CREMA

Center for Research in Economics, Management and the Arts

On the Economics of Remembering and Forgetting in the Digital Age

Working Paper No. 2016-07

CREMA Südstrasse 11 CH - 8008 Zürich www.crema-research.ch

On the Economics of Remembering and Forgetting in the Digital Age

Mark Schelker[*]

1 Information in economics

The digital revolution – the emergence of the internet and new information and communication technologies – has generated much debate on regulating "remembering and forgetting", i.e. the active management of information, and more specifically, regulation on the storage and deletion of information. This chapter provides some basic thoughts on and evaluations of the characteristics and properties of information, the role of government and potential interventions from an economics perspective.

Information is a key resource. In economics, and indeed for some time now, information has been regarded as a very distinct good. It is required for any transaction (e.g., for any purchase in markets) and it is costly to acquire (at least in the form of search and time costs). In fact, information has become one of the key components of economic theory and a key area of economic research. As Acquisti, Taylor and Wagman (2016: 442-443) so precisely put it in the introduction to their survey article on the economics of privacy in the Journal of Economic Literature:

> "The value and regulation of information assets have been among the most interesting areas of economic research since Friedrich Hayek's 1945 treatise on the use of knowledge in society. Contributions to what has become known as the field of information economics have been among the most influential, insightful, and intriguing in the profession. Seminal studies have investigated the informative role of prices in market economies (Stigler 1961); the creation of knowledge and the incentives to innovate (Arrow 1962); the prevalence of asymmetric information and adverse selection (Akerlof 1970); the transmission of private information through signaling activity (Spence 1973); and voluntary disclosures

* Corresponding address: Mark Schelker, Department of Economics, University of Fribourg, Bd. de Pérolles 90, 1700 Fribourg, Switzerland. mark.schelker@unifr.ch.
This paper has been published as: Schelker, Mark (2017). On the Economics of Remembering and Forgetting in the Digital Age. In: Thouvenin, Florent, Peter Hettich, Herbert Burkert and Urs Gasser (Eds.): *Remembering and Forgetting in the Digital Age. An interdisciplinary approach to a complex phenomenon*. Springer-Verlag, Heidelberg. 2017

> (Grossman 1981; Milgrom 1981). It may be proper, however, to think of information economics not as a single field, but as an amalgam of many related subfields." (Acquisti, Taylor and Wagman 2016: 442-443)

The aim of this contribution is not to provide another survey of the literature, but to ask what can be learned from economics on the question of how the availability of information in the digital age might affect our perspective on information, our regulation of information, and our strategies with respect to information. In what follows, economic theory is stripped to its bare bones in order to keep the arguments simple and tractable.[1]

The paper is structured as follows: Section 2 briefly discusses information in the context of transactions between individuals on markets as well as other, non-market interactions. Section 3 changes perspective and examines the role of information for interactions between individuals and authorities, most importantly, public authorities. Section 4 discusses potential information strategies that affect the evolution of the quality of publicly available information. I argue that the quality and content of information is endogenous to its use and possibility to protect it from abuse. This sets the stage for potential future developments and strategies in the use and dissemination of information.

2 The role of information in „horizontal interactions" between individuals

A first dimension consists of the role of information in "horizontal interactions", i.e. interactions between individuals and/or firms, in which the transaction between the agents is not structured by hierarchies and without one party holding formal authority over the other. The standard example is the interaction on markets, but it is not limited to market interactions. Information is essential for any interaction and transaction between individuals. *Per se* there is nothing very special about this setup. There is usually some demand for and supply of information. Individuals make decisions under uncertainty and trade off which information they are willing to provide or acquire, given the expected costs and benefits. Individuals make these decisions knowing that information can be collected, stored and also used in the future. Hence, there is no *a priori* reason for specifically regulating remembering and forgetting. Obviously, the current value of information might be very different from the value of that same information in the future. In most cases, the value of information will depreciate over time.[2] There are instances, however, where the

[1] For an in-depth review of the field of information economics with a focus on privacy issues in the digital age see the excellent article by Acquisti, Taylor and Wagman (2016).

[2] E.g. Landes and Posner (2003) with regard to trade secrets: A trade secret's initial value to a competitor may depreciate due to shifted consumer preferences, technological change or missing out on the opportunity of benefiting from a first-mover advantage. Furthermore, according to

value or relevance of a certain piece of information appreciates over time. Therefore, individuals will have to take into account whether they provide information openly to a group of people (e.g. on Facebook, Instagram, Twitter, etc.) or to a specific person, organization or firm. In the latter cases, standards of information storing, protection, and confidentiality can be agreed upon in formal contracts.

Uncertainty in decision making is nothing specific to information goods. In order to achieve an efficient allocation of resources, standard economic theory posits that transactions between individuals in such a setup require the definition and enforcement of property rights (e.g., Coase 1960). This again is not specific to the digital age. The crucial insight in this setup is that individuals on both the supply and demand side have incentives to anticipate and trade-off the costs and benefits of the provision and/or acquisition of the information *before* taking action. These fundamental incentives are the basis for an efficient allocation, i.e. the acquisition and provision of information.[3]

Regulating remembering and forgetting (beyond the protection of property rights in the economic sense) affects exactly these powerful *ex ante* incentives. On the one hand, intervening in this process (beyond the definition of property rights) via regulation can lead to allocative inefficiency. Such regulations have a strong potential to distort the incentives to trade off the costs and benefits of information provision and acquisition and to cause misallocation. On the other hand, regulatory interventions typically also change the distribution of information in a market, in firms, in society, or other social groups such as families, clubs or clans. Interventions have redistributive character because regulation typically changes information costs and information asymmetries in ways that are context and time dependent (e.g., Posner 1981, Stigler 1980). As such, regulation would also have to be context and time specific (Acquisti, Taylor and Wagman 2016).

Imagine a general right to arbitrarily edit ones' past information. First, such a general right reduces *ex ante* incentives to tradeoff costs and benefits of information provision, which leads to inefficient decisions by either inducing individuals to provide too much or too little information. Second, it incentivizes the "active management" of information *ex post* according to individual needs (and less according to some standards of truthfulness). Beneficial past information will be left unedited, while still true, but unpleasant past information is deleted. Imagine if

Ambrose (2013) roughly 85 percent of the content on the internet disappears within a year and about 59 percent within a week.

[3] Without strong and systematic information asymmetries there is no immediate reason for further intervention. Obviously, there are plenty of situations where information asymmetries can justify intervention (see the standard introductory textbooks by, e.g., Mankiw 2011, Pindyck and Rubinfeld 2012, Gruber 2012, Rosen and Gayer 2013, Tresch 2008). More paternalistic approaches might justify public interventions with the need to help individuals to make better decisions (e.g., Thaler and Sunstein 2008). A different and very rich strand of the literature evolved on strategic information transmission. It analyzes incentives and information transmission in strategic interactions (e.g., Crawford and Sobel 1982, Farrell and Rabin 1996).

people would be free to manage their credit scores or life histories according to their liking. The informational content and, hence, the usefulness of such information would rapidly decrease.

From this perspective, a general right to control and manage past personal information might not be feasible. This, however, does not prevent the case where, after some well-structured legal process, some specific single piece of information is judged irrelevant or personally and/or socially harmful, and, for this reason, it is determined that the information should be deleted.[4] Nevertheless, such rulings should be the exception rather than the rule.

Given the information technologies currently available, there might be reasons to reconsider the role of privacy regulation by rethinking and redefining certain standards of information handling, information protection, or information sharing to make it easier for subjects to anticipate the potential consequences of information provision (e.g., who will have access to personal information, to what extent and under what circumstances, etc.). The protection and enforcement of property rights in the domain of personal information require the definition of privacy laws to protect individuals from the abuse of personal information for private gain. Firms collect and connect information in order to obtain an advantage over customers and competitors. This can lead to market power and requires difficult trade-offs in privacy laws. Acquisti, Taylor and Wagman (2016) present the relevant dimensions of the problem and discuss the potential benefits and costs of such regulation. In the context of basic economics, privacy regulation could be seen as being part of the definition of fundamental property rights. In the case of confidential information being disclosed willingly or accidentally by third parties (given property rights have been defined *ex ante*), or information being manufactured to gain an advantage over customers or competitors, legal sanctions and mechanisms to delete such contents might be in order. Much of this basic regulation already exists and might have to be adapted to reflect more closely the needs of the digital age.

It has to be noted that in a decentralized, dynamic and global environment, involving the internet and the governments of many different countries, the flow of information is hard to control and, hence, even basic regulation becomes difficult to enforce. Regulating remembering and forgetting seems to go beyond the basic definition and protection of property rights, which makes the already demanding problem of enforcement even more complex.

[4] For an discussions of the legal and practical issues (and examples), see e.g., Ambrose (2013), Koops (2011) and Mayer-Schoenberger (2009).

3 The role of information in „vertical interactions" between individuals and public authority

A second dimension consists of the role of information in "vertical interactions", i.e. interactions between individuals and some authority, often public, where the transaction is structured by hierarchies with one party holding formal authority over the other. When authority and positions of power are involved, the set of problems is very different.

Two views have to be separated. First, there is the question of who delegates what competences to whom. In a democracy, the principals (the citizens) delegate decision making power to some agents (politicians and bureaucrats). In what follows I shall refer to this as the "principal-agent view". In order for the principals to control their agents, information on their actions is required. Second, there is the question of the mandate, i.e. what tasks have been delegated. In a democracy, the mandate typically consists of securing property rights, enforcing law and order, providing public goods, and to varying degrees, redistributing income and providing social insurance. To execute the various tasks connected with such a mandate, government agents require information about citizens. Hereinafter, I refer to this view as the "government mandate view".

3.1 The principal-agent view

In democracies, decision making power is delegated from principals to agents and agents are held accountable through regular elections. In elections, unwanted, unable, incompetent, or corrupt decision makers lose their mandate in a rule-based and structured process. Accountability requires that individuals are able to monitor and control public authorities that make decisions on their behalf. Elected officials can only be held accountable if citizens have access to the required information (e.g. transparency laws, official publication requirements, oversight committees, a free press etc.). For obvious reasons, such as national security etc., there can be limits to transparency.[5] However, such limits have to be based on constitutional provisions and/or statutory law and have to be justified explicitly and be authorized and legitimized through the political process. From this perspective, the institutional checks and balances in democratic systems (and in the specific case of Switzerland, the direct democratic instruments) serve the purpose of limiting the (delegated) power of public authorities.

3.2 The government mandate view

In some cases public authorities also have to be able to control and monitor some specific individuals (legal issues, terrorism, etc.). The important difference here is

[5] On the potential limits of transparency from an economics perspective see e.g., Prat (2005), Meade and Stasavage (2008), and for a short popular discussion see Schelker (2011).

that only some few (and not all) individuals have to be monitored and that this monitoring has to be conducted according to clearly specified legal rules. These rules must be transparent and specifically deduced from the underlying mandate of the government and legitimatized through the democratic process. As long as the citizens hold the ultimate power and delegate it to elected decision makers for a limited period of time – which is the most fundamental definition of democracy – government agents should not be able to freely collect information on a majority of citizens, the principals. Combined with the authority of public office, access to detailed information on citizens is an ultimate source of power and prone to be (ab)used to foster the interests of the agents rather than those of the principals. Hence, access to information must be regulated *ex ante* and limited to include only the most fundamental information required, e.g., to provide public services, to uphold the power to tax, etc. Special authority to closely monitor specific individuals (e.g. criminals) might, of course, be granted on the basis of such *ex ante* legitimatized rules. The more information that can be collected and the more authority that is granted to agents, the stronger institutional checks and balances must be to hold public agents accountable and make sure they do not abuse these powers.

This again is not specific to the digital age. It is the fundamental problem of democracy where agents make decisions on behalf of the citizens with all their (potentially conflicting) interests. However, the fruits of the fast technological progress of our times have endowed public actors with new and almost unlimited information gathering and surveillance capabilities. Given the private incentives of decision makers to hold and wield power, these possibilities might induce strong tendencies for public agents to abuse the power vested in public offices. Even solid democratic institutions risk being undermined by such technological capabilities. Hence, the rule of law, democracy, and other institutions and values might be "endogenous" to the power provided by new technologies.

The implications for the discussion on remembering and forgetting in the digital age are obvious: Consensus needs to be reached on the following questions (at least): What should be the limits of information collection (by surveillance, accessing private data archives with or without consent), storing, and accessing by public authorities? The implications and trade-offs of today's government data collection activities have been discussed extensively in the aftermath of the revelations by Edward Snowden and are still in the process of discussion (most prominently and forcefully Greenwald 2014). In this contribution, I would like to focus on the time dimension and the potential implications of today's information collection for future periods.[6]

[6] For a discussion of the role of information over time and an information life cycle perspective see, e.g., Ambrose (2013).

3.3 Endogenous institutions and „sticky information"

Political institutions are in one way or another chosen by the polity and they evolve over time (e.g., North 1990, Aghion, Alesina and Trebbi 2004, Greif and Laitin 2004). The endogeneity of institutions such as democracy, the rule of law, etc. to the information generation and handling capabilities provided by current information technologies is especially problematic given that people are willing to disclose information on the basis of the current legal system and institutions. There is a high degree of uncertainty in how institutions will evolve. At the same time information becomes more and more "sticky". By "sticky" I refer to the fact that all information, once disclosed, is potentially somehow and somewhere saved and stored for extended periods of time and accessible to public authorities. If institutions change over time (due to the aforementioned incentives arising from the enhanced technological capabilities), while information becomes "sticky", the future use of such information (and potential individual cost of such use) becomes highly uncertain and difficult to forecast.

Can individuals deal in accurate ways with such high levels of uncertainty? Individuals might react in various ways:

First, individuals might be highly myopic (i.e., time inconsistency that involves discounting future utility more strongly than predicted by standard expected utility theory) and, hence, they do not care today about future costs. In this case, individuals freely (and carelessly) provide information. The individual time inconsistency and hence, ignorance of potential future costs of today's information provision (maybe even under the pretext that "I'm too unimportant and I have nothing to hide") fosters the accumulation of power of public authorities without further thinking about restricting such powers.

Second, individuals might face a massive collective action problem and behave like free riders in their individual consumption of goods and provision of information. This means that individuals cannot collectively organize to prevent the abuse of individual and private information by public authorities. Individuals will hence behave like free riders and use all the beneficial services, while arguing that they, individually, are too unimportant and themselves too small to take action against a public authority amassing power. They wait for others to organize and bear the cost of resisting an ever more powerful public authority, while privately benefiting from services requiring personal information – the source of this ever growing power.

Third, individuals reduce their provision of information, reduce their consumption of services requiring personal information and thus, renege on the realization of beneficial transactions.

Fourth, individuals organize and overcome the collective action problem to find ways of restricting future abuse of today's information.

3.4 Preventing future abuse of today's information

What are the legal and technical ways of restricting the future abuse of today's information? Are there automatic and credible "forgetting" mechanisms for information, such as providing information with an "expiry date" (Mayer-Schoenberger 2009)? What are the options given the political and legal institutions today? While neglecting the technical solutions to these questions (leaving them to more competent people), I would like to focus on a few (random) thoughts, some more abstract, and some more specific but potentially not achievable.

We are only at the beginning of this "digital revolution". The technical capabilities must be accompanied by a vivid public debate on the limits of public authority and the required checks and balances. The revelations by Edward Snowden and others have sparked a debate and increased public awareness of the issue. Whatever position one takes on these individuals and their motives, we have to acknowledge that the greater public was not aware of the massive data collection efforts, the relatively untargeted collection of data on a large population of citizens (and as a reminder: the principal), and the potential for abuse (at least looming in the background). Therefore, institutional and legal reforms are required to adjust the political and legal system to prevent future (and further) abuse of these new powers going hand-in-hand with technological progress.

A more specific approach is to think about designs of public data collection and storage that reduce the risk of abuse. Obviously, these thoughts only apply to officially gathered information and not to the unofficial information collected by the shadow-organizations of secret services, etc. Effective and credible oversight and limitation of these services requires taking fundamental political decisions and must be subject to the aforementioned discussions and institutional and legal reforms. But protecting citizens from the abuse of officially (and legally) collected information is also in order. One simple idea is to translate the concept of the separation of powers (e.g., Locke 1689, de Secondat (Baron Montesquieu) 1748, Madison 1787, Persson, Roland and Tabellini 1997) to the handling of information in the hands of the public authority. The main idea is to separate the information that is required at some point in time to provide public goods and services from past information, which is still useful (and might be abused according to the previous arguments), but not necessary for the workings of government. An information system could have three components:

Public administration – current working data: This is the system in which current information is stored to process the information needed by the administration to provide public services: e.g., the tax administration might need documents and information on the current income, wealth, etc. of natural and legal persons. This information could potentially even be uploaded, updated and/or complemented by citizens themselves. All or just some of the information which is stored in this current working directory might also be made accessible to the respective

individuals (potentially with the right to edit certain information).[7] The file would contain all necessary and collected information on an individual from the present back to the near past (say, two years). If there were concerns about connecting and storing all the information in one place, separate current working directories might be beneficial (e.g., to prevent the connection of tax and health data) and the time frame might vary for different services. So far, this is not very dissimilar from the current situation with the exception that today's working data is not restricted to contain only required information in a pre-specified and limited time frame.

Independent data archive – archived past data: A complementary system could archive all information older than a certain threshold (say again two years for the sake of the argument). Expired information of the current working directory would then be automatically transmitted to this independent data archive. Again, if judged necessary and useful, there could be separate archives for information that should not be connected. All information in this archive is anonymized and only identifiable with some ID number that connects the different pieces of information of anonymous individuals over time. The data archive should be outsourced to an independent public agency in order to guarantee that the public administration does not have direct access to the anonymized archives (as there might be concerns that the anonymization could be circumvented given sufficient data points). Under certain restrictions parts of such archives could potentially be made accessible for statistical purposes or academic research.

Judiciary – the key holder: Connecting the archived information to a real person would require a key which enables the link between the data archive and a database containing the personal information including the aforementioned ID. Such a database containing the key to identify real persons (personal ID) could be under the control of the judiciary that would only provide the key to access some specific individual's information after carefully evaluating the case given all standard procedures in developed legal systems.

Certainly, there might be more elaborate ideas and concepts on how to control and/or restrict the information access of public authorities. The questions of which individuals or authorities get access to what information and under what circumstances seem to be the key here. Given that information becomes more and more important for the provision of private and public goods, information will be collected and stored. Therefore, we have to carefully think about information storage and access rights today.

---

[7] The details of who can gain access to what information is complex and as such already today a major issue. It seems important that the rules are clearly specified *ex ante* and access is limited to those public agents who require the information to fulfill their duties. The discussion of these details is, however, beyond the scope of this contribution.

4 Is the quality of information endogenous?

Of course the quality of information that is available on individuals, firms, etc. is endogenous to personal or market restrictions. Nevertheless, I want to stress two issues in the context of this article which warrant some explicit discussion.

First, when thinking about a general right of natural (and potentially to some extent even legal) persons to decide over what information is "remembered or forgotten" in the digital age one has to take into account that such a right directly affects the quality of information that is (or remains) available. Moreover, if the information can be altered *ex post* at will, the incentive to optimize information provision *ex ante* diminishes (see discussion in section 2).

Acknowledging the fact that individuals provide information to consume goods and services (private and public), and given the fact that information flows are difficult to control, that information might spread to unintended addressees, and that institutions holding authority might gain access to such information, individuals will develop new strategies in protecting and managing the data available on them. It is important to remember that an individual's behavior typically changes with the evolution of the environment it lives in and the restrictions it encounters.

Obviously, individuals want some, typically positive, information to be public (e.g., university qualifications, and other successes) and to keep some information undisclosed (e.g., bad credit scores). The more that information can be "managed" (i.e., altered *ex post*) to serve personal interests, the more information asymmetries will occur, and the lower the value of such information. The argument is similar for firms and even more striking. Imagine that firms selling products to consumers over the internet with, say, ebay had the right to delete negative customer evaluations. It is easy to see that such a right would undermine the quality of information on the sellers, and the information signals of customer evaluations would lose credibility.

Information asymmetries serve some and hurt others. Therefore some information should be centralized and to some extent be public, whether individuals or firms want it or not (e.g., credit scores, registers on bankruptcy and debt enforcement, criminal records). Provided that *ex post* alteration of information could become more and more common, the quality of the available information would also become more "endogenous" (i.e. determined by the interests of the parties making information available). Therefore, a general right to decide over the content of the information available to others might have serious adverse consequences.

But still, much information is given without explicitly knowing who will have access to that information and how well such information is protected (e.g., see the current discussions about Facebook's and Google's, etc. information policies). In that respect effective "management" of information by an individual is still very unlikely.

For the sake of the argument, assume for a moment that information provision is the result of rational individual decisions and those individuals become accustomed to the potential dangers and pitfalls of the provision of information in the digital world. Can firms and public authorities still systematically exploit individuals by using their information? It would be hard to believe that individuals would not engage in strategies to increase the cost of taking advantage of such information. The obvious strategy that is widely discussed today is to improve the protection of individual information and laws limiting the exchange of information between firms and other actors without the explicit consent of the relevant individuals. Right now individuals provide (with or without explicit consent) accurate information about their geo-location, their contacts, their comments, etc. to almost any provider of services. Some of the services require such information (e.g., the geo-coordinates for a navigation system), others just collect the information without making direct use for the specific service provided. The enormous amount of accurate personal data collected requires sophisticated programs and models to extract information about a human being's preferences and behaviors. Such programs and models exist and they are becoming more and more accurate and useful for commercial and non-commercial objectives. If this is the case and the protection of this enormous amount of individual information becomes more and more difficult and costly, other strategies will evolve.

One such strategy to increase the costs of using information could be to dilute the informational content of the information. Whoever read the Cold War spy novels by John le Carré knows that it is not only about the accuracy and protection of information but also about *mis*information.[8] This is a second channel showing that the informational content is endogenous. Cleverly designed misinformation increases the cost to anybody who wants to exploit personal information to gain an advantage, be it commercial or non-commercial. It is conceivable that there will be a wide range of misinformation services, maybe in the form of apps for your smart phone, that slowly start sending out artificial information on various parameters.[9] Simulating deviations from your usual patterns or in some cases even random information signals within some parameter space increases the noise in the collected data on individuals. Of course, clever data collectors will improve their algorithms and try to separate noise from real information, but this drives up the cost to extract the truthful signal about human behavior. An important question will be how to spread misinformation while still being able to consume services requiring accurate information for personal use (e.g., navigation services, etc.). Another important

[8] From an opposite perspective Eichenberger and Serna (1990) discuss the information strategies used by government officials (agents) and interest groups (not individual consumers and citizens) to differentially inform different groups of citizens to bias policy decisions. They see the dissemination of *mis*information (or "dirty information") as an effective way to systematically affect the distribution (the variance, not the mean) of beliefs among citizens.

[9] Similar services already exist for search queries on internet search engines, etc. It seems however, that it is not yet acknowledged as a more broad-based strategy for normal citizens to increase the cost to those who collect information on individuals for private gains.

question that will surely surface is that criminals and terrorists might also use such technologies. This is certainly a threat, but at the same time it is exactly these individuals who already today use the technologies that are available. The point I want to make here is that average, normal citizens might start to react to the broad-based data collection efforts by firms and the public authorities. If we believe that even stable institutions in solid democratic countries might be endogenous to the possibilities provided by new technologies (see section 3), then it might be a rational decision of average citizens to use misinformation strategies to increase the cost of surveillance. The consequences are the deterioration of the quality of available information which, of course, comes at an economic cost.[10]

5 Conclusion

Not everything is new in the digital age. What is new is the enormous increase in speed and the potential to spread, to store, and to systematically exploit information. A major challenge will be to confine the accumulation of power in hierarchical relationships such as the relationship between citizens and public authorities. Together with the fact that the information provided today will be available to future governments, technical progress might turn today's (relatively) impartial and inclusive institutions into partial and extractive ones.[11]

It seems important to discuss these issues today and now and to rethink our political and legal frameworks to (partially) anticipate future technical capabilities as well as the incentives of the different players in the markets and in future governments. While this chapter focused somewhat strongly on the potential abuse of the technical capabilities of the digital age, it also has to be noted that the same technologies might increasingly enable citizens and consumers to start protecting themselves from infringements. Economics tells us that technical progress affects economic, political and social development, but it is usually hard to foresee the exact trajectory. Economic forces lead the different players to act and react to the ever changing environment. This makes it difficult to predict today what the right legal frameworks are for the prevention of future aberrations. At the same time, the uncertainties about future developments provide the justifications for government interventions or legal

[10] Just to be very clear, this is by no means an endorsement of what is today called "fake news". It is the simple observation that individuals might resort to misinformation strategies as a reaction to a more invasive governments or firms which collect, store and exploit personal information to the potential detriment of citizens and consumers.

[11] Acemoglu and Robinson (2012) argue that a major reason for the failure of some countries to develop is to be found in the institutional setup. Countries with inclusive institutions (i.e., institutions that give the same rights and access to the political decision making process to the great majority of people) have seen higher growth and better development than countries with extractive institutions (i.e., institutions that include only a small fraction of people, the elite, to the detriment of the majority).

changes. Therefore, legal activism and interventionist policies should be met with caution.

6 Literature

Acemoglu, Daron and James A. Robinson (2012). *Why Nations Fail: The Origins of Power, Prosperity, and Poverty*. New York: Crown Publishers.

Acquisti, Alessandro, Curtis Taylor and Liad Wagman (2016). The Economics of Privacy. *Journal of Economic Literature* 54(2), 442-492.

Aghion, Philippe, Alberto Alesina and Francesco Trebbi (2004). Endogenous Political Institutions. *Quarterly Journal of Economics* 119(2), 565-611.

Akerlof, George (1970). The market for 'lemons': Quality uncertainty and the market mechanism. *Quarterly Journal of Economics* 84 (3), 488-500.

Ambrose, Meg Leta (2013). It's About Time: Privacy, Information Life Cycles, and the Right to be Forgotten. *Stanford Technology Law Review* 16 (2), 101-154.

Arrow, Kenneth (1962). The economic implications of learning by doing. *Review of Economic Studies* 29 (3), 155-173.

Coase, Ronald H. (1960). The Problem of Social Cost. *Journal of Law and Economics* 3, 1-44.

Crawford, Vincent P. and Joel Sobel (1982). Strategic Information Transmission. *Econometrica* 50 (6), 1431-1451.

Eichenberger, Reiner and Angel Serna (1996). Random Errors, Dirty Information, and Politics. *Public Choice* 86, 137-156.

Farrell, Joseph and Matthew Rabin (1996). Cheap Talk. *Journal of Economic Perspectives* 10 (3), 103-118.

Greenwald, Glenn (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books.

Greif, Avner and David D. Laitin (2004). A Theory of Endogenous Institutional Change. *American Political Science Review* 98(4), 633-652

Grossman, Sanford (1981). The informational role of warranties and private disclosure about product quality. *Journal of Law and Economics* 24 (3), 461-483.

Gruber, Jonathan (2012). *Public Finance and Public Policy*. 4th Edition. New York: Worth Publishers.

Koops, Bert-Jaap (2011). Forgetting Footprins, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice. *SCRIPTed* 8 (3), 229-256.

Landes, William M., and Posner, Richard A. (2003). *The Economic Structure of Intellectual Property Law*, Cambridge and London: The Belknap Press of Harvard University Press.

Locke, John (1689). *Two Treatises of Government*. 3rd edition. London: Awnsham and John Churchill.

Madison, James (1787). The Federalist, No 51.

Mankiw, Gregory N. (2011). *Principles of Microeconomics*. 6th edition. Mason, OH: South-Western Cengage Learning.

Mayer-Schoenberger, Viktor (2009). *Delete: The Virtue of Forgetting in the Digital Age*. Princeton, NJ: Princeton University Press.

Meade, Ellen E. and David Stasavage (2008). Publicity of debate and the incentive to dissent: evidence from the US Federal Reserve. *Economic Journal* 118 (April), 695-717.

Milgrom, Paul (1981). Good news and bad news: Representation theorems and applications. *Bell Journal of Economics* 12 (2), 380-391.

North, Douglas C. (1990). *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press.

Persson, Torsten, Gerard Roland and Guido Tabellini (1997). Separation of Powers and Political Accountability. *Quarterly Journal of Economics* 112 (4), 1163-1202

Pindyck, Robert and Daniel Rubinfeld (2012). *Microeconomics*. 8th edition. Upper Saddle River, NJ: Prentice Hall.

Posner, Richard A. (1981). The economics of privacy. *American Economic Review* 71 (2), 405-409.

Prat, Andrea (2005). The wrong kind of transparency. *American Economic Review* 95 (3), 862-877.

Rosen, Harvey S. and Ted Gayer (2013). *Public Finance*. 10th edition. New York: McGraw-Hill.

Schelker, Mark (2011). Wikileaks – wo ist Transparenz sinnvoll, wo schädlich? *Neue Zürcher Zeitung*, February 14, 2011 (Nr. 37): p. 17.

de Secondat, Charles (Baron Montesquieu) (1748). *De l'esprit des lois*. Genève.

Spence, Michael (1973). Job market signaling. *Quarterly Journal of Economics* 87 (3), 355-374.

Stigler, George J. (1962). Information in the labor market. *Journal of Political Economy*, 94-105.

Stigler, George J. (1980). An introduction to privacy in economics and politics. *Journal of Legal Studies* 9 (4), 623-44.

Tresch, Richard W. (2008). *Public Sector Economics*. New York: Palgrave MacMillan.

Thaler, Richard H. and Cass R. Sunstein (2008). *Nudge. Improving decisions about health, wealth and happiness*. Yale University Press, New Haven.

von Hayek, Friedrich August (1945). The use of knowledge in society. *American Economic Review* 35 (4), 519-530.