The Economics of Privacy

Chizzy Meka

May 11, 2021

Contents

1 ABSTRACT

The exponential growth in modern technology is continuously widening our digital realm. These technical developments create the need to ensure that our digital rights and privacy are duly protected. As a result, matters relating to our privacy are ever becoming more complex and sophisticated when viewed through different lenses. This article firstly considers how privacy has evolved with time and investigates what the privacy concept means in this digital era. After that, the paper delves into the economics of privacy. It explores the complex interactions between three actors: individuals, organisations, and governments in environments driven by personal data. As part of this examination, we briefly consider the costs, benefits, and trade-offs involved in protecting and disseminating confidential data for all three actors mentioned above. Finally, we then review the personal privacy-concerned legislation, GDPR, and briefly highlight two areas of the regulation that legislators can improve.

2 SEMANTIC EVOLUTION OF 'PRIVACY'

Our world is constantly evolving, and so is the word 'Privacy'. (Browne 1976) considered privacy a legal and social concept and defined it as an individual's right to control, store and disseminate information about themselves.

(Posner 1981) stated that people used the word 'privacy' in three different contexts. Firstly, to refer to the concealment of information. Secondly, to refer to peace and quiet and, thirdly, as a synonym for personal freedom and autonomy. He affirmed that the first meaning was the most prevalent.

(Kovacic 1994) considered privacy in a commercial context. His article on regulated utilities states that regulated utility managers often find themselves in a difficult situation. The author described a dilemma whereby managers need to gather customer data to improve customer service by understanding their clients. However, at the same time, regulated utility managers are always treading carefully to avoid breaching any privacy laws that protect the customers and employees. While this paper does not explicitly define privacy, it implicitly acknowledged it as a legally protected individual right.

(Rust et al. 2002) defined privacy as the degree to which others do not know information about a person.

(Acquisti et al. 2016) acknowledged that privacy is difficult to define because it means different things to different people. And (Posner 1981) above also shares this sentiment. They, (Acquisti et al. 2016), presented three different definitions from previous works. The first definition is from 1890. It defined privacy as the protection of an individual's personal space and entitlement to be left alone. The second 1967 definition described the concept as the control over and safeguarding of personal information. The third definition incorporates dignity, autonomy, and freedom as additional elements that individuals should control.

(Kim et al. 2020) asserted that privacy could not be conclusively defined. Like (Acquisti et al. 2016) above, (Kim et al. 2020), acknowledged that the privacy concept is hard to conceptualise. However, while (Acquisti et al. 2016) believed that this difficulty was because privacy means different things to different people, (Kim et al. 2020) believes that the problem is that privacy is constantly evolving. Nevertheless, amalgamating these two ideas highlights that people's perceptions of the word 'privacy' primarily drive the concept behind the word. In turn, our continually changing world in terms of social views, technological advancements, and legislation changes drives people's perception of privacy.

The paragraphs above show that the meaning of the word 'privacy' has evolved over the last five decades. Even though the descriptions come from different standpoints, i.e., social, legal, and technical, the underlying theme is that privacy is an entitlement and a right of every individual. We note that, unsurprisingly, earlier scholars primarily defined privacy within the legal and social context. But as of the 2000s, the description started placing more emphasis on digital privacy. Given the explosion in internet technologies, the word 'privacy' now almost exclusively refers to privacy within the internet or e-services context.

3 THE ECONOMICS OF PRIVACY

3.1 Individuals

The issue of digital privacy, or lack thereof, is continually gaining traction. This popularity is because our data is constantly merchandised behind the scenes by tech giants supposedly offering us 'free' services (Scholz 2012). For instance, (Stutzman et al. 2013) observed that between 2005 to 2011, Facebook users expressed willingness to keep their data on the platform more confidential. However, over the same period, the social media giant made USD 100 billion from selling people's data to advertisers (Scholz 2012).

As individuals, sharing our private data comes at a cost. Whether we realise it or not, in many cases, we subconsciously weigh up the costs and benefits before committing to sharing our data. For instance, on social media, we share our data to connect with friends and family. We share our location information to use GPS services from mobile apps like Google Maps and Waze. According to (Mungan 2017), people will only consider selling their data if a buyer offers them a price higher than the inconvenience they would experience if a third party disseminated that data. The author dubbed this phenomenon 'privacy cost'. In contrast, a buyer would only consider paying the price higher than the privacy cost if the social value of the information they intend to buy is greater than the privacy cost. Thus, the author concluded that this reasoning makes these privacy-related transactions wealth-enhancing for both the seller and the buyer. But does it? The answer to this question lies in weighing the trade-offs that come with disclosing one's data, a concept (Acquisti 2014) referred to as 'privacy trade-offs'.

Individuals do not generally gain fiscal benefits by releasing their information. They can, however, benefit from services such as personalised customer service when they give up their data. Access to people's data can help companies study their customers' behaviours and gauge reactions to new products and services (Acquisti & Varian 2005). In the long run, this opportunity can help better consumer satisfaction, benefiting individuals. And secondarily foster client relationship, benefiting companies.

Regarding the costs of sharing our data, as (Doyle 2013) said, individuals continually disseminate innocuous bits of their personal information through various channels in these modern times. Some of these channels include social media, mobile app trackers, credit cards and others. These bits of information about us become somewhat 'immortal'. And the high cost to individuals is that a third party can aggregate and analyse them to build an accessible, self-contained, and shareable complete profile. These profiles can provide insights that include, but not limited to, demographic, socio-geographical, behavioural, or mental attributes. Such information can help data analysts learn intimate details about a person's life. Some of these details can include their shopping preferences, daily schedules, and other habits (Małagocka 2018).

(Acquisti 2014) asserts that costs that emanate from privacy infringements or unauthorised data dissemination can take both tangible or intangible forms.

And can affect both data holders (companies in this case) and data subjects (individuals in this case). (Calo 2011) added that these costs could be subjective or objective. He stated that subjective privacy harms come from unwanted perceptions of observation, thus related to the anticipation of losing control over private data. Some examples include anxiety, fear, and embarrassment; the discomfort from feeling surveilled; the shame associated with personal data exposure or uneasiness from expecting an intrusion into one's private life. This class of harms are difficult to quantify and, thus, is not usually legally recognised as 'actual damage' for that reason.

In contrast, objective privacy harms comprise the unexpected or coerced use of data about someone against the individual. Thus, objective privacy harms relate to the ramifications of losing control over private data. For instance, identity theft, the time and efforts invested in removing junk mail; the time invested in warding off telemarketers; the additional monetary amount one pays because of price discrimination.

3.2 Companies

(Małagocka 2018) stated that data had become an essential ingredient for competitive advantage in business and commerce. In this digital age, characterised by an unquenchable appetite for data, information is now considered a resource that can make or break an organisation. Data is now the fourth production factor alongside land, capital, and labour (Pomykalski 2001). And as (Castells 2007) put it, information is a type of fuel resource that is processed using technologies. (Muraszkiewicz 2002) described this type of data as knowledge-constituting information. As stated earlier, data enable companies to optimise marketing resources, acquire and retain customers, develop pricing strategies that cater to different customer segments on a personalised level. This incentive is the single most motivating driving force for companies and their relationship with private data - be it theirs or someone else's data. This factor has helped position data as a new form of currency in the digital sphere. As an analogy, (Małagocka 2018) compared data to oil and its analytic tools to the steam engine.

Value is another benefit that data adds to a company. We can consider companies as a group of assets classified into material and non-material assets. Materials assets include money and technical means. Conversely, non-material assets comprise know-how, brand, trademarks, reputation, corporate culture, and 'dexterity' with information. These assets invariably affect an organisation's position in the market (Małagocka 2018).

Alongside profitability, market domination, robust business alliances, customer relationships, the ability to acquire and leverage data has become additional benchmarks for assessing a company's success (Małagocka 2018). In contrast, companies continually run the risk of breaching laws that protect people's privacy (Kovacic 1994). And as stated by (Romanosky & Acquisti 2009), in the event of a data breach, for example, companies can suffer the cost of holding people's data. These costs can take the form of fines, settlements, customer

notification costs, customer distrust or stock market losses. However, (Gellman 1999) deemed it rare, considering that organisations are generally adept at externalising such costs while internalising the benefits of personal data collection.

The preceding paragraphs imply that any modern company that shies away from participating in merchandising or leveraging data risks stunted business growth and non-optimal profitability. This circumstance could well mean obsolescence for such a company in this era.

3.3 Governments

Most discussions around digital privacy involve the interactions between individuals and companies. Inserting governments as a third actor significantly changes the landscape. The change is of a magnitude that sceptic writers consider governments the arch threat to any entity's privacy. Governments are viewed as the 'judge and jury' regarding privacy matters because they develop policies and legislation governing privacy. At the same time, they often take and use information by force of law. This realism means that private companies cannot obtain certain information if the data subject refuses to disclose the information. However, governments can effortlessly invade the data subject's privacy and acquire said information, armed with the law. For example, the government can mandatorily audit a company's finances (Harper 2012).

Despite the authoritarian perceptions of governmental bodies, specific dynamics in play within the private data marketplace also affect governments. And just like individuals and companies, there are also costs and benefits when governments share information. Governmental bodies can share data with public and private institutions within a country or internationally. Information Sharing refers to the process whereby two parties allow each other access to information belonging to each other. When the parties are government agencies, we refer to the practice as Government Information sharing (Mendes Calo et al. 2014). Some of the gains include efficiency – by averting the duplication of efforts by maintaining the same data; improved internal processes and services – by eliminating inconsistencies and mitigating error; and improved process transparency – by enabling access to information (Fillottrani et al. 2012). In contrast, some of the costs include loss of control over the data, loss of privacy and security, fear of data misuse, citizen distrust in governmental services, and communication interceptions through cyber-attacks and threat to national security (Mendes Calo et al. 2014).

Nevertheless, irrespective of our views on privacy and governmental bodies, governments remain the guarantors of our digital rights. They are in the position to penalise any violators of that right (Goldstein et al. 2018). Privacy-oriented laws are imperative, and legislators cannot keep up with the exponential growth in technology. So, governments must simultaneously preserve individuals' privacy and advocate transparent processes, two tasks that seem mutually exclusive. (Gutwirth & De Hert 2008).

4 LAW AND LEGISLATION

The European Union (EU) has different legislation governing privacy regulating how organisations collect and use our data. The General Data Protection Regulation (GDPR) is a well-known data protection regulation catering to digital privacy that became effective on the 25th of May 2018. The first objective is to make privacy laws homogeneous across the EU. The second objective is protecting EU citizens from data breaches. And the third one is to revolutionise how EU-based institutions handle data privacy (GDPR 2018*a*). GDPR has drastically changed the way individuals and companies interact. It has also influenced how organisations handle individuals' data. From the organisations' standpoint, these changes include possible penalties from non-compliance penalties to meet peoples' consent requirements when dealing with their data (Novikova 2019). GDPR is thus a significant move to give individuals control over their data (Ng 2018). On the other hand, in the United States, privacy-governing laws like these are somewhat underdeveloped (Levin & Nicholson 2005). Following UK's departure from the European Union (EU), legislators transposed EU's GDPR legislation to derive a UK specific version termed 'UK GDPR' (Porter 2020) (Piper 2019) (Palmer 2020).

But has the GDPR worked? The answer is both yes and no. Yes, because GDPR has been ground-breaking, helping protect people from abuse of their data by tech companies. Typical private data abuse is the infamous Facebook's Cambridge Analytica Scandal in 2018 (Wong 2019). Additionally, the GDPR legislation has proven to be a trailblazer that has inspired similarly designed legislation worldwide, including the California Consumer Act (CCPA) (Lucarini 2020). No, because the GDPR still has flaws that organisations cleverly exploit.

GDPR sufficiently regulates discrete personal information that could directly identify or lead to an individual's identification. These types of information include data such as a person's names, address, card details, IP address and demographic data (GDPR 2018*c*). However, it does not satisfactorily address 'derived personal data'. By 'derived personal data', we mean those kinds of information inferred from a person's digital behaviour - see (Doyle 2013) in the Individuals section. Tech giants and social media platforms leverage people's derived personal data for advertisements and targeted marketing. This element creates a significant flaw in the regulation. Thus, we recommend a modification to the legislation to address this aspect of personal information adequately.

GDPR places the data protection onus on organisations, not the customer. However, some companies operate as though the reverse is the case. This practice is problematic because it creates an exploitable loophole for personal data-obsessed companies such as social media giants. For example, Facebook rolled out a 'GDPR-complaint' privacy setting which offered users the option to 'decline' personal data collection (Kraus 2018). This set-up exploits the average user that does not read the privacy policies of different social media platforms. Thus, it perverts GDPR procedures because these platforms should strictly refrain from collecting personal data by default until a user chooses to allow it. So, there should be improvements in the legislation to address such flaws.

5 CONCLUSION

Considering the first actors, individuals, we find that different people have varying attitudes towards privacy, ranging from the indifferent to the paranoid. Regardless, most individuals readily share private information, even for minuscule benefits. We also deduced that individuals' data is centric in digital privacy matters. Both companies and governments are primarily interested in them. The interest exhibited by these two more significantly influential actors creates a dynamic that substantially undermines the little control people have over their data. Thus, we conclude that individuals have the least control over their data out of the three actors. And, if true privacy is about having control over your data, as (Stewart 2018) affirms, we assert that individuals have no true privacy.

Looking at companies, as our second actor, unsurprisingly, these entities are fiscally driven. Money serves as the main incentive behind their constant hunt for personal data. Although the GDPR seeks to curb potential private data abuse, the regulation does not necessarily impose an airtight solution that would guarantee full compliance. So, there are always loopholes that companies can leverage to erode further the apparent control people possess.

The third actor, governments, naturally possess the most control given their status as the policymakers. Most articles reference the interaction between personal data and governments within the context of surveillance. We observed that proponents cite national security interests and crime prevention as the excuse for governments' tendency to target private data. On the other hand, the opposition cited authoritarian mass surveillance as the reason for governmental intrusions on peoples' data. Whatever the reason may be, there are no incentives for either companies or governments to do more to boost individuals' control of their privacy. And the fact that law enforcement and national security matters are outside the GDPR coverage (GDPR 2018*b*) further increases our confidence in that conclusion. However, we must recognise that GDPR is a step in the right direction in levelling the privacy playing field on the 'control' front.

Moreover, the legislation still has its flaws. On that note, we assert that individuals generally only possess absolute control over their data before releasing it in the first instance. Beyond that, we do not have power over what our data recipients choose to do with our information. The legislation is proveably not robust enough to guarantee us the promised control.

References

Acquisti, A. (2014), 'The economics and behavioral economics of privacy', *Privacy, big data, and the public good: Frameworks for engagement* **1**, 76–95.

Acquisti, A., Taylor, C. & Wagman, L. (2016), The economics of privacy, *in* 'Journal of Economic Literature', Vol. 54, IEEE Comp Soc; SERSC; ETRI; KISA; ESIB; IEEE, pp. 442–492.

Acquisti, A. & Varian, H. R. (2005), 'Conditioning prices on purchase history', *Marketing Science* **24**(3), 367–381.

Browne, P. S. (1976), Computer Security: A Survey, *in* 'Proceedings of the June 7-10, 1976, National Computer Conference and Exposition', AFIPS '76, Association for Computing Machinery, New York, NY, USA, pp. 53–63.
URL: https://doi.org/10.1145/1499799.1499809

Calo, R. (2011), 'The boundaries of privacy harm', *Ind. LJ* **86**, 1131.

Castells, M. (2007), 'Communication, power and counter-power in the network society', *International journal of communication* **1**(1), 29.

Doyle, T. (2013), 'Anita Allen: Unpopular privacy: what must we hide?', *Ethics and Information Technology* **15**(1), 63–67.
URL: https://search.proquest.com/scholarly-journals/anita-allen-unpopular-privacy-what-must-we-hide/docview/1287878702/se-2?accountid=14511https://ucl-new-primo.hosted.exlibrisgroup.com/openurl/UCL/UCL_VU2?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:

Fillottrani, P. R., Calo, K. M., Cenci, K. M. & Estevez, E. C. (2012), 'Information sharing-benefits', *Journal of Computer Science and Technology* **12**(2), 49–55.

GDPR (2018*a*), 'Guide to the UK General Data Protection Regulation (UK GDPR) — ICO'.
URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

GDPR (2018*b*), 'Key definitions — ICO'.
URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/#:$\sim$:text=TheUKGDPRdoesnot,purelyforpersonal%2Fhouseholdactivities.

GDPR (2018*c*), 'What is personal data? — ICO'.
URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/

Gellman, R. (1999), 'None of your business: World data flows, electronic commerce, and the european privacy directive', *The George Washington International Law Review* **32**(1), 179.

Goldstein, K., Ohad, S., Tov, M. & Prazeres (2018), *The Right to Privacy in the Digital Age*.

Gutwirth, S. & De Hert, P. (2008), Regulating profiling in a democratic constitutional state, *in* 'Profiling the European citizen', Springer, pp. 271–302.

Harper, J. (2012), 'Why Government is the Greater Threat to Privacy'.
URL: https://www.ipi.org/ipi_issues/detail/why-government-is-the-greater-threat-to-privacy

Kim, J., Baskerville, R. L. & Ding, Y. (2020), 'Breaking the Privacy Kill Chain: Protecting Individual and Group Privacy Online', *Information Systems Frontiers* **22**(1), 171–185.
URL: https://search.proquest.com/scholarly-journals/breaking-privacy-kill-chain-protecting-individual/docview/2030542928/se-2?accountid=14511https://ucl-new-primo.hosted.exlibrisgroup.com/openurl/UCL/UCL_VU2?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mt

Kovacic, W. E. (1994), The Law and Economics of Privacy: Applications to Regulated Utilities, *in* Crew, MA, ed., 'Incentive Regulation for Public Utilities', Vol. 18 of *TOPICS IN REGULATORY ECONOMICS AND POLICY SERIES*, Rutgers State Univ, pp. 113–124.

Kraus, R. (2018), 'Facebook rolls out GDPR-compliant privacy settings worldwide'.
URL: https://mashable.com/2018/05/24/facebook-gdpr-worldwide-compliance/?europe=true#ddE6Ie1lsaqn

Levin, A. & Nicholson, M. J. (2005), 'Privacy law in the united states, the eu and canada: The allure of the middle ground', *U. Ottawa L. & Tech. J.* **2**, 357.

Lucarini, F. (2020), 'GDPR vs CCPA: What are the main differences?'.
URL: https://advisera.com/eugdpracademy/blog/2020/04/13/gdpr-vs-ccpa-what-are-the-main-differences/

Małagocka, K. (2018), 'Who is the payer? The value of private information from the perspective of customers and companies. TT - KTO JEST PŁATNIKIEM? WARTOŚĆ PRYWATNYCH INFORMACJI Z PERSPEKTYWY KLIENTÓW I FIRM', *Acta Universitatis Nicolai Copernici. Nauki Humanistyczno-Spoleczne. Zarzadzanie* **45**(1), 137–149.
URL: https://search.proquest.com/scholarly-journals/who-is-payer-value-private-information/docview/2334657681/se-2?accountid=14511https://ucl-new-primo.hosted.exlibrisgroup.com/

openurl/UCL/UCL_VU2?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&g

Mendes Calo, K., Cenci, K., Fillottrani, P. & Estevez, E. (2014), Government information sharing: a model for classifying benefits, barriers and risks, *in* 'Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance', pp. 204–212.

Mungan, M. C. (2017), 'Conditional Privacy Rights: JITE', *Journal of Institutional and Theoretical Economics* **173**(1), 114–131.
URL: https://search.proquest.com/scholarly-journals/conditional-privacy-rights/docview/1861773845/se-2?accountid=14511https://ucl-new-primo.hosted.exlibrisgroup.com/openurl/UCL/UCL_VU2?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article

Muraszkiewicz, M. (2002), Mobile society, technology, and culture, *in* 'Internet technologies, applications and societal impact', Springer, pp. 187–197.

Ng, I. (2018), 'From GDPR to blockchain, we're getting more power over our data — WIRED UK'.
URL: https://www.wired.co.uk/article/gdpr-personal-data-private-data-accounts

Novikova, O. (2019), 'The New Media Business Model: When Customer Controls the Data', *Journal of Business Models* **7**(4), 34–38.
URL: https://search.proquest.com/scholarly-journals/new-media-business-model-when-customer-controls/docview/2407765658/se-2?accountid=14511https://ucl-new-primo.hosted.exlibrisgroup.com/openurl/UCL/UCL_VU2?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:

Palmer, D. (2020), 'On data protection, the UK says it will go it alone. It probably won't. — ZDNet'.
URL: https://www.zdnet.com/article/on-data-protection-the-uk-says-it-will-go-it-alone-it-probably-wont/

Piper, D. (2019), 'UK: Understanding the full impact of Brexit on UK: EU data flows – Privacy Matters'.
URL: https://blogs.dlapiper.com/privacymatters/uk-gdpr-brexit-flowchart/

Pomykalski, A. (2001), 'Innovation management', *Warsaw: PWN* .

Porter, J. (2020), 'Google shifts authority over UK user data to the US in wake of Brexit - The Verge'.
URL: https://www.theverge.com/2020/2/20/21145180/google-uk-user-data-processing-ireland-usa-authorities-data-protection-gdpr-cloud-act

Posner, R. A. (1981), 'THE ECONOMICS OF PRIVACY', *AMERICAN ECONOMIC REVIEW* **71**(2), 405–409.
URL: https://search.proquest.com/scholarly-journals/economics-privacy/docview/61175702/se-2?accountid=14511https://ucl-new-primo.hosted.exlibrisgroup.com/openurl/UCL/UCL_VU2?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&sid=ProQ:P

Romanosky, S. & Acquisti, A. (2009), 'Privacy costs and personal data protection: Economic and legal perspectives', *Berkeley Tech. LJ* **24**, 1061.

Rust, R. T., Kannan, P. K. & Peng, N. (2002), 'The customer economics of Internet privacy', *Journal of the Academy of Marketing Science* **30**(4), 455.
URL: https://search.proquest.com/scholarly-journals/customer-economics-internet-privacy/docview/224861703/se-2?accountid=14511https://ucl-new-primo.hosted.exlibrisgroup.com/openurl/UCL/UCL_VU2?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&sid=ProQ:ProQ%3Aabiglobal&atitle=The+customer+economics+of+Internet+privacy&title=Journal+of+the+Academy+of+Marketing+Science&issn=00920703&date=2002-10-01&volume=30&issue=4&spage=455&au=Rust%2C+Roland+T%3BKannan%2C+P+K%3BPeng%2C+Na&isbn=&jtitle=Journal+of+the+Academy+of+Marketing+Science&btitle=&rft_id=info:eric/&rft_id=info:doi/

Scholz, T. (2012), *Digital labor: The internet as playground and factory*, Routledge.

Stewart, C. (2018), 'What is Digital Privacy?. And Why Privacy Matters... — by Christian Stewart — Noteworthy - The Journal Blog'.
URL: https://blog.usejournal.com/what-is-digital-privacy-search-encrypt-explains-why-privacy-matters-768ec372bf00

Stutzman, F. D., Gross, R. & Acquisti, A. (2013), 'Silent listeners: The evolution of privacy and disclosure on facebook', *Journal of privacy and confidentiality* **4**(2), 2.

Wong, J. C. (2019), 'The Cambridge Analytica scandal changed the world – but it didn't change Facebook — Facebook — The Guardian'.
URL: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook