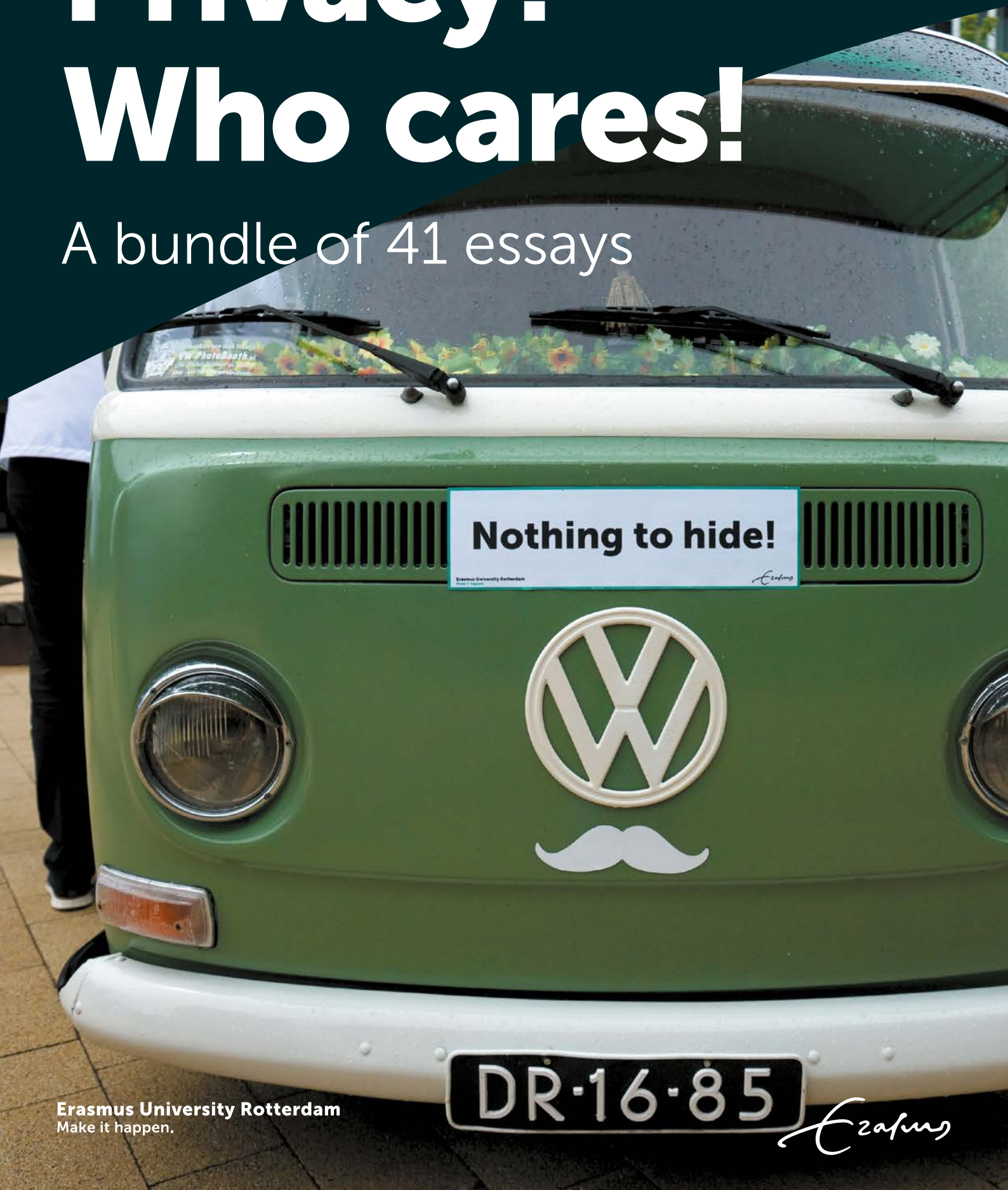
Mind your data.

Privacy? Who cares!

A bundle of 41 essays



Erasmus University Rotterdam
Make it happen.

Colophon

Publication
Erasmus University Rotterdam (EUR)

Coordination
CIO Office

Design
PanArt communicatie en mediadesign

Photography
Arie Kers

Print
DeBondt Grafimedia

Foreword

Trust. **That** is the essence of privacy. Do we trust our government with our personal data? Do we trust corporations and business partners with our personal data? But also... do we trust our university with our personal data? Our university: that's us! Can we be relied on to handle the data of our existing and prospective students, job applicants, our staff and research subjects with due responsibility?

Our university is at the heart of society. At Erasmus University, we respect the trust placed in us by the community, the private sector and the government. Both social impact and valorisation are rooted in trust. That's why we stay on our toes. We want to lead the way when it comes to offering a safe work environment for students, staff and research activities. We work to protect EUR against outside dangers and we take measures to prevent major and minor mistakes or errors.

What's our students' take on privacy? To find out, we organised an essay contest on the theme of Europe's recently-implemented General Data Protection Regulation. We challenged students to share an inspiring perspective on the new privacy regulation from one of the following three angles: legal aspects, aspects relating to governance within organisations or philosophical aspects and social impact.

Well, we definitely got what we asked for. We received no fewer than 41 high quality essays, and from an array of surprising angles and opinions our jury of professionals ultimately selected three winners. They took home a charming little Erasmus figurine and a cheque for 250 euro. This book brings together the various essays that landed on our desk. We've ordered them according to the category in which they were entered, with each chapter headed off by the winning submission.

Reading through the essays, I am confident that the next generation can be entrusted with the complex issue of privacy. I wish you happy reading!

Mirjam Werges
Chief Information Officer, Erasmus University Rotterdam

Table of content

I agree, but to what terms?

Winning essay by: Lisanne van Ruiten
Category: Legal aspects

7th of May 2018
Dear diary, today the world has become too small of a place. After I came home from the beach, I got a friend request from some guy I saw there, but I don't even know him nor did I tell him my name! I am almost sure I had my privacy settings on friends only... Even my friends found it weird and stalkery. Luckily, I can still click 'delete request'.
Love Lisanne

If I could save only one thing from my house, it would be my diary. Not because it contains my secret cash stash, but because it contains my memories, my experiences, and above all, my secrets. For over 10 years I kept it offline, and still do, for one simple reason: privacy.

However, an innumerable amount of my data **is** online, most of it likely without my knowledge and I am sure, some of it, without my consent. Because how many times have you clicked the "I agree to the terms and conditions" without reading them? For me, more times than I care to admit. Only in the past years, I started readings (parts) of what I was previously so blindly agreeing to. Usually, nothing harmful, some data is shared, some data is kept temporarily or not at all. But in case of doubt, I still click the agree button, simultaneously sending just a little part of me for others to keep. My mind quickly justifies the action with "I've got nothing to hide". But, so what? It's **my** data, does that not mean I should get a say in what happens with it?

The recent Dutch privacy law – 'de sleepwet' – shows that the answer to that particular question is a resounding "no". The law will, among others, allow them to access and monitor data from anyone, without reason.

Despite such an obvious violation of our right to privacy, as stated in the 10th article of our constitution, only a slight majority voted against such extreme measures. I was completely perplexed by such results. Can people not see that we're trading supposed safety for our lawful rights? What we have right now is what I like to call "pretend-privacy". Companies and governments **pretend** our data is safe and private, but they cannot guarantee it.

"If I could save only one thing from my house, it would be my diary."

The coming regulation of General Data Protection Regulation is supposed to change this. After the last Facebook scandal, the EU has finally awoken from their dazed, uninterested attitude towards data and social media. Too little, too late? I cannot say, but personally, I do not know if I will ever get rid of the feeling that everything I do online, is always monitored in some way. Maybe George Orwell was not so far off after all: "If you want to keep a secret, you must also hide it from yourself."

25th of May 2018
Dear Diary, today I choose to no longer agree to your conditions. Can you get me another notebook?
Love, Lisanne

Privacy in society

Essay by: Marlous Albers
Category: Legal aspects

According to Al Gore, in the digital era, privacy must be a priority. According to the law, personal data means any information relating to an identified or identifiable individual[1]. Personal data can be qualified as so-called sensitive data, in the sense that stricter measures must be taken. We live in an era that is defined by a global scale (r)evolution of information technologies.

1 Cnil.fr, N.D.

Due to technological developments the collection, analysis, and storage of data has become easier and have strengthened the ability and incentive of firms to gather personal data of their clients[2]. Therefore, it can be stated that the exclusive access to data can be seen as a competitive advantage for firms. Eventually, although technological developments may benefit the consumer, it may also lead to consumers being helpless to control their personal data. By offering free services, personal data can be monetized[3], or firms can behave in an anticompetitive way: e.g. price discrimination facilitated by the collection and use of data[4].

It can be said that the quantity of data will grow tremendously. Annually, it will grow with 40 percent[5]. In some sectors, this percentage is even higher. For instance, the healthcare sector, logistics, transportation and the energy sector[6]. Currently, technology is progressing faster than ever.

The question arises whether the current European regulation can keep pace with these developments. Privacy and security challenges are still not under control. So far, privacy issues are unfamiliar entities in the current (European) legal and normative framework. Risks are not accurately dealt with. To illustrate this, the Data Protection Directive (DPD) 95/46/EC[7] which is currently applicable, was formulated in a whole different technological era. Its outdated provisions have been implemented differently by the Member States of the EU, which has resulted in a divergence in enforcement across Member States. In overall, this resulted in uncertainty and legal fragmentation in the EU.

A regulation that is going to be in force in May 2018 is the 'General Data Protection Regulation' (hereafter GDPR). Hopefully, the enforcement of the GDPR results in a better regulation of both the privacy and security problems, by protecting personal data of all the organizations dealing with data from European consumers. Basically, every organization that processes information related to EU citizens must comply with the GDPR[8].

Hopefully, the GDPR will improve the (European) regulation of personal data and prevent uncertainty and legal fragmentation. Besides this firms hopefully will learn how to deal with this new regulation.

In any case, it shall ensure a unique opportunity to study the legal consequences and implications of the introduction of truly new phenomena into society.

Bibliography

C. Tankard, 'What the GDPR means for businesses', **Network Security,** 2016(6), 5-8.

Cnil.fr, '**personal data definition**', N.D., online via: https://www.cnil.fr/en/personal-data-definition (last visit: 10-05-2018).

G.A. Manne & B. Sperry, 'The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework', **Competition Policy International**, 2015, online: https://www.competitionpolicyinternational.com/the-problems-and- perils-of-bootstrapping-privacy-and-data-into-an-antitrust-framework (last visit: 10-05-2018).

J. Almunia, '**Competition and personal data protection**' (speech Privacy Platform event: Competition and Privacy in Markets of Data), 2012, online: europa.eu/rapid/press-release_SPEECH-12-860_en.html(last visit: 09-05-2018).

K. J. Kuilwijk, '**Big Data, The internet of things and Competition law**', 2016, online: https://www.akd.nl/Downloads/PublicatiesPDF-EN/07-06- 2016_BIG%20DATA_COMPETITION_LAW_KJKuilwijk.pdf (last visit: 10-05- 2018).

P.P. Tallon & J. E. Short & M. W. Harkins, 'The Evolution of Information Governance at Intel', **MIS Quarterly Executive**, 2013, 12(4).

2 Almunia 2012.
3 Kuilwijk 2016, p. 5
4 Manne & Sperry, 2015.
5 Tallon & Diego, 2013.
6 Tallon & Diego, 2013.
7 EU Data Protection Directive (also known as Directive 95/46/EC).
8 Tankard, 2016.

Privacy? Who Cares!

Essay by: Sanne van Essen
Category: Legal aspects

Even though everyone is sharing more of their personal life than ever on, for example, Instagram, we have never cared more about our privacy than we do nowadays. A relevant example of our care about privacy is the renowned Facebook affair.[1] Moribund Facebook users reacted to this affair by deleting their Facebook profile. It is far from ideal if someone else is spreading your personal information for you.

1 N. Confessore, 'Cambridge Analytica and Facebook: The scandal and the Fallout so far', **The New York Times** April 4, 2018, www.nytimes.com.

What looks like a sufficient solution to protect personal data of natural persons in the future is the General Data Protection Regulation, which will be implemented in the member state of the European Union on May the 25th.[2] The protection of natural persons in relation to the processing of personal data is a fundamental right, which needs to be protected. In order to make sure this right will be protected at its best, the European Union wanted to harmonise the legal aspects of the protection of privacy. The Union tried to attain this by, for example, the following decree: companies are obliged to make their privacy statement written in a language that can be understood by any individual. In this statement the enterprises explicitly say what the actual purpose is of the collected data, and for how long they will store this data in their administration. After reading the regulation it looks like the European Union endeavours to do everything to secure the best protection for the companies that collect personal data. The question remains, nevertheless: will this be enough?

"What if a data leak will take place at your insurance company?"

Although this regulation looks like a useful solution for the current shortage in the national laws, there is still a side of the privacy leaks that remains to be unexposed, because there is not such a law that can protect you from the data leaks that will take place. The most significant problem at this side of the spectrum is that companies require more and more personal data. The trend was common for online sites like Facebook.

However, nowadays, even the toys of your kids, your car and your watch our collecting your personal information. During this digital revolution even your medical reports can be found online. Even if you have nothing to hide, no one will like the idea of finding their medical reports or bank details on unknown platforms.

Due to the General Data Protection Regulation, companies are obligated to destroy personal date after some time. This will, obviously, decrease the risk of data leaks. But, what if a data leak will take place at your insurance company? Or at the Ryanair website where you have an account? Is there even a law to completely destroy the risks of a data leak? Those questions will stay unanswered, even with the new regulation. I am sure this regulation will partially mitigate the risks of data leaks and I am delighted with this new law, which can protect our fundamental right of privacy better than our national laws could, but there are always parts of a problem that cannot be solved with laws.

2 Regulation 2016/679 of the European Parliament and of the council.

Unpopular, boring but crucial: **electronic privacy in the 21st century**

Essay by: Carine Huurman

Category: Legal aspects

A lot of wars have been fought over times with only one goal: freedom. During the Dutch revolt, the Dutch citizens fought for their political independence and religious freedom. During the Second World War, the Dutch inhabitants struggled against the Germans because they wanted their freedom back. Nowadays, we also face a "freedom conflict": the huge availability and privacy dilemma of data.

Via cookies it is much easier to adapt to the consumers demand. Via this way, YouTube watchers can stay on the website for ever because every time another, similar video pops up on your screen. Where is your privacy? Another example, if you watch websites as Booking.com or Cheap Tickets the hotel or plane you looked at might follow you the rest of the week. Where is your privacy?

Nowadays, data from individuals and companies is often stored electronically. New apps and new organisations enter the market. Therefore, the privacy rights and protection of data gets more and more important.[1] To secure the future privacy new laws need to be addressed. As the government guarantees the protection of the individual and her rights by law, it has to safeguard the personal data as well. But as the protection of data is not only an issue on a national level but far more wider, it should not only be addressed on a national or European level but also on a worldwide level

The other edge of the coin is that when an individual accepts that his or her data is used for commercial goals, it would give organizations new and legal opportunities to meet the demands of the consumer. It could provide them with information about their location, favourite products and destinations. The same idea as cookies but then more clearly states what happens to the gathered data. Besides that, by making the law considering privacy on the internet more explicit, it will be easier for the government to punish prosecutors.

Because than the law clearly states what is allowed and what is a crime. Less crime would lead to a safer and more pleasant worldwide electronic environment. This would probably lead to a further increase in online transactions, which would boost the economy. Moreover, clearer rules would make citizens aware of what could happen or happens to their data. Nowadays, the rules considering privacy are hidden in a long official document. As a consequence, a lot of internet users skip these privacy statements. Therefore, they are unaware what the consequences actually are.

"But this war about freedom and individual rights has not ended yet."

Therefore in this work, I want to emphasise the importance of privacy and the essence of a clear formulation of the privacy statement not only on an European level but also on a world level. As internet and other electronic transfer will be the future, investing in these networks is essential to guarantee the privacy and individual rights of the citizen. A lot of wars about freedom has been fought. But this war about freedom and individual rights has not ended yet. Therefore, awareness of the citizen and governmental intervention is crucial.

1 EU General Data Protection Regulation," General Data Protection Regulation, European Union, accessed May 2, 2018, https://www.eugdpr.org/.

Mind Your Data

A Legal Inquiry into Europe's Battle for Privacy

Essay by: Yazan Jondi

Category: Legal aspects

Of the endless variety of fiery controversy characterizing the 21st century partisan scene, little is more contentious than the question of privacy; where does it begin, where does it end, and how do we protect it? Overall, the General Data Protection Regulation (GDPR) can be seen as a glimmering light in a sea of uncertainty; a light which has as its objective the refinement of European citizens' freedom.

Such a refinement is to be achieved vis-à-vis the introduction of a new set of digital rights in an age of ever-increasing economic value of personal data within the digital economy. Examination of this regulation from a legal perspective endows us an understanding of the favorable consequences and repercussions associated with the GDPR's EU-wide implementation. The privacy regulation is uniquely distinguished from its predecessor and foreign counterparts by its far-reaching implications not only for governments and business enterprises across Europe, but also for the very citizen bodies which they purport to serve.

"This can be regarded as a democratization of the previously-concealed system of data collection."

Firstly, the legal essence of the GDPR lies in its nature as a regulation; as opposed to a directive, which is an alternative form of EU legal action, regulations carry directly binding legal force throughout all Members States and are directly applicable. This consequently waives the requirement of individual national governments to pass any enabling legislation. In turn, this self-executing character of the GDPR grants it its authoritative nature as a measure determinedly aimed at addressing the increasingly obscure issue of citizens' privacy rights, as well as the limitations on those rights. Despite its classification, however, what truly differentiates the privacy regulation as invaluable are the numerous solicitous provisions contained within.

By compelling data-collectors to clearly document lawful bases for the processing of personal data, the GDPR effectively introduces various new legal mechanisms for the upholding of accountability and transparency in data collection. In effect, this can be regarded as a democratization of the previously-concealed system of data collection; a democratization achieved in full through the rule, letter, and spirit of the law. This democratization process is then furthered by giving unprecedented control to citizens and residents over their own personal data through provisions granting a set of newborn digital rights..Namely, these rights include but are not limited to citizens' right of access, the right to erasure, and the right to data portability.

Strategically, the chances of universal compliance with this new privacy regulation are greatly increased by the GDPR's providing of a strict data protection compliance regime, characterized by severe penalties of eye-watering financial sums. Moreover, the legal basis for compliance is significantly extended by harmonizing the matrix of data protection regulations across the EU; subsequently making compliance easier for both European- as well as foreign-entities. In light of this, we find that the GDPR ought to be welcomed as a fruitful, citizen-oriented policy breakthrough aimed at the democratization of the digital realm; a **digital democratization** to be achieved wholly under the **purview of the law**.

Privacy? Who cares!

An essay on legal aspects of the General Data Protection Regulation (GDPR) on individual privacy rights in the EU

Essay by: Despoina Mouridi

Category: Legal aspects

Introduction

The General Data Protection Regulation (GDPR)[1] was adopted in 2016 by the European Parliament and the Council replacing the EU Data Protection Directive of 1995[2] and it shall enter into force on the 25 May 2018.[3] The new framework appears to enhance the individuals' control over their personal data and to impose stricter obligations upon the collectors and processors of such. The question however is whether the DGPR has an actual impact on the protection of the privacy rights of the individuals within the European Union.

1 Regulation EU 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC, 27 April 2016.

2 Directive EC 95/46 of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995.

3 Regulation EU 2016/679, art 99(2).

The GDPR framework

The GDPR launched a set of novelties in relation to the 1995 Directive,[4] the main of which could be concentrated to a widening of the definition of personal data,[5] to the requisite of express consent of the individual for the control of the same,[6] to the enhancement of the right to be forgotten[7] and to data portability,[8] and most importantly, to the imposition of fines for violations of the Regulation,[9] and the right to initiate individual proceedings for compensation.[10] Additionally, the Regulation enjoys extraterritorial application.[11]

The relation of the GDPR to privacy rights

Following the above, it is fair to argue that after the entry into force of the GDPR, personal data will enjoy a greater level of protection compared to the past. This, however, does not, strictly legally, equal a strengthening of the individuals' privacy rights.

Privacy and data protection are not identical notions in the European Union's legal regime, and this is reflected by the fact that they are separately regulated in the statute (the former by Article 8 of the ECHR and the latter by Article 8 of the Charter).[12]

In the same context, the GDPR does not aim at enhancing privacy rights. First of all, while the previous 1995 Directive contained the word "privacy" 13 times in its text, the word has been completely eliminated from the body of the Regulation.[13] And secondly, the fact that the new legislature comes under the form of a regulation instead of a directive, intends to eliminate differentiations of the national implementation of its provisions, in order to facilitate the transnational flow of personal data, for the sake of commerce.[14] This conclusion is affirmed by the Regulation's recital (9).[15]

Consequently, the GDPR does not address situations involving data collection that plausibly interferes with privacy rights, such as Big Data collection by governments or enterprises.[16] In those situations, the individual is only plausibly identified and therefore the proof of an infringement upon its privacy is seriously hampered. Apart from that, the Regulation does not also answer questions of how the individual can be protected against personal data collection, since much of this activity remains, most of the times, unknown to it.[17]

Conclusion

In conclusion, the GDPR provides for a framework that will enhance the protection of privacy of the individuals in relation to personal data. However, since privacy considerations are not quintessential to the Regulation, the relevant protection can only be limited.

Bibliography

Directive EC 95/46 of the European Parliament and of the Council, 24 October 1995.

Farrel L, 'The General Data Protection Regulation', Business Premium Collection, Recruiter 2017, 6

Kokott J, Sobotta C, 'The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR', 3 International Data Privacy Law, 2013, 222.

Regulation EU 2016/679 of the European Parliament and of the Council, 27 April 2016.

Sloot B, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' in R Leenes et al (eds), Data Protection and Privacy: (In)visibilities and Infrastructures, (Springer International Publishing, 2017, ISBN 9783319561776), 3.

- - , 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation', 4 International Data Privacy Law, 2014, 307.

Voigt P, Bussche A, The EU General Data Protection Regulation (GDPR) A Practical Guide, (Springer International Publishing, 2017, ISBN 9783319579580).

4 L Farrel, 'The General Data Protection Regulation', Business Premium Collection, Recruiter 2017, 6; P Voigt, **A Bussche, The EU General Data Protection Regulation (GDPR) A Practical Guide**, (Springer International Publishing, 2017, ISBN 9783319579580), 3ff.

5 Regulation EU 2016/679, art 4(1).

6 **Ibid**, art 7(2).

7 **Ibid**, art 17.

8 **Ibid**, art 20.

9 **Ibid**, art 83.

10 **Ibid**, art 82.

11 **Ibid**, art 3.

12 J Kokott, C Sobotta, 'The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR', 3 International Data Privacy Law, 2013, 222.

13 B Sloot, 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' in R Leenes et al (eds), **Data Protection and Privacy: (In)visibilities and Infrastructures,** (Springer International Publishing, 2017, ISBN 9783319561776), 3.

14 **Ibid**.

15 Regulation EU 2016/679, rec. (9).

16 B Sloot, 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation', 4 International Data Privacy Law, 2014, 307.

17 **Ibid**.

Privacy? Who cares!

Essay by: Vasilis Zachos
Category: Legal aspects

I do. And so should you. Privacy is a human right that is fundamental to a decent human existence. Less privacy means less autonomy and therefore less or no freedom at all. Privacy is essential to the protection of our dreams and our fears. Our insecurities and our wildest fantasies. From this perspective, privacy is important for the individual.

At the same time, privacy is critically connected to the integrity and the functioning of our democracy and the rule of law. Why? Because the infringement of individual privacy can disadvantage the whole of society. Extravagant? Not really. When the privacy of journalists and their resources is infringed, does this not have significant consequences for our collective right to a free and independent media? When the privacy of lawyers and their clients is infringed, does this not have significant consequences for the right to a fair trial?

When we discuss privacy, we should recognize that privacy includes our self-government to protect our personal information, our right to be let alone and our desire to make our contribution to a free society. Privacy is the wrong right to be half-hearted about. The right to privacy contributes too much to our lives and our democratic society to take this fundamental right for granted.

In the light of national security and complex threats, such as international terrorism and cyber warfare, privacy is under severe attack. From this perspective, privacy is no longer the guarantee against arbitrary government action. Privacy is the obstacle to the desire of governments to organize a society in which all risks are banned. Let us be honest, if you can choose safety or freedom, which one shall prevail? The correct answer should be that is no choice at all!

The trade-off between privacy and security is short-sighted, misleading and utterly dangerous. The devaluation of fundamental rights, such as the right to privacy, will not lead to more safety. Moreover, I would argue that in the context of the trade-off debate, in which privacy and security are presented as antagonistic values, it will most likely result in more insecurity for citizens. Why? For the simple reason that human beings lose one of the most important human rights that makes them full-fledged citizens.

“Let us be honest, if you can choose safety or freedom, which one shall prevail?”

Does this mean that I am naive about the current security challenges that modern states face? Perhaps. Nevertheless, I am convinced that in the long run, it would be harmful to our freedom and to our democracy to accept possible infringement of our privacy for the promise of enhancing security, which is highly contradictory in itself. Privacy and security are no rivals. This cannot be reduced to a dichotomy. Privacy and security should both prevail in the digital age.

To conclude in the words of Billy Graham, I would argue that is indeed true that **once we have lost our privacy, we will realize that we have lost an extremely valuable thing** to human beings.

GDPR- aspects regarding governance in organisations

Winning essay by: Ionuț Hodoroagă

Category: Aspects addressing governance in organisations

Nowadays, being able to control and trace your personal data provided to a company or organization of any kind has increased in significance. That is why I strongly consider that the GDPR will greatly impact the way firms and institutions are governed, as it will now give the customers more power over their data than ever before.

Since the introduction of the Internet, there have been far too many years that allowed unclear user agreements and incorrect data protection of the users of any content. Yet, this will not be of concern anymore, or will it?

“However, in the past years, there have been few known cases of small companies mismanaging user data.”

With the introduction of GDPR, considering its penalties, most of, if not all the firms will have to comply with this regulation. I believe this will greatly affect big successful firms mainly because of the attention they get through all media channels. Clients of those companies who are aware of the GDPR will likely request to know if their rights are fully respected. Following the buzz marketing principle, they will influence others regarding how the company/organization misuses their own personal data.

A very particular example is Facebook, which recently had its CEO, Mark Zuckerberg testify before the Congress of the United States about how the organization he founded, albeit Facebook, compiles and distributes the data of its 2 billion users. This led to immediate changes in policy and user agreements on all the apps that Facebook owns (Instagram, Snapchat, and even WhatsApp recently).

However, in the past years, there have been few known cases of small companies mismanaging user data. That is because the way the regulations are made, the focus is not actually on protecting all the consumers' data, but on protecting the users of big companies' data (as in the users of Google, Facebook and so on).

Considering this, even though small businesses comply with these changes, even partially, should complaints from their users arise, they will most likely be ignored, due to the unimportance of that certain business or due to the very “low” number of complaints from users.

Thus, in the sense described above, the GDPR poses an insignificant threat to small businesses, no matter what approach they take, because breaches in their systems are much harder to detect and by having few users, they can still manage the data the way they consider. Successful businesses, on the other hand, will continue receiving complaints for unfair uses of data, all while having applied the new regulation accordingly. This could be because of “too many” reports from unsatisfied users with regards to their control over data.

While the GDPR seems like a strong new regulation in EU coming with huge sanctions and whose purpose is to protect all users' data and empower their control over it much more than before, it will likely fail on small organizations. This is unfortunate, considering that most of the breaches that remain unsolved are made on those small platforms.

Privacy: we do not care enough about it

Essay by: Maha Ashraf Ali

Category: Aspects addressing governance in organisations

In just fifteen days, 85% of organizations surveyed by Deloitte will collide headfirst with the General Date Protection Regulations (Luysterborg, 2018). These unprepared organizations will face customer backlash for failing to meet their data protection requirements... or will they?

Approximately 91% of the U.S. population does not read the 'terms and conditions' (Cakebread, 2017) that they so quickly agree too – and you cannot really blame them. This section, riddled with complex legal terms, is difficult to understand and is ignored by those who simply want to access a website or use an app. Despite the GDPR now requiring businesses to simplify their 'terms and conditions' for the convenience and the benefit of consumers (In 3 Minutes, 2017), it is still hard to imagine that all consumer's will read this information. For example, with the uproar surrounding Facebook regarding privacy and lack of consumer data protection, the company's stock price rose by 5% (Spangler, 2018). It rose. Facebook was on trial for violation customer's privacy and yet, despite the uproar, not only did its stock price increase, its consumers continued to use and post on the social media network.

How is this possible? The answer could lie in the immense role of social media in our everyday lives. We have come to rely on social media to connect with others, share our lives, and advance our own personal or business interests. In a research conducted by the Ponemon Institute (Clay, 2015), social media and privacy were researched collectively. It was found that while there was an increase of 6% in 'privacy sensitive' customers, these customers were unlikely to change their online activities regardless of any cyber-incidents (Clay, 2015). On the other hand, the number of 'privacy centric users', who would change their behavior given a breach of their privacy, decreases by 8% (Clay, 2015). Perhaps the implication of this startling statistic is that customer's feel powerless to stop their invasion of privacy and have come to accept a world in which none of their information is private.

Perhaps, consumers are right to feel overwhelmed by the grandiosity of this problem. Even if the GDPR is implemented efficiently, only 15% of companies are ready to face this change (Luysterborg, 2018). As for those who can't, they face large fines that could reduce consumer satisfaction. But will those consumer's stop using those services they deem to be of higher value than their privacy? With regards to Facebook and it's linked platforms, the answer is appears to be no.

At the end of the fifteen day countdown, the GDPR will pass. Consumer's may appreciate the idea of being more protected, but whether or not it will affect their life or their usage of web-platforms remains to be seen. For now, consumers will continue to ironically tweet and post about the values of the GDPR on the very platforms lacking the privacy they so desire, but are not willing to sacrifice for.

References

Cakebread, C. (2017). **You're not alone, no one reads terms of service agreements.** [online] Business Insider. Available at: http://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of- service-without-reading-2017-11?international=true&r=US&IR=T [Accessed 10 May 2018].

Clay, J. (2015). How Much Do We Value Security and Privacy on Social Media?. [Blog] **Trendmicro**. Available at: https://blog.trendmicro.com/how-much-do-we-value-security-and-privacy-on- social-media/ [Accessed 10 May 2018].

In 3 Minutes (2017). **Introduction to General Data Protection Regulation(GDPR)**. [video] Available at: https://www.youtube.com/watch?v=n5WJOncaHt4 [Accessed 10 May 2018].

Luysterborg, E. (2018). **Deloitte publishes results of EMEA-wide survey on GDPR readiness | Deloitte Belgium | Risk Services.** [online] Deloitte Belgium. Available at: https://www2.deloitte.com/be/en/pages/risk/articles/gdpr-readiness.html [Accessed 10 May 2018].

Spangler, T. (2018). **Facebook Shares Climb as Mark Zuckerberg Testifies at Senate Hearing.** [online] Variety. Available at: http://variety.com/2018/digital/news/facebook-stock-mark-zuckerberg-testifies-senate-1202749625/ [Accessed 10 May 2018].

GDPR and the value of people

Essay by: Simon Bothof

Category: Aspects addressing governance in organisations

I could say that I care about my privacy. But what does privacy really mean? And what is the result of the new General Data Protection Rules (GDPR) aiming to protect this 'privacy' of ours? Asking the first question to different people results in a range of answers: From not having (too much) personal information publicly available (online or offline), to not wanting to be tracked by any organization (be it private corporations or governments). Even though perceptions about privacy might differ per individual, everybody seems to have some sense of what information about themselves they would rather not share.

But wherever your boundaries between private and public may lie, corporations probably do not agree. Especially corporations in the tech sector seem to have no clue at all about the existence of such boundaries. In the world of big-data and machine learning quantity is key, and therefore a data- collection competition is taking place right now. The fact that this happens is understandable, from an economic perspective, as the prizes to be won are big. The corporation that can gather the most amount of data will eventually be the one who can outperform competitors in, for example, targeted marketing services, facial recognition and predictive software, allowing them to dominate the market once and for all.

Another result of this race for data is, however, that businesses sometimes seem to forget that behind the entries in their database real people exist. People with feelings, secrets and a life of their own. (Tech-)companies see only an unlimited supply of resources, freely provided to them through the use of their services. For them there are no people behind these resources, there is just more information waiting to be gathered, mined and monetized. The GDPR is a good instrument to force businesses to consider the people behind their datasets again. Regulation did exist already, but with this EU-wide set of rules there is a strong power base that can enforce them on even the biggest multinationals. People will no longer be kept in the dark about what user data is gathered by which companies, as businesses are being forced to disclose this and are obliged to ask permission in the first place. And probably even more important is the fact that individuals can take control of their own data again.

No longer will corporates be the sole owners of the data they have gathered; individuals will be the owners of their personal data as well. This allows, for example, for the right 'to be forgotten'. Instead of being just resources for companies, people can be seen as people again, with an intrinsic value going beyond, or actually coming before the potential economic value of the datasets that represent them. This way regulations can help us move towards realizing the democratic dreams of the internet again, as an open and public space that empowers people all over their world, instead of allowing for internet companies to take our powers away.

"The fact that this happens is understandable."

Limitations of GDPR in the Age of Planetary-scale Computation

Essay by: Andrew Dryhurst

Category: Aspects addressing governance in organisations

I believe that the GDPR is a timely and necessary piece of legislation. The two main advantages of the GDPR are that it signifies an end to the unchecked data extraction practices of the large-scale Internet platforms that have characterized Web 2.0. Secondly, the GDPR's emergence alongside the revelations about Cambridge Analytica's malicious manipulation of Facebook's non-existent screening processes has brought the issue of data into the realm of public consciousness and debate.

However, whilst the GDPR represents a step in the right direction, it is not sufficient to deal with the megastructure of planetary-scale computation that Benjamin Bratton refers to as 'The Stack'. New forms of data regulation need to be underpinned by a new conception of data that attributes it with emergent properties that go beyond an homeostatic entity that can solely be understood in terms of its form and content.

"If we do not grapple with the question of value we could very well steer into to an irreversible situation."

If we look at platforms such as Facebook or Google, their use generates a cycle wherein the curation of user experience simultaneously shapes and is being shaped by emergent new user preferences.

Another example is the case of machine learning (ML) and artificial intelligence (AI). The data that is (and isn't) fed into AI is imbued with the motives, biases, and worldview of those who are inputting the data. Secondly, it is often unclear to the human observer exactly how AI makes the decisions that it does, thus causing us to question our own rationality through the dialectical production and reproduction of value. That is to say, we will learn from the outputs provided by the AI and use abductive reasoning to try and understand not only the results, but how it reached the conclusions in the first place.

Consequently, regulation such as Article 22 (1) of the GDPR which states that every person has the right, **"not to be a subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her,"** is insufficient because no decision is solely based on automated processing, and the data involved has emergent properties that differ depending on the context surrounding its use.

Furthermore, planetary-scale computation has transformed our political geographies. They are no longer demarcated by divisions by land pertaining to nation states, but are contestations of sovereignty between states, private actors, and digital platforms that are occurring simultaneously in the material and digital arenas. Before effective regulation can be formed to deal with this new paradigm, we first need to understand the political rights and ethical responsibilities of platform users in relation to states, markets, and platforms themselves. This requires a new language that is situated in the multifarious and abstract forms of value that are present at this current moment of platform capitalism. Large platforms are already shifting their business models from data extractivism to the leasing of 'AI services' that are built with our data to Governments and private actors (Morozov 2018). If we do not grapple with the question of value we could very well steer into to an irreversible situation.

Sources

https://www.theguardian.com/technology/2018/jan/28/morozov-artificial-intelligence-data-technology-online

https://www.youtube.com/watch?v=IXan6TvMqgk

https://tuinvanmachines.hetnieuweinstituut.nl/en/stack-and-posthuman-user-interview- benjamin-bratton

Connecting the People of the World

Today's Most Lucrative Way to Spy on the Masses

When Discreet Collection and Processing of Private Data for Commercial Purposes Officially Gets Recognized for Its Abusive Nature and Criminal Potential

Essay by: Isaac Gabel

Category: Aspects addressing governance in organisations

On May 25th, 2018 a long overdue supranational legal enforcement approved by the Parliament of the European Union (EU) on April 14th, 2016 will be enacted, the General Data Protection Regulation (GDPR). The revisited regulatory measures aim to protect EU citizens from cunning institutional strategies for amassing sensitive private information for careless commercial gain.

Abusive secretive practices of regular and systematic collection and processing of private data have long been neglected, mainly due to lay people's indifference for the act. Ignorant people often express indifference for reckless private data collection and processing because of a commonly occurring failure to realize the unimaginable and far-reaching direct and indirect real world impact and implications the use and abuse of sensitive information can have in inappropriate or greedy hands.

Trust in commercial institutions for privacy matters is frequently undue, as we fail to realize the type and vast amounts of obtained personal information, together with how fast and easily digital information can be transferred, leaked or stolen, either willingly or unwillingly, and either knowingly or unknowingly, potentially getting in the hands of obscure or sinister third parties. Recently several high-profile privacy infringing data breaches have reached public debate, but more often than not the most shocking, prevailing and significant privacy scandals remain unpublished and unmentioned. The enforcement of the GDPR is evidence of raising concern of the prevalence, increasing impact and potential implications of unethical amassing and handling of private and sensitive information.

Under the GDPR several noticeable compulsory policy changes have been introduced for all entities involved in the acts of data collection, storage and processing of EU citizens. First we can note the wider jurisdiction the GDPR employs, reaching even out of the EU as long as the subject of data collection is situated in the EU. Moreover, any monitoring of activity or behavior is subject to GDPR legislation, even when no financial transactions take place in the process.

Applicability extends to both data collectors and processors, enforcing the presence of representatives in the EU carrying full responsibility. Financial forfeits for breaching privacy and data protection requirements are supposedly high enough for the regulations to be taken seriously. The regulatory specifications concerning properly informed consent from data subjects have been elaborated. Long and easily ignored terms and conditions with easily overseen or vague privacy matters aren't allowed anymore. Short, clear, sufficiently informed and separate consent is required before the start of data collection and processing. Additionally, withdrawing consent must be possible and equally straightforward.

"Accessed personal data should be portable and transferable."

Data subjects get increased rights of transparency and control over their data, such as the right to access collected personal data, including where and for what purpose it is being processed, free of charge. Accessed personal data should be portable and transferable. Furthermore, data subjects have the right to be forgotten, implying complete erasure of personal data and a halt of processing by third parties.

Whether the GDPR will hold true to its purpose and promise of restoring and ensuring public privacy protection is still unclear.

Privacy? I (should) care!

Essay by: Tjark Gall

Category: Aspects addressing governance in organisations

With one scandal following the next, data protection and privacy rights discussions are breaking out everywhere. People shout for the government and companies to revise their policies and save us… Without undermining the government's role, what data are we talking about? Is it not the data which we all choose to share? Is it not the data which we voluntary uploaded to endless social media and information platforms? Is it not the data which we provide by answering superficial quizzes and future predictions on Facebook or by confirming the regulations of yet another variation of Candy Crush?

Everyone (excluding minors!) should know for himself what she or he wants the world to see and what not. And yes, maybe some large data mining companies might use them to show specific advertisements or political campaigns, but this is no secret anymore for over a decade. And is it not still each individual who clicks on them or decides what to buy or who to vote for?

"Did it convince me to believe that we are living on a flat disc?"

A few weeks ago, I watched a video about the Flat Earth Society in my Facebook feed and became curious (and considered a better alternative than working on my thesis). I started watching it. After several more about people building their own rockets to prove NASA's photos wrong or fascinating attempts to explain the theory, I stopped and decided to turn my attention to more substantial things. I did not think about it anymore. However, over the next couple of days, Facebook recommended me more and more videos about the same flat-earthers and other conspiracy theories. Did I watch some of them? Yes, for sure. Did it convince me to believe that we are living on a flat disc? No, at least not yet. But I am sure that another 100 videos will not change my mind either.

I firmly believe that despite political efforts and better protection policies, we should start with ourselves and do not forget what data we are talking about. There is no question if it is wrong to misuse our data for hidden interests. But we should be able to decide which information we purposively want to share with the world and which not. The data we are talking about is called personal data for a reason: It is the data about and more importantly, from us. Therefore, I want to answer the questions of 'Who cares?' with 'I (should) care'! And with that, I mean every individual out there who complains about the governments not protecting us from ourselves and seconds later already clicking on something again, uploading more personal information, and filling yet another form of an unknown origin… We should know better!

Data is the New Black Gold

Essay by: Noémie Metz-Vinez

Category: Aspects addressing governance in organisations

Private data has been a crucial matter after the Cambridge Analytica scandal and the newly EU regulation. The GDPR will impose protection of data subjects in the EU territory for a safe free movement of personal data within the EU but also increase safer trade practices in a competitive market.

The GDPR brings the challenge for organisations to protect the right to privacy for consumers while developing their activities (e.g. "pay as you drive" or using biometrics technologies). Whereas in the USA, the Patriot Act enables spying on its citizens and on foreign citizens without notice (American Civil Liberties Union, n.d.).

On a governance point, the GDPR does not simply imply extra costs. Although companies will need to pay for DPO unit, DPIA, staff training, data portability system, etc., these costs are balanced by advantages, as listed below:

Reputation advantage: data protection and cybersecurity are one of the main concern for governments, customers and stakeholders (Facebook's shares price fell by 6.8% after the announcement of a data breach by Cambridge Analytica (Christopher Brennan, 2018)).

Competitive advantage: building trust between business and customers, benefiting from data portability (mobility of customers and data recovery without manual treatment), harmonizing competition between companies operating with EU consumers

Costs reduction: internal company rules, safety measures and procedures will be the same in order to streamline departments

Lessen the risks of fraudulent behaviours: the more unified the procedures are, the less the breach will occur or the more it could be detected

As part of the governance, organisations will have to appoint a DPO who will assume the compliance with the regulation and holds the Record of processing. Each new project must be analysed under the aspects of the privacy "by design" and "by default". The clients and the supervisory authority must be informed in any case of "data breach". Acceptance and information of the processing are reinforce for the clients, to whom companies must reply quickly (Trendmicro.com, n.d.).

A challenging point for the governance is to raise awareness about GDPR regulation among the teams and to train them. Nonetheless, GDPR could be challenging for EU firms regarding foreign companies.

Many software used in European companies are from USA, and have no competitive EU offers.

How foreign firms will be compliant with the GDPR which is compulsory for each company having customer on the EU territory? During Zuckerberg's testimony for the Cambridge Analytic, he agreed to apply the GDPR, which is a positive new for Facebook users. However, Facebook changed its headquarters from Ireland to its home country in California (Alex Hern, 2018). This could be considered as "treaty shopping", meaning that because Facebook is now based in the USA, 70% of users' will not be protected by the GDPR (Etienne Combier, 2018).

To conclude, as the use internet has been expanding dramatically over

"Internet has been expanding dramatically over the past 20 years."

the past 20 years, organisations and customers might not be fully aware of the consequences of their present actions. Provided that an user is fully aware of the risks and has read thoroughly the terms and conditions, what power do they have in a case like the Cambridge Analytica scandal?

Sources

Alex Hern. (2018). **Facebook moves 1.5bn users out of reach of new European privacy law.** TheGuardian.com [online] Available at: https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law [Accessed 4 May 2018].

American Civil Liberties Union. (n.d.). **Surveillance Under the USA/PATRIOT Act.** [online] Available at: https://www.aclu.org/other/surveillance-under-usapatriot-act [Accessed 4 May 2018].

Christopher Brennan. (2018). **Facebook stock plummets amid Cambridge Analytica scandal.** NYDailyNews.com [online] Available at: http://www.nydailynews.com/news/world/facebooks-faces- scrutiny-world-cambridge-scandal-article-1.3883495 [Accessed 4 May 2018].

David Berreby. (2017). **Click to agree with what? No one reads terms of service, studies confirm.** TheGuardian.com [online] Available at: https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print [Accessed 4 May 2018].

Etienne Combier. (2018). **Données personnelles : sur Facebook, seuls les Européens seront protégés.** LesEchos.fr. [online] Available at: https://www.lesechos.fr/tech-medias/hightech/0301590955498-donnees-personnelles-sur-facebook-seuls-les-europeens-seront-proteges-2170756.php [Accessed 4 May 2018].

Julien Lausson. (2018). **Mark Zuckerberg face aux sénateurs : les 10 points à retenir.** Numera.com [online] Available at: https://www.numerama.com/politique/344306-mark-zuckerberg-face-aux-senateurs-10-points-a-retenir.html [Accessed 4 May 2018].

Trendmicro.com. (n.d.). **EU General Data Protection Regulation (GDPR)** [online] Available at: https://www.trendmicro.com/vinfo/us/security/definition/eu-general-data-protection-regulation-gdpr [Accessed 4 May 2018].

Privacy? Who cares!

Essay by: Roy Ouwerkerk

Category: Aspects addressing governance in organisations

The hologram projection on the wall of your favourite series automatically closes as the episode ends. It recognises that it is time to meet up with your friends, to go out for dinner, as you discussed online. The wardrobe opens, your jacket ready, and as you walk outside without touching a single door, you see the light shutting down behind you. An autonomous car is already waiting for you, and when you arrive at the restaurant, facial recognition ensures that you don't have to search for where your friends are sitting. Your wristwatch helpfully reminds you of your low-carb diet. You are ready for dinner, all thanks to the wonders of an ubiquitous flow of information.

Of course, your 'favourite' series is only your favourite because of algorithms that determine your taste. It's true; you genuinely enjoy this series. You would have liked to apply make-up before leaving, but the episode was timed to end precisely before you had to leave.

Obviously, you wouldn't want to arrive late, to be seen as anti-social; that's a strong indicator that you might need psychological assistance. You don't, though; you've always been wearing proper black clothes. You know that your wardrobe's data is sent to the national clothing company, to gain insight into the clothing preferences of its customers.

Once, you might have preferred red clothes. But now, it's an issue of public safety, to be able to recognise undesirables by their clothes. The wardrobes of paedophiles are stocked with red, while ill people temporarily get green clothes. Wearing only black is fine, given the benefits.

This essay is not written to show how a utopia of convenience can be warped into a dystopic panopticon. Because we're already there. Of course, it is exaggerated, much like Black Mirror is – until China's Social Credit System reached headlines. It's all based on what is happening currently, here, too.

I should care. I should not want to end up in the second paragraph. But I, and many others, don't care.

Do I not care because I live in a modern country, with a healthy political system, with laws and regulations, further protected by the EU? Maybe, but that is too easy an answer.Instead of dismissing this question with 'laws will be made', I'd like you to actually think it through. How free are your choices, when algorithms decide for you – and is that bad? Does it become bad when the government is involved, instead of a commercial company? Why so, why not the other way around?

"Your wristwatch helpfully reminds you of your low-carb diet."

There's a challenge for you: Can you take the ideas from the second paragraph, and write a third paragraph that is positive, like the first paragraph? What is needed for that? Which ideas can be kept, should be changed, or must be removed?

Will you remember your answer? Or will you let something worse become the new norm? Because I think that is why I don't care; it's 'normal'. I wonder when a Social Credit System will be normal.

Capitalism in the age of big data

Essay by: Xavier Venn Asuncion

Category: Aspects addressing governance in organisations

The hologram projection on the wall of your favourite series automatically closes as the episode ends. It recognises that it is time to meet up with your friends, to go out for dinner, as you discussed online. The wardrobe opens, your jacket ready, and as you walk outside without touching a single door, you see the light shutting down behind you. An autonomous car is already waiting for you, and when you arrive at the restaurant, facial recognition ensures that you don't have to search for where your friends are sitting. Your wristwatch helpfully reminds you of your low-carbon diet. You are ready for dinner, all thanks to the wonders of an ubiquitous flow of information.

The continuous rise of big data and increasing attention to data protection and regulation such as the implementation of the General Data Protection Regulation (GDPR) could lead to the eradication, or at the very least, reinvention of the capitalist system. This may be attributed, in general, to the crucial the use of big data to influence consumer behavior and to formulate strategic marketing activities. Hofacker et. al (2016) explains this using the steps of consumer decision-making process provided by Blackwell et. al (2005). The steps and the corresponding application of big data, according to Hofacker et. al (2016), are briefly explained below:

Problem recognition: a gap in what consumers have prompts desire to avail products or services. Discussions in social media, for instance, can be monitored to identify dissatisfactions in certain products as well as to reveal emerging demands Search: this is where the consumer looks for different alternatives for a product they are looking for. Data on search activities could provide information on which factors could encourage successful and purchases on different digital platforms.

"Digital platforms provide avenues for product reviews and comments."

Alternative evaluation: the digital space provide for vast number of options for consumers. Search behaviors could provide insight on hidden rules on how consumers decide among different product options.

Purchase behavior: Online and non-online purchase environments already incorporate digital recording of purchase behaviors. Consumption: Many goods and services are consumed digitally such as media consumption e.g. Netflix, iTunes; online check-in to hotels and restaurants; uploading pictures of food and places in Facebook and Instagram etc. These activities are recorded digitally which produce data that could inform strategic marketing.

Post-purchase engagement: Digital platforms provide avenues for product reviews and comments which could obviously be used to improve delivery of goods and services.

Although discussed in brief, these show the importance of big data among private groups selling goods and services is. As such, the GDPR, as it makes acquisition and processing of consumer data for private companies more difficult, could lead to reduced effectiveness in marketing and other related where consumer data play a significant role. This is in conjunction to the increasing use of big data to fuel innovative disruptions that could reshape organizational forms (Schrage, 2018) . Schrage further argues that big data could result to data-rich markets where data are more essential for markets to flourish rather than money. This could be perceived within the study of socio-technical transitions whereby the interplay between human and technical systems provide for societal configurations or socio-technical regimes.

Big data have encouraged niches that are penetrating the capitalist regime. We could therefore see that regulations such as the GDPR that hamper the capacity of private companies to access and process consumer data would be detrimental for them especially as the role of big data in marketing is continuously increasing and reshaping the system. This could especially affect EU where the private sector shares a major contribution in the economy as well as in the delivery of important goods and services.

More privacy equals more autonomy

Winning essay by: Mark Tieleman

Category: Aspects of philosophical and societal impact

Imagine you were offered a free floor cleaner. In addition to its cleaning service, this machine also keeps track of your conversations, who comes by, where you go, what you possess and much more. It saves this data in files, with information you would not even tell your spouse and closest friends, and then sells it to third parties, like insurance companies, for them to use as they seem fit. Would you take this free cleaning service? I would not, because this kind of surveillance is a direct assault to a person's privacy and autonomy.

Autonomy is a central value for humans, according to Kant, a philosopher of the enlightenment. He viewed it as the capacity to self-govern, to live one's own life in accordance with reason, in the absence of manipulation and distortion from external influences. Kant's autonomy is the basis of morality and the ability to act freely. It is inherently interwoven with privacy. Privacy's most basic definition is the right to choose when, to whom and to what extent somebody discloses information about themselves. It is a condition to be a human, to be a citizen, to be yourself - without privacy these things are not possible.

It enables people to be vulnerable and to make mistakes without the fear of judgement and eternally being reminded of faults from the past. Privacy is a part of who we are and therefore we should have ownership over it. This is not the case online. What you tell your psychiatrist should not be used by marketeers to sell you self-help books. Users do not own and control the data that contributes to their online self, which is a very rich and personal account of them. That is the reason why they have no privacy online and this has consequences for their real self, in the real world. They cannot fully be who they want to be, if this online self is public and pins them down to what they were, or did. This makes it hard for people to reinvent themselves in our current age and is a direct assault on their autonomy.

"They cannot fully be who they want to be."

The recent crisis with Cambridge Analytica at Facebook, which sold the privacy of their users to third parties that use this for commercial or political gains, is an example of the problems with online privacy. One could argue; it is within the autonomy of the users to sell their personal data for the 'free' services Facebook provides, but people are generally not aware of what is happening with their data and what they sign up for when they accept the terms and conditions, since nobody reads them and no alternatives are given. The EU is implementing a new legislation to empower the people against (big tech) companies, but a lot of the responsibility to safeguard privacy lies within the users.

The new EU laws are a beginning for users to take their autonomy back and restrict the breach of privacy. Users can get insight into their data, what the company does with it and request the deletion of it, because it is their right to be forgotten, even in the digital age. Don't stupidly go 'smart'. Mind your data.

Societal Impact of the General Data Protection Regulation and How it Affects You

Essay by: Rogier Abcouwer

Category: Aspects of philosophical and societal impact

When I entered my personal e-mail address on a data security website[1], to my surprise, I found that my email address had been breached six times. My compromised data includes passwords, email addresses IP addresses, and user names. What does this mean? It means that six websites where I created an account were breached by cyber criminals who intend to use the hacked email addresses for malicious purposes. Was I personally affected? No, at least, I don't think so. My information was simply in a stack with millions of others, which was uploaded to illegal websites. Luckily, my data was not used for crim- inal purposes, and I changed my passwords since. Others can be less lucky.

1 https://haveibeenpwned.com

"The question then is, why should you care?"

This is because personal digital data can hold a lot of value for companies, but also for criminals; they can make purchases on someone else's credit card, perform identity theft, or even blackmail people. Some even make a living with this type of criminal behavior. These criminals can be very hard to find as they are often hidden behind walls of VPNs, different IP addresses, and dark-web browsers. For this, and other reasons, the General Data Protection Regulation (GDPR) was introduced by the European Union, in an effort to give more dig- ital rights to European Citizens, and will go into effect in May 2018. One of the aspects of the GDPR is that companies now have to include data protec- tion measures in their default business processes for products and services. In addition, any data breaches have to be reported to supervisory authorities. In the case that firms do not meet these standards, they can be fined for up to 4% of their yearly turnover.

The question then is, why should you care? It might be useful to see for yourself if your email address has ever been breached. I think it is important to realize that these types of cyber crimes do not disproportionately affect some people rather than others. It can happen to anybody, at any time. Last year the University's own email database was even breached! You should care, because otherwise the moment you care, it will be to late and you will have been an unfortunate victim of a data breach.

Luckily, we now know that the European Union is looking out for the (digital) interests of it's citizens. By giving us a set of "digital rights", firms have to be more careful with our private data and personal information. Prevention is better than cure, as they say. While most people might not even notice that the GDPR has gone into effect (except for that annoying notification on Facebook, or Instagram), the societal impact of such a set of regulations is huge. You can compare it to a vaccine, which stings a little at first (especially for the firms), but can save a lot of trouble later on. So next time when you check your updated privacy policy, know that it is for the good of society.

Privacy? Who cares!

Essay by: Muskan Achhpilia

Category: Aspects of philosophical and societal impact

What is Privacy? The most generic essence encompasses the element of being away from the public scrutiny and revolves around the idea of having an individual right to authorise disclosure of circumstances related to oneself. With the high sovereignty that one has which governs every decision or action especially, in the virtual world, it appears quite questionable why we constantly are bombarded and encounter concerns and controversies over privacy and the lack of it in the virtual world and now, with the upcoming implementation of GDPR.

When the existence or the creation of information is in one's own hand, it seems unreasonable why one should be overly concerned with what is shared or accessible. While many argue that the current laws concerning privacy breed intrusion and surveillance, the choice to enter this arena is completely dependent on one's own decision.

The very nature of the internet involves several parties and stakeholders and this should be realised by any individual to decides to participate in this medium of sharing and communicating. One of the most dominant stakeholder involved is the government. Government surveillance is necessary to ensure the security of its citizens. Even though most of the citizens think that their information should be disclosed with their own authorisation, they rarely realise that extending this friction and hindrance in accessibility would also protect the interest of individuals involved in illicit or unlawful activities.

From a myopic view, one may merely see protecting one's own interest and how certain information should not be accessible to certain parties however, contemporaneously many people do not realise that they are promoting the concealing of the wrongdoings, communications and information of the criminals who are involved in activities right from child trafficking to terrorism; this would never in the long-term yield a benefit to the individual or the society at large. WikiLeaks an organisation for example, which possesses a massive amount of important data and functions as a protection intermediary can potentially greatly enhance the security of a nation and prevent wrongdoings. It can be argued that individuals can be more informed and aware about the flow of information

"Government surveillance is necessary to ensure the security of its citizens."

however, I believe that preventing access is not the most desirable route to follow. In real life also, one does not face full-proof privacy whether it's your neighbour or a friend, there is always some revelation of information that might not be originally intended. If individuals are highly concerned about who accesses their information they should be more cautious, rather than preventing the legal authorities from reaping the advantages of technological advancements in protecting the society.

Privacy? Who cares!

Philosophical aspects and societal impact of the EU General Data

Essay by: Ioannis Athanasiou

Category: Aspects of philosophical and societal impact

The widespread use of the Internet, in the context of personal and professional activities, leads to the collection of data and the creation of information tanks. The provision of personal data by citizens is now a prerequisite for access to private and public-sector products and services. Personal data are transformed into commodities and consequently individuals become vulnerable to the manipulation by private and public authorities.

The opacity of new technologies and the fact that European citizens are less well informed than those responsible for processing personal information, have raised the need for a consistent and uniform application of personal data protection measures in the European Union. The implementation of the EU General Data Protection Regulation (GDPR), which will replace the Directive 95/46/EC, aims to remove legal ambiguities and uncertainty about the rules of law in the Member States in the new digital age.

"The big bet undoubtedly lies with the European citizen, after pressing the 'enter' key..."

The GDPR will strive to balance this unequal relationship between subjects, controllers and processors of data, ensuring that subjects' rights are expanded and the responsibilities of the latter two are increased and tightened. It is a set of principles and procedures related to the quantity, quality, collection, processing and storage of the subjects' personal data to ensure that they are efficiently protected.

Businesses, regardless their size, object, location and legal status, must abide by new legislation. They need to make a fair and legitimate processing of data in a transparent, confidential and objective manner. The amount of data required will be limited and eventually be collected, processed and stored for clearly defined purposes and timeframes. As far as the data subjects are concerned, their "shielding" and their right to self-determination will be enhanced. The protection of their privacy will be ensured and their active participation in the data management processes will be widely pursued.

It is obvious that complying with the GDPR is one of the most important challenges for businesses. Those who will incorporate its requirements, will shape a business culture that respects the personality of the customer-subject through consistent information and accountability, acquiring a competitive advantage in the future of a clean and healthy business-client relationship. Such a privilege will increase their turnover, with positive social consequences, due to the rising employment rates. On the contrary, businesses that will not comply with the GDPR, will have to confront not only unfavorable financial consequences, but also reputation issues, potentially harmful and devastating for their own existence.

Furthermore, the transparent relationships imposed by the GDPR will shape socially active subjects, citizens who follow their data, are interested, control, participate and contribute to the purpose for whom they had disposed them.

In any case, businesses will sooner or later have to adapt to the GDPR, or else they will not survive. However, the main question for the GDPR effectiveness is addressed to the citizens- subjects. Are they eager to 'board the vessel' which carries and leads their data into the vast internet sea? The big bet undoubtedly lies with the European citizen, after pressing the 'enter' key...

Big brother is not only watching you, but also using your data!

Privacy, who cares?!

Essay by: Jefke Daems

Category: Aspects of philosophical and societal impact

We all know that our online privacy is constantly being violated. Companies say they only collect data to analyse their clients behaviour and to improve their services. But in fact, information is also being collected for advertising purposes or government surveillance. Trending news items on Facebook are constantly being controlled and can be manipulated. News is supposed to be objective. Therefore, the violation is double; through the invasion of privacy and through censorship. Digital business-to-consumer communication has increased and is still growing.

A new era has started and everybody should be aware of the risks that come with an economy that is increasingly information-based and potentially adversely affects our lives. Sharing personal data should not necessarily be a problem, it depends on how these data are processed. Security is a major component of privacy. Therefore, major legislation has been issued to protect privacy. The General Data Protection Regulation (EU-GDPR) sets new rules[1] for companies on how to manage and share personal data. EU-GDPR is far stronger than existing rules, but will it be enough?

EU-GDPR has been adopted by the European Commission in 2016 and has to be implemented by all EU Member States by May 25, 2018. It addresses the protection of personal data of EU citizens, but in the future it will and must affect worldwide internet because of its global nature. The penalties are very strict. Fines are set at 4 percent of a company's global income or €20 million (whichever is higher).[2]

Consumers can, for example, request insight in all personal data a company has collected[3] (to verify!). Consumers also have the "right to erasure[4]" and the "right to data portability[5]". Companies will have to ask permission in order to be allowed to collect your and my data: click to proceed, but isn't that too easy? Mr. Mayer-Schönberger, professor of Internet Governance and Regulation at the Oxford Internet Institute, University of Oxford, says consumers are not trained in protecting their data. Clients are requested to give "consent" or "leave"

"Security is a major component of privacy."

the use of the device. They blindly accept all terms without checking them. That is why a law with give people even more responsibility does not ensure better data protection. Another reason people blindly accept the terms could be explained through two phenomena called: "the privacy paradox[6]" and "privacy fatigue[7]". The pleasure of using apps like Facebook serves as an incentive for people to ignore privacy concerns. Consumers also feel a loss of control with respect to the online management of personal data because of the frequent data breaches recently.[8] This matter is addressed in the book: Computers in Human Behaviour.[9]

In the future, the privacy of natural persons must be protected even more effectively. Companies have to carefully consider how they deal with analytics and advertising; more transparency is required. GDPR is nevertheless a good basic law!

1 The EU-GDPR exits of 99 articles and 173 Recitals.
2 Article 83 GDPR (General conditions for imposing administrative fines).
3 Among other: article 15 jo 46 EU-GDPR (also called "the right to Access").
4 Article 17 EU-GDPR (also called "the right to be forgotten").
5 Article 20 jo Recital 68 EU-GDPR.
6 Privacy paradox means: people state they are concerned about their privacy, but in fact continued use of online social networks.
7 Privacy fatigue means: consumers feeling a loss of control in managing online personal data and aren't concerned about their privacy any longer.
8 Article 33 jo 55 jo 34 EU-GDPR (also called "breach notification").
9 Written by: E. Mitchell Church, Ravi Thambusamy and Hamid Nemati.

Trade in your privacy for your 15 minutes of fame

Essay by: Cihan Deniz

Category: Aspects of philosophical and societal impact

The current day conundrum is the internet and how companies, tech giants and the internet media can use and abuse your data without your consent. The internet in its infancy seemed innocuous and everyone used handles or fake names. No one really cared whose face was behind hoola-hoopgirl45. Current day however, technology and identity is interwoven with each other. We share our basic and even our most intimate information under our real names.

Where Pyramus and Thisbe were to confess there love secretly between a crack in the walls, we now announce relationships and even engagements on publicly on social media. We want our 15 minutes of fame. We want the benefits of technology without thinking about the consequences of participating.

We don't read the 40-page long Terms of Service and accompanied Privacy Policy in which we clearly give permission that third parties are collecting and distributing our data. We don't care that companies are collecting our demographic details with ad-trackers, cookies and tracking-cookies. We just want to watch the umpteenth cat video or smash candy on our transits.

And consequently we act surprised, appalled and even outraged when it is revealed that major technology giants sell our data to the highest bidder. It is clear that it is our own fault we let it come this far. It is now hypocritical to demand more control over our personal data when we ourselves were willing to relinquish it so easily. We did not act responsibly in the first place.

So is privacy a hot topic in the Netherlands? Barely. In a last-ditch effort to save our privacy from government institutions, only half of the Dutch people cared enough to vote on the so-called "Sleepwet"-law in which the government assigns itself more power to circumvent privacy of its citizen for more security. Benjamin Franklin had an apt saying: "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."

The current status of privacy in China and Korea is much more interesting however. Policemen in China have special goggles that can instantly identify the person being viewed and for example if a civilian is walking through red lights, he or she is instantly notified for breaking the law and is issued a formal warning.

In Korea internet-anonymity does not exist and discriminatory and hateful messages are always linked back to the commenter and given proper punishment through official means. While these are extreme examples of surveillance, it highlights how far governments are willing to go to trade our non-existent privacy for perceived security.

"So is privacy a hot topic in the Netherlands? Barely."

We need to change our fundamental concept of privacy before we start a witch hunt on those who trade and deal in privacy.

Privacy? Who cares!

Essay by: Loïs Gampierakis

Category: Aspects of philosophical and societal impact

Protecting our privacy. That's what this new law is all about. But how private is life, anyway? Google a name and within minutes the results tell you all about the person behind it. You might even find an embarrassing prom-picture that was made not to be found.

The first time I heard about this referendum, my thoughts were pretty positive. I thought about the safety of our country, my family and about my own. I had no problem with the government being able to follow my every move. And why would this be a problem if you have nothing to hide?

But soon I realized my opinion wasn't as common as I thought it would be. Multiple friends, co-workers and fellow students did not share my point of view. As soon as I saw the news, I recognized that the majority of young adults didn't want to give up more privacy than they already did.

"I thought about the safety of our country, my family and about my own."

One fellow student tried to make me understand the importance of privacy. He told me that he felt like the government is trying to take his rights away. "First that donor-law", he mumbled slightly disturbed, "And now they want to take my privacy away?". He seemed affected by the conversation. It was pretty tough for me to understand that people feel this overpowered by the idea of having less privacy, especially because we live in an era where privacy is a very deceptive phenomenon in general.

In a time of individualization it might be a good idea for the government to keep a closer eye on us. It might be important for this society to think in a way of protecting us again instead of the egocentric thought of protecting **me**.

Knowledge Equals Power

Essay by: Henriët Graafland

Category: Aspects of philosophical and societal impact

What would I be able to find if I get access to your smartphone? Probably, a lot of information in chats, pictures and videos. All these data are potential targets of privacy violation. Still, we keep collecting, saving and sharing our lives on the internet. Companies as well as governments gratefully use our data to improve the promotion of their products or to guarantee our safety. Even academics relish in the thought of a complete database which they can analyse to prove their own right. This is not new at all. What then, has changed over time what makes privacy legislation a necessity?

Access to information was crucial for even the earliest forms of trade. The quantity of knowledge traders had, determined the negotiations with other traders and the resulting profit they could make. They gathered at important places where information was shared, called hubs. If not at least one member of the trading family was part of such a hub, there was a big chance of losing out on important information, which worsened the trading position of the family. The trick was not to share valuable knowledge with rivals, while traders obtained the best information for themselves.

Over the course of a very long time, the number of hubs grew and got better connected. In the famous coffeehouses of the eighteenth century, every novelty was discussed elaborately and radical ideas spread fast. But the state had become quite powerful, and not everyone dared put his name under controversial documents and statements, for this could have political consequences. There was still a great need of privacy.

This changed gradually after the French Revolution of 1789, when power was divided among three institutions and the private and public spheres got separated. This made sharing of radical information safer, because individuals were protected by freedom of speech and the state could no longer use all the information that was available.

Since communication and transport revolutionised in the nineteenth and twentieth centuries, the world has been connected even better and information can be shared very fast. On the other hand, because Europe has known a long time of freedom for individuals, the need for privacy has disappeared. We think that the division between the private and public spheres still protects us. Of course, we worry when we find out that our data is out on the street, but we argue that this is simply the consequence of globalisation.

However, in this globalised world, knowledge equals power more than ever. Interests of individuals and organisations still oppose each other, while the division between private and public knowledge is not clear anymore. In our urge to collect all information, we have forgotten the value of privacy. That is why we need privacy legislation: to draw a line between what may be out on the streets and what is best is to keep a secret.

“In our urge to collect all information, we have forgotten the value of privacy.”

Short bibliography

Arianne Baggerman and Rudolf Dekker, De wondere wereld van Otto van Eck: **een cultuurgeschiedenis van de Bataafse Revolutie** (Amsterdam: Uitgeverij Bert Bakker, 2009), 397- 403.

John Barrell, “Coffee-House Politicians”, **Journal of British Studies** 43 (2004), 210-217 and 222-227.

T.C.W. Blanning, **The Culture of Power and the Power of Culture: Old Regime** 1660-1789 (Oxford: Oxford University Press, 2002), 2-13.

Andrea Colli, **Dynamics of International Business: Comparative Perspectives of Firms, Markets and Entrepreneurship** (London: Routledge, 2016), 34-35.

Joost Kloek and Wijnand Mijnhardt, 1800: **Blauwdrukken voor een samenleving** (Den Haag: SDU Uitgevers, 2001), 62-63.

John McKay et al., **A History of Western Society. Since 1300**, 11th ed. (Boston: Bedford/St. Martin’s, 2014), 526-527.

William Outhwaite, ‘Jürgen Habermas’, in **Key Sociological Thinkers**, ed. Rob Stones, 2nd ed. (Hampshire: Palgrave Macmillan, 2008), 253-254.

Essay GDPR

Essay by: Nico Heidari Tari

Category: Aspects of philosophical and societal impact

Human beings are extraordinarily creative creatures, and every few years (or perhaps days?) we come up with novel ways to earn money. One man's trash is indeed another man's treasure, as in today's circular economy even rubbish must be recycled back into the system in an intricate feedback loop. 50 years ago, it was unimaginable to consider the following could earn money: the clicking of a button on a computer mouse.

Of course, pragmatic issues inhibited these individuals to generate such imaginative cognizations, the computer mouse was still being invented! But today, we know that the buttons we click in our private homes, can send cartoonish dollar signs into the eyes of the economic data-bourgeoisie that feed off our data, as a sort of weird drooling leech.

But dear reader, please do not interpret my whimsical metaphors as indicating a negative tone. On the contrary, I could not be more positive about this situation. This type of development elucidates the human ingenuity to prosper with goods that were hitherto deemed useless! However, we have bitten off more than we can chew, and have hence arrived in somewhat of a pickle. The data corporations have become so high-tech and intricate that they are able to cause serious harm to our human dignity. What should we do? Should we all enter into an "into-the-wild" project, where we say goodbye to our technological gizmos, and return to a more simple life, far away from the dangers of neo-capitalism?

"So they can be violated without the perpetrator even being aware that the law is broken!"

I say no! The potentiality of technology to improve our lives is far too valuable to leave behind. But that does not mean we can just sit back and watch idly by how the capitalistic super-monster strips down our basic rights to privacy and transmogrifies it into commercial gains. The GDPR is a splendid way to counteract the wishes of this dreadful ogre, but I must emphasize that it is not enough. This law provides many positive innovations, e.g.: better sanctions for lawbreakers, and better rights for erasure of data. But the problem with laws is that they can be broken. Another problem with laws is that often they are open to interpretation, so they can be violated without the perpetrator even being aware that the law is broken!

What we need right now is awareness. The same awareness that enlightenment philosophers wanted to share with all of their contemporaries to bring power back to the people. And it should not be only the wealthy aristocrats that have the knowledge to manage their data. Everyone should have media literacy to a certain extent. So, dear university students, go out into the world and discuss. Discuss these issues with everyone! With your parents, your siblings and your dog. Even with your friends who do not follow the news. This is what the famous philosopher Habermas would have wanted, everyone engaging in rational debates on contemporary issues, thereby contributing to a healthy public sphere! Only in this manner, can we escape the nuisances of postmodern neo-capitalism.

Privacy? Who shares?

Essay by: Leon Hoeneveld

Category: Aspects of philosophical and societal impact

A philosophical issue might be the distinction between caring and sharing.

The issue can be made cristal clear with the following consideration:

What you share is not private.

If you care about privacy, the logical standpoint would be not to share anything. A society without sharing, for instance sharing culture, f.i. rules and regulations, would be no social structure.

The liberal standpoint would logically be: anything that needs to be shared is obstructing freedom. The personal freedom of a person is liberating yourself from the need to share. In which case social structures should be considered prisons.

A liberal point of view on privacy would be to get rid of social structures. Social structures, with it's sharing, being the publicality of a person.

This consequential view on a liberal point of view is to be considered extreme and faulty, a kind of straw dog. But as a thought experiment it clearly shows the distinction between caring and sharing, from a perspective on privacy.

Caring could be caring for the things we share, and can share. The environment should be safe for us to share a wide range of opinions and activities. If the need for privacy obstructs people in what they can share, a paradox occurs. Sharing would be giving up freedom. When sharing means giving up freedom, society fails in it's prime directive, being a public place.

The analysis of the privacy issue, showing a paradox of freedom, asks for a different approach on what privacy could mean to be. Privacy could mean to be protection of the possibility to share, and not removing information from the public space. Privacy could mean to be a kind of insurrance that shared information would not result in any bad consequence. An insurrance that the information value of shared data is a kind of holy. That any misuse of the information would be punishable.

The question that remains, with this conclusion, is what "misuse" of information would be. If information would be that an illegal deed had been done, or a criminal fact was commited, would calling a person to it's repsonabillity be "misuse"? What if a person would lose it's job after sharing excesive alcohol or drug use?

The responsabillity of a person, as part of a social contract, is something that needs attention, but is a private matter. Society should care for an insurrance against misuse of shared information, without restriction for sharing.

A commercial company would have the situation of not thinking about a pink elephant, when someone shares a pink elephant. The company tries to get people to give up their rights on privacy, if this is an option. And there might not be a user account while the company still has user information.

"A liberal point of view on privacy would be to get rid of social structures."

Protection against "misuse" could be something as abstract as restricting the quantity of advertisements. This might be better than forbidding advertisements on conditions.

Do you want to live forever?

Essay by: Marenne Hoogenboom

Category: Aspects of philosophical and societal impact

According to the EU, the GDPR is designed to – amongst others – protect and empower all EU citizens' data privacy. This privacy concerns personal data, referring to any information relating to an identified or identifiable natural person. Interestingly, you are only considered a natural person from birth to death. So what happens with your data after that?

In The Netherlands, when a person dies, the government automatically informs all public institutions. The private sector, however, remains uninformed. That implies that your data does not die with you. Even though eternal fame might sound appealing, do you really want to live forever?

Privacy can be an intangible concept. Even more so, privacy after death might be hard to grasp. However, in other situations this right for privacy is already protected after passing away, with good arguments. For instance, the oath of secrecy of your doctor remains valid – unless there are compelling circumstances. Why is that so essential? Imagine that one of your parents has a genetic disease. Would you like this information to be available to your health insurance? The same holds for other professions that carry similar responsibilities.

"The oath of secrecy of your doctor remains valid."

So why is continued privacy so important? Most importantly, in my opinion, data that is still out there can pop up unexpectedly. Imagine a five-year membership anniversary letter that arrives at your relatives long after you are gone. They are, again, confronted with their loss. Or think about special offers that are sent to you because some time ago you requested information about adding some additional, perhaps provocative, TV channels to your subscription. Aside from taking your relatives off guard, it might affect their perception of you or sparkle questions in a situation where you are no longer there to explain them the details.

When you are not around anymore you cannot exercise the rights given by GDPR, including the right to both access and delete all of your data, known as "the right to be forgotten". This implies that you cannot control what data is erased and what is not, thereby running the risk of living on forever.

To mitigate this shortcoming, the company Closure was founded. As a centralized party for the private sector, it unburdens relatives by ending all subscriptions, contracts and (social media) accounts after the loss of a beloved one. Not only does this save relatives time and money, it also gives control to those you leave behind. Providing them this comfort, will allow you to truly rest in peace.

To conclude, real protection of your data – claimed to be a goal of GDPR – can only be achieved when privacy remains intact, both during and after your life as a natural person. Since GDPR is not supporting this (yet), entrepreneurs are taking matters into their own hands. Because, as Queen already said, who wants to live forever?

Privacy? Who cares!

Essay by: Melani Kaitalidi

Category: Aspects of philosophical and societal impact

Living in the age where information is going around as fast as the river flow, people are becoming more concerned about their privacy. Internet and media, shared communication and transparency, the existence of this "cloud" where all the information is stored. The fact that different agencies and organizations can find a large amount of information about people without directly involving them, sometimes without them even being aware of it. What about privacy?

The answer is that all that information is taken from somewhere and it had to be put there by someone in the first place, one way or the other, which is a free decision made by that "someone". Therefore, is it really a violation of privacy, if the information that has been exposed by the people themselves is put on the internet and then used?

There are many ways of recruiting and using the information found on social media. We are always being told that what we post, for example on facebook, will stay there or somewhere even if we decide to delete it. In times of people being so involved in media, their image and self-representation through internet, they have to take into account that the audience of that vast virtual space is unlimited. If in the first place you decide to open up the facts that were chosen to convey through media, it is freely taking a risk about where this information could end up.

The frustration over privacy and its invasion can be understood, as people always want to control what they own, such as the information about them, but is it really still theirs when they decide to share it? It is debatable, such as the question of transparency. It seems that privacy that people want to hold on to is not that much about them wishing to keep that information, but it is more of how it can be used. The governments in many cases do not seem to be transparent enough for people to trust them with providing their full information. This inability to trust because of the lack of transparency therefore makes people fear their own transparency. As for so many years people fought for their rights, where privacy and control over it falls under this category.

"As for so many years people fought for their rights."

Privacy is protection, therefore are people afraid since they hold on to it? It is in itself a simple concept. If we think about it, what would our world look like if all of us gave up our privacy, including every single individual. Maybe in this case there would be more acceptance, maybe that would simply create more freedom, or would it do the opposite? Overall, it is what people define as privacy, what it means to them. The question still remains the same, is it really an invasion of privacy if information is extracted out of the sources people have provided to the public themselves? Maybe it is about our own choices.

Unintended collisions

when inner dialogues turn into data.

Essay by: Laurens Kolks

Category: Aspects of philosophical and societal impact

In an era featuring an unprecedented range of options to express one's inner thoughts, the notorious trial of Dutch nurse Lucia de Berk – receiving broad media coverage during the early 2000s – still has scientific relevance. This essay focuses on its particular significance for the phenomenon of privacy, or more specifically: the protection of inner dialogue as private matter.

In four consecutive cases Lucia de Berk was convicted for multiple murder and attempted murder of patients in hospitals where she had worked, initially receiving both a life sentence and compulsory psychiatric treatment. After spending more than six years in prison, her case was reopened, and due to newly discovered exculpatory evidence De Berk was released from jail. Two years later the former nurse was exonerated of all charges, making her trial one of the most severe miscarriages of justice in recent Dutch history.

"Arguably the most intimate of conversations."

Lucia de Berk's case had been controversial from the outset because of the prosecution's fragile construction of indirect evidence: an amalgam of debatable interpretations of medical data, conclusions derived from statistics (!), and personal writings such as excerpts from Lucia's diary, which will be our main concern here. As it turned out, police investigations into her personal life had 'revealed' that De Berk was a productive diarist, who allegedly liked reading Tarot cards and Stephen King novels.

Amongst the many words and sentences that Lucia confided to her diary were a certain amount of ambiguous phrases such as: 'a great secret' and 'admitted to my compulsion'. These phrases' particular choice of words – and more importantly: the omission of words that would have rendered them less enigmatic – turned out to be very unfortunate, as the prosecution interpreted them as evidence confirming their multiple murder narrative.

Lucia's personal writings suddenly became suspect: her inner thoughts – whether fact or fiction – that had materialized into texts, were now considered to be valuable data. When Lucia's daughter was asked to explain why her mother had written these cryptic manuscripts, her answer was deceivingly simple: Lucia's diary was never meant to be read by anyone but herself.

De Berk apparently kept her diary for a reason that many others do: to correspond with the self. In this distinctively private type of correspondence – in which sender and addressee are one and the same – communications can be quite indirect and still transfer 'clear' meaning. Moreover, in this particular type of correspondence, 'storing' inner dialogue in written text can serve many purposes: the exploration of fantasies being one of them.

When expressed inner dialogues are viewed upon as data, something crucial happens: they instantly gain in credibility and turn into raw material for interpretation. The conversation with the self is pulled towards a force that renders both its content and participants defenseless: the assumption that all expressed considerations are possibly connected to the author's behavior in the physical world. Through privacy, the inner dialogue – arguably the most intimate of conversations – is protected from that, against which it cannot defend itself: an unintended collision with reality.

Philosophical Aspects and Societal Impact of GDPR

Essay by: Jakub Kucharski

Category: Aspects of philosophical and societal impact

The General Data Protection Regulation (GDPR) was approved in 2016 by European authorities and becomes enforceable on 25 May 2018. Its scope entails providing EU citizens with greater control over how both domestic and foreign companies process and use their personal data. One of the main objectives is the clarification of consent, making it easier for consumers to both understand the conditions and be able to withdraw their personal data at any time.

A major positive consequence of the GDPR for consumers is increasing the importance of their autonomy, defined here as full awareness and commitment to a decision regarding data privacy. Under the new regulation, bundling consent terms is outlawed, requiring organizations to break down their conditions. Each separate field requiring consent for processing private data will now have to be approved by the consumers individually. This should increase their understanding and accountability for the conscious decision of providing consent.

In practice, GDPR will shift the focus from freedom of choice to autonomy of consumers. Until now, consumers were usually presented with broad, often-times difficult to interpret statements regarding the handling of their personal data. The regulation will promote the consumer's understanding of information processing and usage, but perhaps more importantly, will give them the right to fully withdraw at any given time with the guarantee of complete erasing of their data.

Combined with the new obligation for companies to notify authorities of a security threat within 72 hours and their customers without delay, the GDPR should result in a new behavioural trend in society. Not only will the consumers be better informed and aware of how their information is being used, they will also become more aware of hazards concerning their privacy. Should such a threat be discovered, we could witness continent-wide withdrawals of personal data from the affected provider.

This perspective should trigger a cumulated effort of companies to pay more attention to the privacy of their users. Recent scandals, such as Facebook's connection with Cambridge Analytica, show that even the biggest players in the industry have historically disregarded the importance of safe-keeping their customer's data safe. At the same time, they reveal that customers were often unaware of how their personal information was being used, despite having free choice of consent, their ultimate decision was not fully autonomous.

"Freedom of choice will be combined with understanding, as well as fully and truthfully informed consent."

As the lack of customers and mass panic caused by personal data mishandling could prove disastrous to providers, we might be about to witness a major shift in the philosophy of the industry. Companies will have to focus on becoming 'data-banks' rather than processors, the safekeeping of privacy should become the number one priority, perhaps even over outright profitability. GDPR essentially liberates the consumers and gives them the ability to make or break an organization handling private data.

GDPR, therefore, will have a major role in shifting the power towards consumers in the world of big data. Their autonomy will become dominant, freedom of choice will be combined with understanding, as well as fully and truthfully informed consent.

Privacy? Who cares!

Essay by: Anja Lauter

Category: Aspects of philosophical and societal impact

The issue of personal data protection is most certainly growing in the digital age when more and more people actively participate in the online world. However, when asked about the extent to which the own personal data is somewhere in the depths of the internet, many remain clueless. Many tend to accept cookies on website within the blink of an eye, not knowing or, even further, not caring that not only general data such as names can be saved but whole activity profiles are created.

Those activity profiles are analyzed and sold to third parties which use them to custom-tailor advertisement based on your preferences. When it comes to the seemingly endless opportunities and pages the internet has to offer, one may forget about the saying 'nothing in life comes free' but we are so used to linking the concept of paying to the concept of money that it is often overlooked that the currency of the future is considered to be data and information. Namely, YOUR data and information.

"This is the boundary which will turn us into glassy citizens."

Of course, even if you are aware of this deal that happens in the background, you may think that sharing your data is not a high cost for you compared to the services of millions of free websites and you might even find interesting offers among the customized advertisements. Maybe you firmly believe that you have nothing to hide and that your data is not very valuable, that it does not make a difference when you browse on Amazon and Facebook instantly changes its ads according to the products you just browsed. Let's take this a step further. To a step where your personal data does not only consist of browsing activities but also some data from online medical registries for example. The more delicate the data becomes, the more important it becomes all of a sudden who has access to your data. This is the boundary which will turn us into glassy citizens. Maybe we do not mind potential employers to know about our search for the latest summer shoes but how about sensitive data in regard to our recent treatment of a STD?

Most likely multi-level policies and strict enforcement will help to protect citizens' data from being shared beyond permission of the owner. However, there are two main factors that work against the formulation of such measures. Firstly, the societal division which separates the so-called 'digital natives' which refers to everybody growing up actively using the internet, and those who have experienced the phenomenon of the internet in their adult years. Unfortunately, most politicians belong to the latter category and have less expertise on the subject than younger generations. And secondly, the most important factor against effective data protection is the outsized willingness of the majority of people to feed the internet their personal information thus making their protection almost impossible. It seems that people who 'have nothing to hide' yet have a lot to lose.

Potlatch and Privacy

Essay by: Sietse Leeflang

Category: Aspects of philosophical and societal impact

In the contemporary ''Western'' tribe the potlatch lives like never before. It only manifests itself through the private into the public sphere. Lets elaborate a bit further on this.

What did I understand with privacy? Privacy is the covering sphere, the sphere which stands opposed to the public sphere. Opposed to, because the public sphere is a sphere where you cover the things you don't want others, who are not themselves in your private circle, to know. What is covered depends wholly on time and place. But mostly the covered subjects are such which carry a taboo value in them.

What might be taboo depends, as with what is private, on who you ask. So in a society that appraises material wealth there might also be a taboo on how much salary someone earns and thus one's salary is something private. Or a different example: culture where the body is a sexualized and objectified, there can also exist a taboo on showing naked bodies in public space, and nudity is restricted to the private sphere. It might be clear that private is this what one keeps from the public sphere because its objects have potential status within the concerning community.

This was for a long time the prevailing dichotomy: the private opposed to the public. But a contemporary phenomenon, the internet, could be seen as a dialectical outcome of the two. Internet is many things at once and one of these things is a way to communicate; thus it also forms a community. This community begins in the private and opens up to the public. Therefore internet is something which allows one to stand both in the private and the public sphere at the same time. This brings new ways in relating with each other, new ways to think about the other. Because the other who was once outside in the public can now enter the more private and vice versa. One way to think about this new relationship of public/private sphere is the potlatch.

The Potlatch in history is a offering ritual from tribal America where different native communities compete in offering the most of their belongings by destroying them. It's a status ritual with a cleansing effect to restore the ownership balance within the community. After the offering the tribe members have to start again from scratch. In a contemporary society where everything is about utility, ownership and status, the destruction of belonging seems senseless, but the potlatch ritual could be said to be found in the way contemporary women and men are willing to give up parts of their privacy online in order to showcase their wealth and status. Considering privacy as people's inner bouncer who decides what gets to be shown to the online community and what stays in the sphere of the taboo.

"What is covered depends wholly on time and place."

The potlatch is the status ritual where people show the other tribal members in the online community how much destruction they can do - on a constant holiday, bacchanalian dinners in new sweatshopped clothes. In rigorous hedonism today's rabble can show their status by a constant sacrificing consumerism. This sacrifice can be called flaunting or fundraising. The problem with this present day potlatch ritual is that cleansing effect and by that the equalizing of the tribe not goes to the whole tribe but only to a certain few. This emphasizes the status and taboo surrounding consumerism and its objects even more. With an effect in the long term, that some have to show off even more while others can only live in awe of this ritual. So the question I like to raise now is: How much more privacy the tribe is going to sacrifice to display the cul-de-sac it is on?

Can privacy ever be protected?

Essay by: Nelly Matar

Category: Aspects of philosophical and societal impact

One of the most important warnings in 1984 is that the past can be erased and history can be changed. **"Who controls the past, controls the future; who controls the present controls the past"** (Orwell 1949). The lack of privacy in modern society has led us to question the "who" of the world foreshadowed by Orwell (1949). Tech giants like Facebook, Google and Twitter have taken on the role and instilled a once far-fetched dystopia into a real "Big Brother" of the 21st century.

Philosophically, what actually defines privacy and how has a lack of it always been a villain in the tale? Naturally as humans we are social animals with a need to know (McLeod 2018). The need to know about our work, our environment, but most significantly the need to know about the lives of people around us no matter if they have an impact on us or not. Lack of privacy has always existed however, clearly the evolution of technology has propelled the extent to which we are comfortable with our innate nature and the presence of Big Brother.

"This will cost them time but will it cost them a loss of users?"

On May 25th the EU takes a stand of modern heroism against the "antagonists" of privacy attacks by implementing the General Data Protection Regulation (GDPR) (Solon 2018). The measures protect citizens of the EU and hold companies liable for acts against privacy. The extent to which this will eliminate privacy invasion is questionable due to our innate nature however explicitly it may give a sense of freedom to the people of EU.

As citizens, the regulations will allow private data to rightfully be their own if wished to remain so. The power of Big Brother suddenly shifts from the hands of companies to the public. Whether this change is for the better depends on which eyes you view society with.

Companies will be impacted negatively as they are the ones who have been watching. Policies must be re-written and customers must be informed. This will cost them time but will it cost them a loss of users? Social media enables people to connect, to engage in their social nature on a macro-scale. Humans may not be willing to give this up despite their concern for protection. Thus, the GDPR allows them to freely continue using medium for connection, to see what goes on in peoples lives. But is this not a breach of privacy in itself, to see where someone is having lunch, what one is listening to.

It clearly boils down to the question of whether privacy can ever be protected but what can be said is that the GDPR explicitly gives a sense of reassurance which settles the uproar in modern society. It aims to shift the who in Orwell's 1984, to the citizens and seemingly it is a good thing but in the long run, one cannot know whether this era of Big Brother will be better, it is up to us as users to ensure this.

Bibliography

McLeod, S. (2018). **Social Identity Theory | Simply Psychology.** [online] Simplypsychology.org. Available at: https://www.simplypsychology.org/social-identity-theory.html [Accessed 10 May 2018].

Orwell, G. (1949). **1984**. 2nd ed. London: Harvill Secker.

Solon, O. (2018). **How Europe's 'breakthrough' privacy law takes on Facebook and Google.** [online] the Guardian. Available at: https://www.theguardian.com/technology/2018/apr/19/gdpr-facebook-google-amazon-data-privacy-regulation [Accessed 10 May 2018].

The philosophy of personal data

Essay by: David Pacuk

Category: Aspects of philosophical and societal impact

There is a centuries old saying that, despite its antiquity, keeps proving to have lost none of its value in the modern age: **knowledge is power**.
As a sociologist, I can't help but refer to Foucault here. In developing the analogism of **power-knowledge**, Foucault assented to the idea that power makes use of knowledge and knowledge is shaped by power. If we look at the contemporary nation state, we can see how essential information is in exercising control over people.

Take for example the recent controversy surrounding the **sleepwet**; here it was constantly emphasized how indispensible this law supposedly was for the preservation of security – though at the cost of privacy.

In regards to such matters of state surveillance, many draw comparisons with Orwell's 1984. Largely a just comparison, I would argue. Aren't we continually observed in most of what we do, after all? Isn't data constantly gathered? And like Foucault, as inspired by Bentham's **panopticon**, discussed: doesn't that mean that we are being disciplined on all sides? I'd say that these arguments ring with truth, but that we need to go a step further: beyond discipline. Because we're not just dealing with the authoritarian character of surveillance, but also with the ways in which we identify ourselves as people.

Consequently, we need to be aware of the flipside of this story: power also shapes knowledge. Nowadays we find ourselves in a situation where we constantly identify ourselves; if not voluntarily through social media, then for example by check-in for the train – and such processes even transpire without us being aware through the gathering of so-called **big data**. As follows, many of the freedoms that we have gained, like the luxury of mass communication through the Internet or the ability to travel by train with the mere swipe of a card, are also part of systems in which our identity is constantly monitored. In that regard the famous statement by McLuhann once again seems almost prophetic. **The medium is the message**. Who we are as people is defined – or, profiled – through the media that we use in our daily lives.

"Power also shapes knowledge."

So what do I think of the GDPR? From my perspective, it's a minimal step in the right direction. That is, it provides the necessary toolset to protect citizens' right to privacy in this day and age. How this will work out in practice depends on how jurisprudence develops and how organizations and institutions react to the legislation. However, what is most crucial as far as I'm concerned is that people become aware of the status quo and willing to confront it. Of course it's important that problems are resolved and prevented within the present context, but beyond that lies a major public issue concerning the systems that we depend on and the values that we design them around. Most of all I would thus like to see everyone become critically aware of and outspoken about the fundaments of our daily enterprise. **Mind your data!**

No man is an island. No man stands alone.

Essay by: Arthur Petit

Category: Aspects of philosophical and societal impact

Behind John Donne's prose hides a biological truth. Homo Sapiens is indeed a social mammal, whose chances of survival rose when living in groups. What led humankind to evolve is the increasing complexity of those societies; from the hunters and gatherers of the first men, to the specialization of later civilization into labour division.

But what drove this evolution? Bluntly, it can be reduced to **information sharing**. Prehistoric men shared hunting spots, edible berries, and whatever would better benefit their community. Trough the invention of writing, a couple thousand years before our era, and later on of printing, around the mid-15th century, information spread faster than ever, to a limited yet increasing group, larger than ever before in History. This undoubtedly peaked at the Renaissance, where arts & sciences blossomed in unprecedented breakthroughs.

"Think of how many 'terms and conditions' you accepted without reading them."

Fast-forward to the 21st century. The exponential technological evolution led to humanity's greatest information sharing tool - the mighty Internet. Yet this same invention also opened a box of Pandora, with countless new risks, and in particular, the rise of profit-driven, unethical commerce. In particular, businesses with large resources were quick to realize that knowing more about your customer allows for more accurate segmentation, and in return, higher conversions. In that regard, companies were numerous to use methods, which could be qualified as cunning if they were not so crooked. Think of how many 'terms and conditions' you accepted without reading them.

Now, one might object that these companies are free to operate however they want, just as consumers are free to refuse those services. But what is revolting is the underlying assumption these companies make –aka the monetization of user data. In our society, data generation is a pre-requisite. From womb to tomb, we are assigned names, dates of birth, medical information, bank details, and more recently, social media accounts and related posts, IP addresses.

These informations are crucial for companies to better understand their consumers, and ultimately, sell the product solving their needs at the right time. Google, to name the titan of this industry, has for example persuaded people of handing in their data, in exchange for free emails -Gmail. Of course, this data is then sold for billions.

This kind of scam will one day appear as scandalous as the buying of Manhattan island from Native Americans for 24$ worth of beads. But even worse, some data is taken from users without their consent. In this case, it almost seems like a digital slavery, with one's data being mercilessly and unwillingly exploited.

In our modern world, the question "Who owns my data" will determine who possesses wealth, and ultimately power. The GDPR will not perfectly shield citizens from data abuse, but it has the merit of pioneering into the neglected field of data privacy regulation. One can only hope it will get people to think critically, and determine which kind of data could be –or has been- used against them.

Privacy and the autonomous subject

Essay by: Andrea Pogliano

Category: Aspects of philosophical and societal impact

Imagine living in a house with a big telescreen that records all your actions. Imagine, on the other side of the screen, a Thought Police, constantly checking upon you. How would you feel? George Orwell tried to answer this question in his novel 1984, where he depicted a dystopic world in which everything is under the rigid control of the 'Big Brother'. In such a scenario, people lose any form of privacy, they are violated even in their inner thoughts. One of Orwell's goals was to criticize totalitarian regimes, which destroy any form of privacy. Orwell in this way wanted to underline the importance of the value of privacy as fundamental part of a human being.

This conception of privacy as one of the rights of thinking beings emerged during the Enlightenment, when many philosophers reflected about the intertwining of property and privacy. Property was seen as the most concrete kind of privacy, the right to protect one's endowments from the others (Locke).

Privacy then assumed a broader meaning, coming to indicate everything that pertains to the private sphere. People may want to shield their goods as well as information about themselves, they need the freedom to decide what to reveal and what to conceal. Moreover, they want to decide who can access such personal information as they are something strictly intimal.

All these notions are rooted around the concept of individual subject: the Enlightenment created the idea of a rational thinking being, that is independent and finally in control of himself. This called for measures to protect such independence and thus privacy was born, in this sense privacy can also be considered a product of Enlightenment.

The new-born concept of privacy found application in many documents of the late 18th century, from the Declaration of the Rights of Man of 1789 ("Since property is an inviolable and sacred right, no one shall be deprived") to the American Bill of Rights of 1791 ("The right of the people to be secure in their persons, houses, papers, and effects, ..., shall not be violated"). Since then, privacy was defended and regarded as a necessary condition in the life of men, this view surviving in the 19th and 20th centuries.

In the 21st century a new approach to privacy is developing. Advances in technology, in the form of internet and social network, enhanced the reachability of knowledge but at the same time menaced the concept of privacy as previously intended. On one side people can choose to have more information, they are free to obtain more knowledge.

"On one side people can choose to have more information, they are free to obtain more knowledge."

On the other they are limited in their own freedom and autonomy since they have lost the full control over their own information. The concept of privacy has therefore undergone a change and the philosophical challenge is now to find the right trade-off and balance between public and private.

Bibliography

Orwell, G. (1984). 1984. San Diego: Harcourt Brace Jovanovich.

U.S. Const. art. IV.

The Declaration of the rights of Man and the Citizen. art.17.

A Paradigm Shift for Sovereignty on Today's High Seas.

On the European General Data Protection Regulation (GDPR) and Digital Identity.

Essay by: Gilliam San De Vos

Category: Aspects of philosophical and societal impact

In the year 1603, Captain Jacob van Hemskerk, an employee of the VOC, attacked the Portugal merchant vessel the Santa Clara, acting on what seemed to be his own volition. The merchant loot was subsequently return to company shareholders.

The controversial incident which took place during a tense warring period between the two countries set in motion a protracted legal battle as Portugal sued for return of its goods; a religious faction of the VOC rejected the plunder based on how it was acquired; and the existing Dutch legal system had no provision for the act.

Consequently, the VOC consulted the then 20 year old political theorist, Hugo Grotius, to devise a justification for the event. Realising that there was in fact no legal antecedent, Grotius was forced turn to philosophical first principles and reasons. What ensued were a series of0argumentation underpinning what has eventually come to be known as the theory of international law, with its conception of the "high seas" tenet (**Mare Liberum**) that posits the independence of the seas from sovereign power.

"Like the high seas of the past, the internet serves as an infrastructure with boundaries that flow between diverse and often contested jurisdictions."

We currently live in a world today which shares many parallels to the early modern period. Growing sovereign imperialism has shrunken our cartography as rapid technological innovations have since continued to facilitate the movement of information, goods and people. Like the high seas of the past, the internet serves as an infrastructure with boundaries that flow between diverse and often contested jurisdictions.

As acknowledged by Christopher Allen, a technologist at the forefront of internet digital self-sovereign identity, web based applications nowadays are the nation states whose jurisdiction are projected throughout its borders. Evident with the case of these nation states throughout history, as these applications grow, its boundaries continue to ever expand encroaching upon freedoms of internet users. Data subjects are forced to accept legal terms of service when using these web applications which in fact grant very few "rights". Internet applications are far from democratic political systems, with powers that extend beyond even nation states. Subject identity and the rights to free expression are of at the mercy of these web applications.

We have since come a long way as legal limitations to the powers of national states have been founded. Certain universal and inalienable rights have since been established in each and every human being; we have moved away from nation states with absolute powers. These rights are now to be extended to the digital realm. With the introduction of the **European General Data Protection Regulation (GDPR)**, the first steps are being taken. Sharing many principles articulated in an influential 2016 essay by Allen, the GDPR can be considered a sort of "Digital Bill of Rights". However, we must recognise that such regulations have limitations by design and serves only as a small step toward the ultimate goal of digital self-sovereignty.

Relying on simply **goodwill** and trust of data controller and processors, the GDRP mandates the "data protection by design and default" which is certainly a challenging task from a regulator's perspective. What should not be taken for granted are the centralised models of digital storage and transmission which are now in the process of being replaced by distributed ledger technologies, namely **blockchains**.

A Brief Anagnorisis in the Times of Zuckerberg

Essay by: Clement Taffin

Category: Aspects of philosophical and societal impact

"Gonna pose in front of my laptop camera as I have my mental breakdown so my assigned FBI agent sees it." Funny memes like these, scattered all over the internet (specifically Facebook, and for those who blog, Tumblr) saturate my every day timeline. But this privacy concern isn't new – is it?

You could arguably say we've been worried about our privacy since we started thinking about those little cameras we're surrounded by. Minuscule laptop ones, front-facing ones on our smartphones, even surveillance cameras sometimes concern us. Except when they don't. Sometimes we get so used to certain things they become part of the everyday, embedded into the fabric of our routine, as if the omniscient eye of the surveillance lens was never a cause for pausing and worrying in the first place.

Society seems to work this way. A bit on the hypocritical edge, we call out those who invade our cherished privacy, but turn the script around a few times and we consume these invasions just the same – think about following tabloids or reading stories on your "discover" section of Snapchat.

Where do you think the celebrity gossip stories and their paradoxically private lives come from? It doesn't seem to matter much what happened to their personal information; it was packaged and sold for consumption the second you tapped into the screen. Same goes for Facebook – Zuckerberg memes filled the platform itself, calling him a lizard and an alien who feeds on human information... while you tag your friends and laugh at these jokes displayed on the condemned source itself.

I'm not one to be a complete pessimist, I like to think of the glass as half-full. But I've also come to realize we're all very keen on giving up our location services to our social media apps and essentially **need these settings** if we're lost in a city we don't know and need to access Google Maps. I guess it's become more of a compromise rather than an unfair battle: we agree to give up our privacy because we need services in return.

"This privacy concern isn't new – is it?"

Whether it's tapping onto the screen to look at the latest Kardashian feud (don't tell me you don't have some sort of pseudo fascination with this Klan) or memes about Zuckerberg in Zuckerberg's information goldmine, the way we think of privacy has essentially been the same since those conspiracy theories about people peeking through your laptop camera surfaced.

Truth be told, people are society and society is composed of people – becoming literate in your privacy rights, learning what your priorities are, and raising concerns in your community is something a lot of us believe we simply don't have the time for.

So what happens next? We try to compromise. Or we connect every single social media application because it's easier to log in once than to separately remember each account detail. We carry one email with no back-ups. We try to not rely on the Cloud, but our phones have limited storage. We go on our browsers and consent to cookies because we need the information these websites might give us. What is the societal impact of protecting our privacy? Realizing that we have any privacy left to begin with.

Privacy? Who cares!

The philosophical aspects and societal impact of the GDPR

Essay by: Jay van der Vlist

Category: Aspects of philosophical and societal impact

Privacy is important, not only for individuals but also for the democratic values of a society as a whole. Privacy is easily taken for granted and the real value of it often only becomes palpable when one is deprived of it. Recent examples of the fragility of privacy include Facebook's Cambridge Analytica scandal, the teenage girls whose private pictures are being 'exposed' in instant messaging chats and the oppressed and enjailed journalists and scholars in Turkey.

Although few would disagree with the fact that privacy is indispensable, many people often fail to act with the utmost deliberation and care with respect to their own privacy.

Partly due to the increasing digitization with its long and vague terms and conditions, it is has also become more difficult to keep track of which information one shares and who they share it with. Privacy debates have grown to be so complex that some people decide to conclude that privacy is of no concern to them, not seldomly without adding that they personally have nothing to hide.

"The lack of solidarity, the loss of public life and the isolation of the individual that came with it."

NSA whistleblower Edward Snowden once made the following analogy with respect to such reasoning: "When you say I don't care about the right to privacy because I have nothing to hide, that is no different than saying I don't care about freedom of speech because I have nothing to say or freedom of the press because I have nothing to write"[1]. Even if someone has nothing to hide or say, they should still protect the right to privacy as the merits that stem from it are of pivotal importance to the workings of a healthy democracy.

It is essentially a matter of solidarity. Privacy is not only for whistleblowers or threatened journalists. For instance, solidarity with respect to the right of privacy also enables people with a medical condition to insure themselves or criminal offenders to rehabilitate into society. In her acclaimed book The Origins of Totalitarianism, Hannah Arendt names the eradication of solidarity as a sine qua non for totalitarianism. According to Arendt, the lack of solidarity, the loss of public life and the isolation of the individual that came with it, paved the way for the Nazi and Soviet regimes. Hence, it is not very remarkable that there currently is a resurgence in the popularity of Arendt's ideas.

On the one hand, things that used to happen publicly (e.g. shopping, eating, socializing) are increasingly being replaced with online solutions and, on the other hand, far-right politics are gaining ground in many places in the world. The people who claim they have nothing to lose when it comes to privacy, are mistaken. It is fundamental to the workings of a solidary and democratic society. Similar to the outcome of the recent 'sleepwet' referendum, the General Data Protection Regulation aims to safeguard what many people consider to be their most valuable possession: their right to a private life.

1 https://www.theguardian.com/us-news/2015/may/22/edward-snowden-nsa-reform

Between Kafka and Orwell.

A critique on the focus of the current privacy debate.

Essay by: Stijn Voogt

Category: Aspects of philosophical and societal impact

Since the rise of the Information Age, several events, in example the NSA-, and Facebook-scandals, have triggered public debates about privacy. These debates are often about the infringement of privacy rights, and have recently become topical again in discussions about the 'General Data Protection Regulation' (GDPR). In these discussions we basically hear the exchange of the same worn out arguments again and again. I think that it is time to broaden our perspective on the crux of digital privacy.

Already in 2004, privacy theorist Daniel J. Solove pointed out the importance of the way debates on privacy are framed, because it determines the way people think about the subject[1]. Important, whereas there actually is a lot to think about. Nevertheless, current debates do not often transcend the superficial view on privacy as conception of an individual freedom. In fact, within this narrow meaning, which I like to call first-line privacy, privacy becomes limited to nothing more than a free living space in which we will not be subject to the interfe-rence of others. Yet, a broader scope on the meaning of the concept of privacy is possi-ble, and involves fundamental principles such as democracy, autonomy, and the presumption of innocence.

In his book "The Digital Person", Solove reacts on this more substantial, or second-line, approach of privacy. He makes a distinction between two classic-literary metaphors for today's privacy difficulties, using George Orwell's "1984" and Franz Kafka's "The Trial". In Solove's opinion, when it comes to unjustifiable breaches of privacy rights, people would often unjustly refer to the Big Brother, who is watching them. Solove argues that in that Orwellian view the State, or any other oppressor, would be undoubtedly known to the public, whereas reality is not all that simple. There-fore, he rather refers to "The Trial".

In this novel the protagonist Joseph K. suffers from a far less obvious force, which is controlling his personal life. Based on a detailed dossier of which he does not know the content, Joseph gets arrested and finally executed. Although this is only a literary fiction, it comes pretty close to the present-day person's loss of privacy control. The world digitalises in a rapid tempo, while people are hardly capable of understanding the mechanisms that keep track of their online personal data[2].

That Joseph K.'s fictional world is becoming increasingly realistic can be con-cluded from the findings of technology-researchers Frank Pasquale and Danielle Citron. The duo states we are currently living in a so-called scored society, wherein people are reduced to a compilation of data[3]. In other words, governments, as well as companies, and employers are keeping citizen's score in order to determine their suitability for a certain right or specific service. This system, which is mostly based on digital data processed by algorithms, influences peoples' behaviour in ways they are not even aware of.

> **"Privacy becomes limited to nothing more than a free living space."**

Considering this miserable perspec-tive society is threatened with, it is neces-sary to alter the debate. Not only could the discussion use a more Kafkaesque perspec-tive. One should also be more aware of the consequences of second-line privacy viola-tions, instead of focussing on the more obvious first-line.

1 Solove, D. J. (2004). The Digital Person: Technology and Privacy in the Information Age. New York and London: New York University Press.
2 Martijn, M., & Tokmetzis, D. (2018). Je hebt wél iets te verbergen: over het levensbelang van privacy. De Correspondent.
3 Citron, D. K., & Pasquale, F. A., (2014). The Scored Society: Due Process for Automated Predictions. Washington Law Review, Vol. 89, 2014, p. 1-; U of Maryland Legal Studies Research Paper No. 2014-8. Available at SSRN: https://ssrn.com/abstract=2376209

Privacy? Who cares!

Philosophical aspects and societal impacts.

Essay by: Milan Weber

Category: Aspects of philosophical and societal impact

What is the current philosophical trend concerning privacy and what are the societal impacts of the question about privacy in the time in which we are living? Around forty percent of the world population is connected to internet and this number is growing.[1] From this perspective we can conclude that the meaning of the word privacy is constantly changing or at least it has changed when we compare it with for example the meaning it had fifty years ago.

1 "Internet Users," Internet Live Stats, last modified May 9, 2018, http://www.internetlivestats.com/internet-users/.

Nowadays, ethical questions are asked about the accessibility of personal data and what people can do with it. Some people say that we are living in a post-truth era.[2] This current trend means that we face difficulties concerning the plausibility of official organisations who promise or guarantee that our private data is protected. So, before questioning the ethical aspects of privacy, we should focus on the reliability of the institutions who make privacy laws.

"Do we trust the European Union to do what they promise?"

Within the realm of ethical philosophy, multiple philosophical perspectives can be used to shine a light on this current debate. From the perspective of Hegel, one might argue that we should embrace the idea that organisations have access to our data, for his notion of freedom is linked with the idea that people accept certain laws, given by a national or international government.[3]

However, the question is to what extend we can trust that the General Data Protection Regulation will increase our privacy. People might agree that their personal data needs to be protected and that individuals need to have the right to know where our data is stored. But the main question is: Do we trust the European Union to do what they promise?

This postmodern view on reality has influence in the way we are looking at official organisations in the time in which we are living.[4] The impact on the society is that people are sceptical towards such announcements and it seems that people do not know what to believe. This attitude is also fed by news items that doubt the reliability of these new privacy laws.[5]

The postmodernist view on official organisations seems to result in the fact that people doubt to what extend these new regulations have influence on their privacy. Ethical questions concerning privacy can be asked when people regained their trust in the official organisations that control privacy regulations.

2 William Davies, "The Age of Post-Truth Politics," **The New York Times**, August 24, 2016, https://www.nytimes.com/2016/08/24/opinion/campaign-stops/the-age-of-post-truth-politics.html.

3 Sally Sedgwick, "Philosophy of History," in **The Oxford Handbook of German Philosophy in the Nineteenth Century**, ed. Michael N. Forster and Kristin Gjesdal (Oxford: Oxford University Press, 2015), 436-452.

4 Mark T. Gilderhus, "Postscript: Culture Wars, Postmodernism, and Other Issues," in **History and Historians: A Historiographical Introduction** (Upper Saddle River, N.J.: Prentice Hall, 2010) p. 111-125.

5 Rosemary Smith, "Will the GDPR Really Make a Difference to Consumers," Data Protection Network, accessed May 9, 2018, https://www.dpnetwork.org.uk/opinion/will-the-gdpr-really-make-a-difference-to-consumers/.

Erasmus University Rotterdam (EUR)

Burgemeester Oudlaan 50
3062 PA Rotterdam, The Netherlands

www.eur.nl