FH Wedel

IT Engineering Master

WS 2019

Seminar Paper:

The economics of privacy

Author:

Imane Berchid,

Imm: ITE103601

Semester: 3rd semester IT Engineering

Supervisor:

Prof. Dr. Gerd Beuster

January 2020

Table of Content

Introduction 3

I. The economic theory of privacy 4

1. Privacy as an economic good 4

2. The evolution of the economic theory of privacy 5

II. Benefits and costs of disclosed and protected Data 10

1. Benefits and positive externalities of disclosed data 10

1.1 Data Holders 10

1.2 Data Subjects 13

2. Costs and negative externalities of disclosed data 14

2.1 Data Holders 14

2.2 Data Subjects 16

III. The evolving privacy debate 18

1. Privacy and regulation: regulation vs. self-regulation 18

2. Privacy and technology 19

Conclusion 21

Bibliography 22

Introduction

Nowadays, thanks to the advances in technology, the ability to collect, store and process information has become much easier and less costly. Companies can record details of each customer transaction, websites log their visitors' behavior and data aggregators gather information from different sources to build profiles of individuals. As a matter of fact, daily activities and personal information can be tracked online through information technology and social media, which may happen without the person's knowledge or consent, and thus raises privacy concerns. [37] Collecting such data enables businesses to better serve their customers in order to retain them, and also to attract new ones, using powerful data mining and machine learning algorithms to do predictive analytics, targeted marketing and build recommendation systems, in order to stay competitive in a rapidly growing market.

On the other hand, people also benefit from sharing their information. They can receive personalized services and targeted marketing to serve their needs, and they can use others customers feedback to help them in their decision making process, given the panoply of choices available. Nevertheless, individuals remain skeptical about the security of their data and want to avoid the misuse of their information.

In this regard, the issue concerning privacy arises as a result of a conflict of interest between its commercial value and the respect for an individual's right to privacy, which led to the emergence of the economics of privacy as an important discipline that involves regulation, technology, people dynamics and business efficiency. Economics can help us understand how individuals and organizations make decisions about the usage and protection of personal data, and what the outcomes of these decisions are. [37]

In this seminar paper, we will explore some of the economic consequences of the protection and revelation of customers' personal data and examine some of the privacy tradeoffs and debates associated with the sharing of such data.

I. The economic theory of privacy

The economics of privacy aims to analyze how individuals, firms and policy makers interact in markets where personal data play a key role. In this section, we analyze the concept of privacy as an economic good, and then we present the evolution of the theory of the economics of privacy by reviewing different works on the subject.

1. Privacy as an economic good

The concept of privacy has always triggered the interest of lawyers, political scientists, sociologists, philosophers and psychologists, but only since the 1970s that of economists. [36] Privacy concerns personally identifiable data, such as name, birthday, location, browsing behavior and purchase history. This information can be considered as an economic good for at least two reasons [25].

First, individuals value privacy as an intermediate as well as a final good. Privacy is seen as a an intermediate good when, for example, consumers want to avoid being charged higher prices if firms have the ability to identify their willingness to pay for a product or service, and thus engage in price discrimination. On the other hand, it can be considered as a final good when individuals feel uncomfortable sharing their personal information or feeling that they are being watched and tracked. [3]

Second, privacy is a non-rival good from a firm's perspective. This means that information shared by consumers with a firm is still valuable and available to other firms that may be interested in it. In fact, consumers still own their private data and can consider trading it with other firms. [25]

Many factors influence individuals' privacy concerns and the way they make the decision of disclosing or protecting their data. Researchers from different disciplines have attempted to estimate the value that individuals assign to their privacy and their personal data, and they came to the conclusion that such valuations are strongly context dependent. In fact, we can distinguish three types of transactions in which consumers make decisions about their privacy. The first type occurs in ordinary markets, where personal information can be considered as a "by-product" of an exchange of an ordinary good, such as purchasing a product or booking a flight online. In this case, consumers unknowingly trade their data in order to be able to use certain platforms or services online. This revealed information may be collected, analyzed, and then used by these platforms in different ways. [3]

The second type of transaction occurs in what can be called the “market for personal data”. It is when consumers provide personal information in exchange of free services, such as social networks, search engines and email programs. Another kind of exchange in this second type of transaction involves data intermediaries that trade consumer data among themselves or with other data holding firms, and data subjects are not active agents in such transactions. [3]

The third type of transactions occurs in what may be considered as the “market for privacy”. In this type, consumers explicitly purchase privacy-enhancing products to protect their personal information or hide their browsing behavior, such as encryption programs. [3] The evolution of data mining and analytics tools will continue to affect these different markets, both positively and negatively, leading to complex tradeoffs, which will be discussed in the following chapters.

2. The evolution of the economic theory of privacy

We can distinguish three waves characterizing the economics of privacy research. The first wave emerged in the 1970s and early 1980s, it was characterized by economic research works produced by the Chicago School scholars such as Stigler and Posner, and consisted of arguments around the positive and negative outcomes touching the individual and society as a result of personal data protection. [4]

In the neoclassical economic theory of perfectly competitive markets, the availability of relevant information to all market participants leads to economic efficiency. For example, when a product’s prices from each firm offering it are known to all consumers, it leads to lower prices and thus enhances consumers’ welfare. [2]

In accordance with this theory, the protection of privacy can be seen as a source of inefficiencies in the marketplace, since it enables the concealment of information that may be important. For example, protecting the personal information of a job seeker who falsifies their background and expertise to a hiring firm will negatively impact the company's hiring decision and thus profitability. [36]

In the same line of thought, regulatory involvement in the market of personal information is seen to remain ineffective, given that individuals tend to disclose positive personal information and hide negative ones. In this case, economic resources would also end up being inefficiently used or unfairly rewarded, due to the lack of information about their quality in the marketplace. [44]

However, this initial theory presenting privacy as a source of inefficiencies faced criticism from economists from this wave and later waves. In fact, firms may end up inefficiently over-investing in personal data collection, and the assumptions of rational behavior, based on which the Chicago School's privacy models were built, may fail to represent the complexity related to the consumers' decision making concerning their privacy. In addition to that, the private benefit of information acquisition may outweigh its social benefit, and in certain settings, it may have no social value, but will only redistribute the wealth from ignorant to informed parties. [20]

Murphy and Daughety and Reinganum also refute the Chicago School theory. In a model where each individual cares about their reputation, they show that individuals tend to distort their actions to preserve their reputation under publicity, while they choose the optimal level of activity under privacy. As an example, keeping information about people checking in drug and alcohol rehabs private can be welfare enhancing for the society, since exposing such information to the public may hinder many individuals from seeking treatment. On the other hand, when charitable contributions are made public, the donations may increase, since such acts positively contribute to the reputation of the donors. [33], [13]

The second wave emerged in the mid-1990s, as a result of the information technologies progress, such as the spread of electronic databases and the advent of the Internet, which led to new concerns around the use of personal data. This wave was characterized by the specificity of the privacy scenarios considered, and the growing awareness of the role of information technologies. The works were focusing on new issues such as the establishment of markets for personal data, and the economic implications of the secondary use of personal data. [4]

In this wave, some of the concerns related to the secondary usage of personal data were highlighted. While a consumer may willingly share their personal information with a firm in order to get certain benefits, they have neither the awareness nor the control of how the firm will use that data. The latter may be sold to third parties to generate profits that the individual will never share, or may even cause them trouble if their data is misused, for spam or price discrimination, to cite a few, and many consumers cannot afford the acquisition of privacy protection under standard market conditions. [49] Other concerns related to personal data are caused by the development of low-cost technologies for data manipulation. [50]

In addition to the possible individual costs from data protection, there exist some social costs. Using a repeated prisoner dilemma[1] game, Friedman and Resnick show that the use of cheap pseudonyms results in a distrust of newcomers as an inherent social cost. Thus, privacy of identity can be a hindrance to trust building in the society. Nevertheless, they show that it is also possible to minimize those social costs while protecting privacy, by using intermediate forms of identity protections. [16]

Noam argues that the protection of personal data depends on the valuations of the parties interested in it rather than regulation. So, if the consumer values their data privacy more than the marketing firm does, even with the lack of laws protecting it, they would be willing to pay to keep it protected. However, the lack of regulation will affect which party should pay the other for access to or protection of the data. [34]

Laudon suggests the creation of information markets, where people can trade their personal information in exchange for some compensation. Following the same line of thought of the Chicago scholars, he argues that a system based on property rights over personal information would better meet the needs for both parties. [29] However, this would require proper legislation to define and manage these rights. While the assign-

[1] The prisoner's dilemma is a standard example of a game analyzed in game theory that shows why two completely rational individuals might not cooperate, even if it appears that it is in their best interests to do so - Wikipedia

ment of property rights is generally welfare enhancing, giving the consumers the right to trade their data may undermine the consumer surplus. [4]

The third wave is a more recent one; it is characterized by a significant increase in economic research works around the economics of privacy at the start of the twenty-first century. It is also characterized by studies done in more formal economic models and empirical analyses, including lab experiments. Furthermore, it is more related to the new economic issues raised by the development of information technologies including search engines, behavioral targeting, and social media. [4]

The economics of privacy is closely linked to the studies on price discrimination based on consumer identification. Although these studies consolidate the notion of tracking and personalized pricing, they do not explicitly consider privacy issues in the online environments.

Villas-Boas and Fudenberg and Tirole study a duopoly model in which consumers have a choice between remaining loyal to a firm or leaving it for the competitor, a phenomenon they call ”consumer poaching". They show that a firm is always motivated to offer discounts to a rival’s customers who show a preference for the rival’s products. Such discounts aim at reducing consumers’ price sensitivity for a firm’s products and result in an increase in prices later. [51]**,** [17]**.** Another strategy is called “price for information", where firms offer lower prices in order to gain some knowledge about their customers [10]. Jeong and Maruyama and Jing identify conditions under which a firm should discriminate against its first-time and repeat customers. [24]**,** [26]

Taylor shows that, in the presence of tracking technologies that provide tracking capabilities to merchants, the role of privacy regulatory protection in enhancing welfare will depend on consumers’ level of sophistication. In the case of naïve consumers, privacy protection through regulation may be necessary, because they may unknowingly be subjects to price discrimination applied by merchants based on collected consumers’ data. Such regulation would not be needed if consumers are aware of the way their data will be used, and could adjust their buying decisions accordingly. [47]

In certain scenarios, strategic consumers may worsen a firm’s dynamic targeted pricing, by choosing not to buy a product instantly once they anticipate future prices, they can avoid being identified as a past consumer and benefit from lower prices targeted at new consumers. [52] Such strategic behavior may negatively impact the firm's sales and even push them to voluntarily adopt privacy-friendly policies. Companies may even be disposed to develop their own privacy enhancing policies to maximize their profit, without any regulatory intervention, and the more companies detain power in the market, the more they are willing to commit to privacy enhancing policies. [4]

On the other hand, data holders - such as Amazon, Google and Facebook – play a major role in the economics of privacy. Such companies act like data intermediaries, since they sell advertising space to the advertisers, and provide services to the users. Information about users can be collected based on the searches they do and the products they view online, which can be used for targeted marketing. In this regard, targeting reduces search costs for consumers, improves matches between consumers and firms and leads to more intense price competition. However, targeting benefits could be negated if the search engine decides to charge a very high advertising fee to the advertisers. [11]

Intermediaries can manipulate the matching between consumers and firms by directing consumers towards firms they would not have visited otherwise, if the intermediaries receive certain fees from these firms in return of the visits. Thus, the intermediary can manipulate the elasticity of demands faced by its affiliated firms. [19]

By analyzing the acquisition of user information by an advertising platform and its sale to advertisers, Bergemann and Bonatti prove that the more precise the user information is, the fewer records the advertisers tend to buy. As a result, a data provider may choose to limit advertisers' access to users' data in order to sell more records and generate higher profits. [5]

Other works study the interactions between sellers and buyers depending on how they can track and access data about each, and different approaches to limit the release of consumers' information. Finally, we can conclude that both advertisers and intermediaries often don't have the optimal incentives to match consumers with products. [4]

II. Benefits and costs of disclosed and protected Data

In this section, we study the economic value of privacy by exploring some of the outcomes of disclosing and protecting personal data. We start by considering the positive externalities from disclosing data in the first part of this section, and then we study the negative outcomes that could result from it. We refer to consumers as data subjects and to firms as data holders.

1. Benefits and positive externalities of disclosed data

We begin by presenting the economic benefits of disclosed personal data, for both data holders and data subjects, as well as highlighting the opportunity costs suffered when valuable data is not disclosed.

1.1 Data Holders

1.1.1 The benefits of disclosed data

We are living in a data-driven commercial revolution, where individuals play two major roles of customers and data producers. With advances in technology, it is easier today to draw accurate profiles of individuals by analyzing their online browsing data, purchase history and personal traits, collected from social media, cookies, packet inspection and databases. There is a growing interest in individuals' data, which is purchased, sanitized and combined to be later sold to public and private organizations.

Firms can significantly benefit from individuals' data, which they can use to improve their marketing capabilities through targeted marketing -that is at the same time highly effective and less costly- not only to retain their current customers but also to attract new ones, by addressing the right set, thus increasing their revenues. [2]

By applying data mining and machine learning algorithms on large amounts of data, firms can make accurate predictions about customers demand and preferences. They can build and continuously improve recommendation systems and enforce profit-enhancing price discrimination. In addition to that, they can redesign and update their products and services to match the expected demand from customers [2]**.**

An example to illustrate these benefits is online advertising. In 2008, fifty-six of top one hundred websites (based on page views), accounting for 86 percent of page views for that group used some kind of online advertising, and probably got most of their revenues from doing so. By 2012, $36.6 billion were spent on digital ads, ahead of cable TV ($32.5 billion) and slightly below broadcast TV ($39.6 billion), with a rate of growth faster than all other types. By 2015, digital ad revenues had reached $52.8 billion, a third of overall advertising approximately. [15]

Unlike their offline peers, online ads can be tailored to each individual based on their online behavior, (such as search history, sites visited, clickstream data on a given site). Various and constantly evolving technologies (such as web bugs, or flash cookies, etc.) allow advertisers to track consumers' browsing activities and gain insight into their interests. Such "targetability" results in cost reduction of ads on customers unlikely to be receptive to them. [4] Furthermore, advertisers can monitor and improve the effectiveness of online ads more than in other marketing channels, referred to as "measurability", which allows higher revenues for marketers and merchants. [2]

The credit market offers another example of how the collection and analysis of flows of consumers' data can be beneficial. In the USAs, the credit-reporting industry is among the most regulated in terms of data protection. The collected information by credit reporting agencies, which is analyzed then sold, contributes to the efficient allocation of credits, and thus to provide added value to both the market place and the consumers. [39]. Moreover, sharing information about their customers leads banks to an increase in lending to safe customers and thus decreasing default rates[2] [35], and credit scoring provides the ability to target more generous loans to lower-risk borrowers among individuals with lower income. [14]

Organizations also benefit financially by selling customers data to other firms. This is the case of Web 2.0 enterprises, such as social networks, for which consumers' data is a valuable product that can be sold to marketers, advertisers and data aggregators interested in the behavioral and personal data generated by these platforms. This is also

[2] The default rate is the percentage of all outstanding loans that a lender has written off after a prolonged period of missed payments. A loan is typically declared in default if payment is 270 days late – URL : https://www.investopedia.com/terms/d/defaultrate.asp - 25/12/2019

the case for other firms which produce other type of products but which customers' data may be valuable to other organizations. [2]

Finally, the aggregation of data can be beneficial even when the personal data is anonymized. In fact, firms can benefit from drawing consumers trends based on the analysis of such data. Companies such as comScore, for example, analyze web trends by combining behavioral and survey observations of millions of online consumers and then provide their clients insightful data that can be used for competitive intelligence, market testing, and segmentation analysis. [4]

1.1.2 The costs of data collection and the costs of protected data

It is important to highlight the costs and investments necessary to collect, process and store personal data. While the costs of collecting and storing data have been decreasing with the technology progress, the implementation of systems that make efficient use of data is not easy. [4]

Moreover, firms can endure opportunity costs when potentially helpful data is not available, and they can face significant competition disadvantages against those who have access to data. Furthermore, the lack of customers' data and uncertainty about possible legal retaliations resulting from data collection may construct a hindrance to product innovation.

Privacy regulations can also have a negative impact on the advertising industry. In this regard, evidence shows that after the ePrivacy Directive was passed, there was a significant decrease in advertising effectiveness. This can impact many web-based businesses that rely on online ads as a primary source of revenue. [4]

In the healthcare sector, privacy regulations may affect the adoption of EMRs (electronic medical records). EMRs allow medical providers to manage patients' data electronically rather than using paper records, which enhances the efficiency and quality of these records. [4]

Although EMRs were invented in the 1970s, by 2005 only 41 percent of US hospitals had adopted a basic EMR system. This reluctance is due to several reasons; including the concern about patients' responses to this new technology and the privacy regulation that may hinder their adoption in case hospitals misuse them – for example to exchange patients' info with other hospitals. [4]

Finally, the lack of data may also negatively affect the work of policy makers, researchers, or healthcare providers, such as in the case of national surveys, if the participation is made optional (example: the Canadian long-form Census questionnaire participation decreased significantly after it was made optional). [2]

1.2 Data Subjects

1.2.1. The benefits of disclosed data

Data subjects may directly or indirectly benefit from sharing personal information with organizations. They can receive tangible benefits such as discounts or free trials, or intangible benefits such as personalized content and recommendations. In some cases, individuals can profit from giving their data to third parties in return of improved services, targeted offers or even less junk mail. Some economists have proposed a "propertization" of privacy (see [49], [28]) where the individual can sell their own personal information into a marketplace, or try to buy back the privacy right of that data. [2] Targeted advertising can also have advantages for individuals: it can both provide them with information at less search costs, as well as other free services such as news. Moreover, these ads may be visually less invasive compared to non-targeted ads. [2]

Consumers may also get positive externalities when there is a secondary market of personal data. For example, when data provided to a website makes the service more convenient on another site, such as Facebook Connect, which enables authentication to some third party websites, thus reducing signing up costs for users. [2]

It is important to note that the analysis of behavioral and decisional data collected from online sources, from sensors and from other economic agents may lead to early identification of trends that would otherwise be hard to notice in a limited period of time, which can benefit the society as a whole. For instance, the monitoring and aggregation of online searches can lead to early detection of infectious diseases outbreak; the combination of inputs from mobile devices may be used for traffic and congestion control; data from remote and distributed sensors on consumers' machines may be used for environmental monitoring. [2]

Furthermore, more access to genetic and genomic data can result in significant improvements in overall health care. In fact, it can help in developing treatments, vaccines, and immunizations and can be used in providing targeted and personalized medicine. [4]

It can be argued that such benefits may be fulfilled without customers having to disclose personally identifiable data, by using privacy enhancing technologies which makes it possible to both satisfy the need for preserving privacy and the need for sharing data. [2]

1.2.2. The costs of undisclosed data

Some of the highlighted advantages mentioned before can turn into opportunity costs if the data is disclosed from being used in many applications that can benefit the society.

At the individual level, the opportunity costs of undisclosed data may become more significant, since more products and services require providing some personal information. For instance, an individual who decides not to join Facebook in order to protect their data will not be able to use a website that can only be used through Facebook authentication; or could miss an event that is only announced on Facebook. [2]

2. Costs and negative externalities of disclosed data

In this section, we examine some of the negative externalities of disclosed data and highlight some of the costs of protecting data.

2.1 Data Holders

2.1.1 The Costs of Disclosed data

Data holders can suffer tangible and intangible costs from disclosed data, some of them related to the collection of data, and other to the way it is used.

Online and offline companies have been punished by the market for data collection behaviors that were seen as invasive of consumers' privacy, although not necessarily illegal. A famous case was Amazon.com's dynamic price experiment in September 2000, when a customer had purchased a DVD for $24.49. The following week, he found that the price on Amazon had risen to $26.24. However, after deleting cookies and removing all the electronic tags that could identify him from his computer, he found that the price fell to $22.74. As a result, Amazon.com suffered a significant PR (public relations) damage. The company had to reimburse customers who had paid higher prices for the DVDs and promised to renounce dynamic pricing, or price discrimination. [2]

Another negative outcome touching many companies is data breaches, involving their customers and employees. While they may or may not be due to malicious acts, breached organizations can end up suffering huge costs, including fines, legal fees, and redress costs. [2] For example, Facebook lost around $13 billion in value after data breach affected 50 million of its users in 2018 [27].

Firms may also lose customers who think that their data is not well protected, or lose transactions from these customers. However, it remains difficult to estimate these effects with precision, due to the possible mismatch between customers' intentions and privacy decisions, in addition to the possible desensitization that may result from getting used to privacy issues. [4]

2.1.2 The costs of protecting data

Protecting consumer data can be costly for firms in two ways. First, firms can give up the potentially profitable data collection and mining in order to avoid any potential privacy costs. This can be considered as an economic opportunity cost. Second, firms may invest, and sometimes over-invest, in data security and protection in order to avoid privacy issues. [2] There was also an increase in security investments in US firms after the passing of data breach disclosure laws. [21]

Additional costs include the social losses due to "incoherent privacy policies", as a result of the uncertainty around the level of protection required for various types of personal data, for both the consumers and the firms. This leads to generating additional costs for learning about the admissibility of a given data practice, and may lead to eventually inefficient investments in data protection. [42]

2.1.3 The benefits of protected data

There is an ongoing debate on whether firms can benefit from protected data. While missing the benefits that could be got from collecting personal data, they may limit the costs related to the misuse of such data. Moreover, offering some privacy services may also indirectly benefit the firms. For example, some anonymous payment systems may have authentication features that could decrease the risk of fraud; or investing in firewalls and encryption of server data may also protect the company's information systems. [2]

2.2 Data Subjects

While disclosing personal data can benefit consumers by offering personalized products and useful recommendations, there are several negative externalities that result from data sharing. The uncertainty related to the privacy costs can be compared with "the blank cheque" metaphor; the fact that an individual is disclosing private information to other parties is similar to signing a blank cheque to them. The cheque may never be returned to them or may be back for a certain price. This price could go from a simple feeling of embarrassment, to an annoying spam or a catastrophic case of identity theft. [2]

Consumers may suffer price discrimination and may be offered products inferior to the ones they would have found otherwise. There is evidence of price discrimination based on information collected online about consumers, as well as evidence of "search discrimination", directing them towards products that they don't need or which are not the best choice for them [31]. Certain online retailers may even be applying dynamic pricing based on their ability to predict visitors' locations, and physical distance from a rival store. [48]

Available information can lead to other types of discriminations, such as in the job market, where applicants can face discrimination in hiring and wages based on their race, religion or sexual orientation. Such data can be inferred from their resume, or easily obtained online as many candidates publicly share personal information through social media. Even though the law prohibits employers to ask about such personal information, it has become easily accessible to them with low risk of detection. [4]

Evidence also shows that employers use criminal records to filter candidates [8]. As a result, individuals with criminal records are more likely to experience job instability and wage decline. However, it was found that the probability of recidivism declines with time spent without committing a criminal act [7], and eventually an ex-offender can be considered as a non-offender after some time. In those cases, there could be some positive outcomes from forgetfulness [6].

Privacy may also overlap with information security. In fact, many topics are of interest to both privacy and security researchers, such as spam, identity theft, and data breaches. A study by Ferris Research estimates that in 2009, the cost of spam, accounting for decreased user productivity, was about $130 billion, with $42 billion in the United States alone. In 2012, Rao and Reiley estimated a much lower overall societal cost of spam, $20 billion [38]. While spam results in a low cost per user, since all internet users receive it, identity theft results in larger individual costs. In 2006, identity theft resulted in corporate and consumer losses of $61 billion, with 30 percent of known identity thefts caused by corporate data breaches. [4]

Another emerging trend is the testing for genes. Nowadays, a number of companies are offering genetic testing to individuals at affordable rates. Even though US laws limit insurers' ability to get hold of such data, marketers and advertising firms may be interested in it. If advertising platforms and data aggregators get access to such data, they can use it to build risk profiles for individuals and their biological relatives and improve their targeting. [4] Finally, personal information can also be misused to target people with vulnerabilities. For instance, data brokers sell lists of individuals suffering from addictions such as alcoholism or gambling. [4]

III. The evolving privacy debate

1. Privacy and regulation: regulation vs. self-regulation

The debate around means to protect privacy while maintaining the benefits of information sharing is stressed by the empirical studies of privacy tradeoffs. Much of this debate has studied and compared the benefits of regulation and self-regulation.

On the one hand, there are views that support the regulatory solutions to the privacy problem. Among the advantages of such solutions is to make it easier for data subjects to interact with different concerned entities with different privacy policies. [32] Another reason is the potential costs that consumers and merchants bear in the absence of privacy protection. In fact, consumers may suffer costs caused by identity theft, spam, and investments made to protect their data, and firms can undergo sales costs caused by privacy concerns among the consumers. [4]

On the other hand we find advocates of self-regulation. Some suggest that, for both firms and consumers, the costs that may arise from privacy violations are much less than the costs of privacy protection. [39] In this regard, self-regulation may work when the concerns over disadvantageous customer response lead advertisers and firms to use less intrusive targeting of ads [30], to comply with their privacy policies and to use more privacy-friendly methods and avoid spam [22].

Information privacy is seen a major problem and its growing importance led to the evolution of privacy regulations in the United States and in Europe, which adopted divergent privacy models. While the EU opts for regulatory solutions, such as the General Data Protection Regulation (GDPR), the US suggests guidelines rather than enforcing principles, such as the Federal Trade Commission (FTC 2012).

Self-regulatory solutions generally depend on transparency and control, and thus they are based on the individual’s capacity to properly manage and be informed about privacy settings and concerns. Transparency and control mechanisms have been the subject of several critiques, which expressed doubts about their ability to appropriately protect consumers’ privacy. Studies about transparency mechanisms have emphasized their limitations, including the failure of privacy policies to properly inform consumers about the way their data will be used [23]. Moreover, providing users with more perceived control over their personal information may lead them to take more risks with their personal information, and to share more sensitive data with other parties. [4] Several authors have suggested the establishment of markets where individuals can trade their personal data, and many startups began offering such services, such as the concepts of propertization (see [28]; [50]; [43]) or licensing of personal information [42]. However, the future success or failure of such markets is still not clear. In fact, when interacting with such services, consumers are faced with the same obstacles related to transparency and consent as in the traditional privacy policies, including the estimation of the value of their data. Furthermore, in the lack of regulation, the risk of secondary usage of personal data persists. In addition to that, much of the personal data that interests advertisers in the data generated from the interaction between users and other online services, like search engines and social networks, and such services would not be willing to cede the data that their technologies are generating. [4]

To conclude, the economic impact of regulation is heterogeneous and context dependent, and appears to be more complex than a mere choice between two models, but will rather need the development of specific features of regulation to protect personal data, while maintaining the beneficial outcomes related to its proper use. [4]

2. Privacy and technology

The advances in technology have led to the increase in the amount of personal information produced and gathered by individuals, nowadays referred to by “Big Data”, as well as the ability to use data mining to infer more sensitive information about them. With evolving data mining and analytics tools, in addition to new technologies such as facial recognition, and the Internet of Things, there is less and less personal information which cannot be accessed and monitored. [4] It is even possible to re-identify anonymous data as highlighted in a study conducted on health data. [46]

Although detailed personal data improves the services targeting, which is likely to benefit the consumers, a high risk of abuse persists. For example, studies of cases of algorithmic discrimination show how advertising technologies employed by a search engine can reveal racial bias [45]. Personal data may also be used to influence individual decision making [9] which raises questions about the limits of an individual’s autonomy.

On the other hand, technology can be used to minimize or avoid risks to privacy and data protection. The idea of shaping technology according to privacy principles has been discussed since many years, addressing among other the principles of data minimization, anonymization and pseudonymization. This led to the term Privacy Enhancing Technologies (PETs), which covers the broader range of technologies that are designed for supporting privacy and data protection [12]. Identity Management Systems (IMS) are a type of PETs which give the user the control over the type and level of information they can reveal.

Encryption technology has also seen considerable adoption and gives the parties involved control over access to information. However, rationality does not guide decision making in privacy [37]. So, even with the adoption of encryption, the difference it makes is that it allows consumers to be paid in exchange of revealing their information [34]. Furthermore, PETs such as anonymity could provide the consumer with bargaining power to reveal their information, over which they have increased control, and such anonymity technologies are not found to be beneficial to consumer welfare. [1]

Nevertheless, concerns are raised by the use of these technologies, such as their role in affecting the way in which the personal data will be used and its impact on the economy [18]. In addition to that, reducing the granularity of the data resulting from the use of PETs may lead to decreasing its economic value, which raises questions about the costs generated by their use, including implementation costs as well as opportunity costs, and which party should bear those costs, the data holders or the data subjects.[4]

Finally, questions about optimal retention policies concerning big data are also raised; such as the impact of “right to be forgotten” suggested by the European Commission on privacy protection and on the benefits of data sharing. [4]

Conclusion

In today's competitive market, individuals' personal information is of a commercial value. It is used to generate consumer surplus and satisfaction, and improve business efficiency and decision making. This information could include an individual's credit history, medical records, criminal and civil reports, employment history and background checks done by firms and government agencies. However, there is a growing concern about unauthorized commercial use of personal data, which may lead to numerous costly consequences for the individuals, such as price discrimination and identity theft. [37]

Advancement in information and communication technology has made it more difficult to evaluate the privacy risks associated with the interaction between individuals and other party. Social media, for instance, have fostered the culture of disclosure. Meanwhile, users lack in awareness and sophistication, which is required to protect their data, and privacy protecting services require more efforts and expertise from the users' side, which limits their efficacy. [37]

Such concerns have led to new regulations across governments, some protecting privacy, such as the EU Data Protection Directive and the US Children's Online Privacy Protection Act, and some legalizing its erosion, for instance, by allowing trade in personal information under certain circumstances; e.g., the US Gramm–Leach–Bliley Act of 1999, and some suggesting the implementation of additional controls for users (e.g., the US Federal Trade Commission's 2012 online privacy guidelines).

To conclude, the balancing of data protection and sharing needs a case by case study and combinations of regulatory interventions, technological solutions, and economic incentives to increase individual and societal welfare, and any solution to privacy should not negate the benefits of information sharing, but rather balance between these benefits and privacy protection. It is also necessary to highlight the need for increased consumer education on internet trade to help them make well informed decisions about their personal information. [4]

Bibliography

[1] Alessandro Acquisti and Hal R. Varian. (2005). Conditioning prices on purchase history. In Marketing. Science.

[2] Acquisti, A. (2010). The economics of personal data and the economics of privacy. The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines.

[3] Acquisti, A. (2013, September 12). The Economics of Privacy:Theoretical and Empirical Aspects.

[4] Alessandro Acquisti, C. T. (2016). The Economics of Privacy. Journal of Economic Literature .

[5] Bergemann, D. a. (2013). Selling cookies.

[6] Blanchette, J.-F. a. (2002). Data retention and the panoptic society:The social benefits of forgetfulness. The Information Society .

[7] Blumstein, A. a. (2009). Redemption in the presence of widespread criminal background checks. Criminology .

[8] Bushway, S. D. (2004). Labor market effects of permitting employer access to criminal history records. Journal of Contemporary Criminal Justice .

[9] Calo, R. (2014). Digital market manipulation. In G. W. Review.

[10] Chen, Y. a. (2009). Dynamic targeted pricing with strategic consumers. International Journal of Industrial Organization .

[11] Cornière, A. D. (2011). Search advertising.

[12] Cybersecurity, E. T. (n.d.). Privacy enhancing technologies. Retrieved January 2020, from https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies

[13] Daughety, A. a. (2010). Public goods, social pressure, and the choice between. American Economic Journal: Microeconomics .

[14] Einav, L. M. (2013). The impact of credit scoring on consumer lending. The RAND Journal of Economics .

[15] Evans, D. S. (2009). The online advertising industry: Economics, evolution, and privacy. Journal of Economic Perspectives .

[16] Friedman, E. a. (2001). The social cost of cheap pseudonyms. Journal of Economics & Management Strategy .

[17] Fudenberg, D. a. (2000). Customer poaching and brand switching. RAND Journal of Economics .

[18] Goldberg, I. (2003). Privacy-enhancing technologies for the internet, II: Five years later. Second International Workshop on Privacy Enhancing Technologies.

[19] Hagiu, A. a. (2011). Why do intermediaries divert search. RAND Journal of Economics .

[20] Hirshleifer, J. (1980, December). Privacy: Its origins, function and future. Journal of Legal Studies .

[21] Hoofnagle, C. J. (2007). Security breach notification laws: Views from Chief Security Officers. University of California, Berkeley.

[22] Jamal, K. M. (2003). Privacy in e-commerce: Development of reporting standards, disclosure, and assurance services in an unregulated market. Journal of Accounting Research .

[23] Jensen, C. a. (2004). Privacy policies as decision-making tools: an evaluation of online privacy notices. SIGCHI conference on Human factors in computing systems.

[24] Jeong, Y. a. (2009). Commitment to a strategy of uniform pricing in a two-period duopoly with switching costs. Journal of Economics .

[25] Jevons, D. (2014, October). Too much information? The economics of privacy. Retrieved December 15, 2019, from /www.oxera.com: https://www.oxera.com/agenda/too-much-information-the-economics-of-privacy/

[26] Jing, B. (2011). Pricing experience goods: The effects of customer recognition and commitment. Journal of Economics & Management Strategy .

[27] Kelleher, K. (2018, September 29). Facebook Loses Around $13 Billion in Value After Data Breach Affects 50 Million of Its Users. Retrieved 12 2019, from fortune.com: https://fortune.com/2018/09/28/facebook-stock-falls-after-security-breach/

[28] Laudon, K. C. (1996). Markets and privacy. Communications of the ACM .

[29] Laudon, K. (1997). Extensions to the theory of markets and privacy: Mechanics of pricing information. Stern School of Business - New York University.

[30] Lohr, S. (2010). Privacy concerns limit online ads, study says. New York Times.

[31] Mikians, J. L. (2013). Crowd-assisted search for price discrimination in e-commerce: First results. The Ninth ACM Conference on Emerging Networking Experiments and Technologies,.

[32] Milberg, S. J. (2000). Information privacy: Corporate management and national regulation. Organization Science .

[33] Murphy, R. S. (1995). Property rights in personal information: An economic defense of privacy.

[34] Noam, E. M. (1997). Privacy and self-regulation: Markets for electronic privacy. In U. D. Commerce, Privacy and Self-Regulation in the Information Age.

[35] Pagano, M. a. (1993). Information sharing in credit markets. The Journal of Finance .

[36] Posner, R. A. (1981). The Economics of Privacy. In T. A. Association (Ed.), The Ninety-Third Annual Meeting of the American Economic Association.

[37] Rajamani, J. Z. (2008). THE ECONOMICS OF PRIVACY, Privacy: People, Policy and Technology. International Conference on Information Security and Assurance. Pittsburgh, Pennsylvania: IEEE computer society.

[38] Rao, J. M. (2012). The economics of spam. The Journal of Economic Perspectives .

[39] Rubin, P. H. (2001). Privacy and the Commercial Use of Personal Information. Kluwer Academic Publishers .

[40] Rubin, P. H. (2001). Privacy and the Commercial Use of Personal Information. Kluwer Academic Publishers.

[41] Samuelson, P. (2000). Privacy as intellectual property. In Stanford Law Review.

[42] Samuelson, P. (2003). The social costs of incoherent privacy policies. Presentation, IBM Almaden Privacy Institute.

[43] Schwartz, P. (2004). Property, Privacy, and Personal Data. In Harvard Law Review. The Harvard Law Review Association.

[44] Stigler, G. J. (1980, December). An introduction to privacy in economics and politics. The Journal of Legal Studies .

[45] Sweeney, L. (2013). Discrimination in online ad delivery. ACM Queue .

[46] Sweeney, L. (1997). Weaving technology and policy together to maintain con. The Journal of Law, Medicine & Ethics .

[47] Taylor, C. R. (2004). Consumer privacy and the market for customer information. RAND Journal of Economics .

[48] Valentino-Devries, J. J.-V. (2012). Websites vary prices, deals based on users' information. Wall Street Journal .

[49] Varian, H. R. (1996). Economic Aspects of Personal Privacy. Technical report, University of California, Berkeley.

[50] Varian, H. R. (1997). Privacy and Self-regulation in the Information Age. In U. D. Commerce., Economic aspects of personal privacy.

[51] Villas-Boas, J. M. (1999). Dynamic competition with customer recognition. RAND Journal of Economics .

[52] Villas-Boas, J. M. (2004). Price cycles in markets with customer recognition. The Rand Journal of Economics .