earlier, personal data is being used by tech companies to make a profit. It is generally assumed that data embody tremendous and increasing value. Personal data has intrinsic

---

105 European Parliament and Council, *Recital 7 of General Data Protection Regulation*, (EU) 2016/679, (May 25, 2018).

106 Wiebe, *supra* note 102.

107 *See* Guy Zyskind, Oz Nathan and Alex 'Sandy' Pentland, *Decentralizing Privacy: Using Blockchain to Protect Personal Data*, presented at 2015 IEEE Security and Privacy Workshops 180–184, (San Jose, CA, USA, May 21-22, 2015).

108 *See* Joe Wallen, *As Of Today, European Consumers Can Profit From Selling Their Own Personal Data*, FORBES, October 11, 2018.

109 Wibson, *It's Your Data. Get Paid For it., Wibson*, (2019), *https://wibson.org/*.

110 *Id.*

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

value and value depending on the context of its use. The value will have to be assessed, either through the platform that enables the control of personal data or by the traditional movement of the market, i.e. supply and demand.

Fourth and finally, the allocation should be given to the data subject. Some may argue that the controller or the processor are the ones entitled to this allocation. However, throughout this article the argument has been that the consumer/user are the ones not who are not benefitting from their data. The way for them to do so is by recognizing their ownership over their data. After recognising that the user owns their personal data, then they can trade with it and transfer it to a third party.

As proof of the characteristics required for ownership of personal data, there are proposals to establish new property rights in data based on intellectual property rights. These proposals include the specific design of a data right which is further developed in the next paragraph.[111]

First *protection* should be conditioned on the "coding" of data. Then, the subject matter would be limited by a requirement of added value or novelty. Added value requires a substantive *valuation* and novelty draws the question of whether data have been created or stored before, in other words, asking whether it is new data or not. The next issue is that of who data rights should be *allocated* to. In a digital environment, there are many stakeholders who could complicate the allocation. Further limitations, natural to intellectual property rights, are stipulated as to the scope of a data right. As an example, the copying of already existing data, a limit in duration and prolongation in the trademark.[112]

This proposal in the area of intellectual property reinforces the argument that a legal framework that includes such characteristics will determine the property of personal data. If ownership could be regulated, then the exchange of personal data would have a solid foundation for trade. Either as a good, as proposed in this article, or as a licensing right subject to an intellectual property framework, as the example above mentioned. In any case, ownership is made possible through compliance with these characteristics.

A legal framework that addresses elements of consent, protection, valuation and allocation would conclusively determine the ownership of personal data. As a consequence, it would contribute to creating a strong legal foundation to enable the trade of personal data.

B. *Counter Position*

This article argues that personal data should be considered a property right to legally enable its trade. However, there are opinions against the al-

111 Wiebe, *supra* note 102.

112 Wiebe, *supra* note 102.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

location of ownership and trade of personal data. To create a more objective argument, it is important to make reference to four strong counter arguments.

First, some authors argue that ownership of personal data represents two main problems: the concept by itself and the fact that the data subject can ever have full control over it. It is complicated to conceptualize ownership of a piece of personal data to a single, specific individual. Sometimes the same piece of data belongs to more than one subject. For example, someone's date of birth is the day the mothers gave birth to them. Some argue this is a reason why a data economy will not work. A data economy, where the individual has ownership over their data, would involve individuals storing the data in a kind of data bank account where they can control, manage and exchange it. In the previous example, would it mean that the child can store half of the data related to the day of birth and the mother the other half? For individuals to have full control over their data companies would be required to be completely transparent and comprehensible about the ways someone's data will be used.[113] Some authors state that in virtualized infrastructures, physical control over data is almost impossible.[114]

Second, the regulation of trade also implies difficult scenarios, including the allocation of value. Data is not like money because its value depends on its context and how it is used. It also depends on the way it is stored, if it is as metadata then it has value through the compilation and not by itself. The allocation of the value also brings up the problem that not only the individual contributed to the value of the data but different agents do as well. All of them could be said to have some interest in data. The problem becomes bigger in analytics and big data where the value of the data is not by itself but through the group of data being analysed and modified.[115]

Third, another strong position is the one that questions the fact that through informed consent the data subject will have appropriate control over their data. The Internet has proven that consumers do not necessarily read through pages and pages of complex privacy policies and terms and conditions.[116] In order to comply with laws, companies draft their policies with information that cannot be absorbed by ordinary individuals. So how can the data subject make an informed decision if the information provided is completely biased?[117] The concern that arises is that consent will face the same problem in allowing the trade of personal data.

---

113 Wiebe, *supra* note 102.

114 *See* Qumodo Ltd, *Personal data: ownership, consent, and appropriate control*, Medium, December 11, 2018.

115 Wiebe, *supra* note 102.

116 *See* Alan Chiu & Geofrey Masters, *Practical aspects of licensing in the cloud*, in Privacy and Legal Issues in Cloud Computing 261-290 (Anne S Y Cheung ed, 2015).

117 Qumodo, *supra* note 114.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

Fourth, technology companies can be diminished by a change in the marketplace of personal data. Currently, they gather data at no extra cost and free will, only complying with privacy protection. However, if the basis for the transmission of personal data is consent, the data subjects will have too much control over it.[118] The data subject will be able to withhold its data at their discretion. Too much protection might be counterproductive to the market. Others argue that it might even impede innovation, which would be best served by an unlimited flow of data within a policy of open data and open innovation.[119]

This section enumerates strong arguments and concerns against the ownership or trade of personal data. However, this article has shown that the trade of personal data is already a reality, whether it is legally acceptable or not. Thus, these counter arguments could be taken into consideration when drafting a legal framework to enable the trade of personal data. For example, when drafting a legal framework for personal data as an asset, to state ownership, it might be the case that joint ownership applies. The framework should specify the rules for the allocation of value. Whether the consumers are initial right holders, as this article argues, or entrepreneurs or commercial entities, which hold rights as well. And in the case of consent, it could include alternative mechanisms to secure that consent is sought in a way that is both transparent and explicit.

The previous section mentioned that new technologies already exist for the control over personal data, so it is safe to say that control would not be a problem in case of trade of personal data. A legally recognized trade could result in a change of the rules of the market, but this article argues that neither innovation nor the companies will be negatively affected. On the contrary, the exchange of personal data will be led mainly by supply and demand and less restricted by governmental intervention. If companies have to pay for data, they would carefully consider the quantity and quality of data worth collecting and paying for. This would create more efficiency in the interest of all stakeholders.[120]

Even though there are strong arguments and possible constraints to the trade of personal data, this article sustains that its data is an asset in today's economy that is already being used and exchange an object of trade. A legal framework that sets the rules will contribute to fair and transparent practice. The next section specifies the proposal of this article.

C. *Trade of Personal Data*

Data flows are increasingly cross-border; therefore, their sale should be regulated by an international organization. In the first section of this article,

118 *Id.*

119 Wiebe, *supra* note 102.

120 *Id.*

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

it was noted that APEC is an international organization that more freely regulates the cross-border exchange of data, it could also be the body that innovates in the creation of a legal framework for the trade of personal data.

This article proposed that a legal framework for the trade of personal data could be done by APEC, as it is the least restrictive regarding cross border data flows. APEC is used here as an example to create a realistic scenario of how a personal data-trade framework could be issued as a privacy framework. The regulation could also be done as a chapter in a free-trade agreement or convention. For example, the CPTPP already contains a provision for the cross border flow of personal data within their e-commerce chapter. Sooner or later the trade of personal data will be included in legal regulation. This investigation does not dig further which international body is the most likely to do so, rather emphasizing the importance of doing so.

Now, using as an example trade of personal data regulation through an agreement in the APEC, the United Nations Convention on Contracts for the International Sale of Goods could prove to be useful to draft the content of the framework. The United Nations Convention on Contracts for the International Sale of Goods sets out international principles that could be used to govern the formation of contracts for personal data. This Convention strictly applies for sales of goods and personal data is neither considered a good or service so legally it does not apply. Nonetheless, the United Nations Convention on Contracts for the International Sale of Goods is used as an example to demonstrate which elements would be necessary to include in a contract were data to be legally considered a good.

First of all, an offer on personal data should be made which has to be accepted for the contract to exist. Counter-offers could apply. Like any other sale, the price has to be fixed and the good has to be delivered. Finally, the contract would have provisions in case of breach of contract.[121] Consent by the right holder is a crucial element for international treaties to allow the cross-border data flows. Thus, if the data subject made the offer it could be considered as consent to fulfil the regulatory requirements. In general, once consent is given, personal data could be transferred.

The transfer of property might represent a challenge because personal data is a tangible good and can be replicated an infinite amount of times. Personal data could be transferred through a licence, just as software is, this would require particular technology, for example, a blockchain code. The fact that personal data is transferred as the subject of IP rights should be further developed in another research paper. For the moment it is relevant to mention that personal data could be transferred with the protection of blockchain in exchange for a price.

[121] United Nations Convention on Contracts for the International Sale of Goods, opened for signature Apr. 11, 1980, 5 UNTS 1489 (1988).

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

This provisions translated to the personal data will read as follows: The user of a Website that allows the use of his or her data, for example in data analytics or any use other than the one required to access the Website by itself, will offer his or her data in exchange for a price. Otherwise, the personal data introduced in the Website will only be used to navigate within the Website. Another case could be one of the surveys and direct sale of personal data, where the user and the Website directly make a contract of sale, and any other purpose than the transfer of personal data would come at a price.

In both cases, personal data has to be controlled. It could be licensed for a determined period or accessed several times via a license. New technological developments could ensure control. One of the reasons for considering the sale of personal data as such is so that the data subject is adequately compensated for the exchange of their data. Through a contract of sale, this compensation is monetized in the price.

Besides the traditional characteristics of a sale, the legal framework could include the aspects discussed in the *Counter Position* section of this article. It would be important to state how ownership and value will be allocated and what the requirements for transparent and explicit consent by the data subject will be.

To sum up, the legal framework that establishes the structure of trade of personal data has to be created by an international organization that influences the market in different countries, such as APEC. It needs to have a contractual legal base, for example, the provisions set in the United Nations Convention on Contracts for the International Sale of Goods. Finally, it should address the specific requirements and possible conflicts given the nature of a transaction of personal data in a virtual environment, as in the Internet.

In conclusion, the trade of personal data will not go against current privacy regulation. As long as the subject gives their consent, trade is possible. However, a legal framework that effectively sets the legal structure for the trade of personal data is required. Given the increase in cross-border data flows, it is of the interest of the international community to do so.

Trade in personal data is a reality that can no longer be avoided. Even if there are constraints for the regulation of personal data, it is necessary to legally recognize its ownership and trade to contribute to the control and protection of it. A legal framework could enhance certainty and transparency as to the beneficiaries of data.

V. Conclusion

The notion of trading with personal data might seem a bit unconventional due to the risk it may generate to the privacy of individuals. However, commerce is a human activity that, in some instances, does not respond to morality but the demands of the market. This article has shown how companies

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.2.14173

already make a profit out of the use, collection and processing of personal data. This social factor exists, even if the legal community argues that it goes against privacy protection. Personal data can be used as an asset in the digital economy.

This article argues that the consumer, thus the data subject, should share the profits their own personal data is producing. Some people have found ways to reach that goal, either through surveys, apps or even through experiments. The legal recognition of trade of personal data is necessary, that recognition should be done by an international body in response to the cross-border data flows that enable the exchange of information around the world. The trade of personal data is an international matter.

This proposal might seem negative for the corporations that currently are making a profit out of personal data. However, it could turn out to be in their favour, given the fact that free trade will be promoted and the collection of data will be more efficient and transparent. The consumer who consents to such practices and has the necessary protection is unlikely to claim misuse of their personal information. In that sense, corporations could avoid huge scandals that end up costing them millions of dollars. Creating a legal framework of this practice legitimises the already existing trade in personal data.

The legal recognition of the trade of personal data will create an environment in which the consumer receives compensation from the data they introduce on the Internet, the tech companies will use personal data with the express and affirmed consent of the data subject, and the digital trade will continue to develop in a legitimized but less restrictive manner. Furthermore, allowing trade in personal data will trigger the development of proper technologies to control the access and management of personal data. Hence, consumers will protect their own privacy.

Some may argue that legally the trade of personal data is not possible due to the constraints that the allocation of ownership generates. However, this article proposed different perspectives that can be incorporated into a framework that would address specifically how personal data is an asset. Besides the privacy framework, there is no previous material for regulating the current cross-border data flows that generate millions of dollars to technology companies. While lawyers debate the legal basis for personal data, consumers are giving away their data for free.

If the international community is against allowing the trade of personal data, the question would be: How will they control the use of extrinsically personal data? Digital trade is growing, and the law has to evolve accordingly. In the near future, governments will include in their agenda the need to regulate the profits made out of personal data. This article suggests that organizations like APEC should innovate and start incorporating in their agendas the drafting of trade frameworks for personal data. It is important to accept and deal with social forms that might seem to go against government policies but are more incorporated into society than the existing policy.

Received: April 2nd, 2019.
Accepted: June 7th, 2019.