Joint Discussion Paper Series in Economics

by the Universities of

Aachen · Gießen · Göttingen
Kassel · Marburg · Siegen

ISSN 1867-3678

No. 14-2016

Wolfgang Kerber

Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection

This paper can be downloaded from
http://www.uni-marburg.de/fb02/makro/forschung/magkspapers/index_html%28magks%29

Coordination: Bernd Hayo • Philipps-University Marburg
School of Business and Economics • Universitätsstraße 24, D-35032 Marburg
Tel: +49-6421-2823091, Fax: +49-6421-2823088, e-mail: hayo@wiwi.uni-marburg.de

MACIE PAPER SERIES

Marburg Centre for Institutional Economics

Nr. 2016/3

Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection

Wolfgang Kerber

MACIE, Philipps-Universität Marburg

Marburg Centre for Institutional Economics • Coordination: Prof. Dr. Elisabeth Schulte
c/o Research Group Institutional Economics • Barfuessertor 2 • D-35037 Marburg

Phone: +49 (0) 6421-28-23196 • Fax: +49 (0) 6421-28-24858 •
www.uni-marburg.de/fb02/MACIE • macie@wiwi.uni-marburg.de

Philipps Universität Marburg

Digital Markets, Data, and Privacy: Competition Law, Consumer Law, and Data Protection

Wolfgang Kerber*

February 2016

Abstract

The digitalisation of the economy with data as the new critical resource is a technological revolution which requires an adaptation of the legal framework for markets and the economy. This paper analyzes the privacy concerns in the digital economy from an economics perspective. What can we learn from economics whether and to what extent we need legal rules helping to protect privacy? Particularly important are the complex tradeoff problems between benefits and costs of privacy and disclosure. This paper claims that it is not sufficient to look for policy solutions only in one field of the law, as, e.g. competition law or data protection law, rather an integrated approach from different regulatory perspectives is necessary. This paper focusses on competition policy, consumer policy, and data protection policy as the three main regulatory perspectives that are relevant for privacy concerns. For all three policies it is discussed from an economic perspective how these policies might help to remedy market failures in regard to privacy rights and privacy preferences of individuals, and how a more integrated regulatory approach can be developed.

Keywords: digital economy, Big Data, privacy, data protection, competition law, consumer law

Forthcoming in:
Gewerblicher Rechtsschutz und Urheberrecht.Internationaler Teil (GRUR Int), 2016

* Professor of Economics, Marburg Centre for Institutional Economics (MACIE), School of Business & Economics, Philipps-University Marburg, kerber@wiwi.uni-marburg.de.

I. Introduction

Despite the controversies about competition cases as the European Google search engine case there is a growing awareness that the challenges through the internet, digitalisation, and data analytics are much more fundamental than the concerns that have been raised from a competition perspective in regard to Google, Facebook, and others. It is the collection, generation, analysis, and commercial exploitation of data that is at the core of the digital economy, and it are these data that are the new valuable and critical resource for the competitiveness of firms and entire economies. These data come from many sources: They might be given voluntarily (for "free" services as the use of search services and social networks), might be observed (cookies, tracking web surfing, sensor data) or derived (from other data). Data analytics allow much better predictions about the preferences and behaviour of individuals, more and better innovative products and services, and huge cost reductions for firms as well as new and improved public policies (health, safety, security, and education).[1] However, due to the unprecedented amount of data that are being collected about the behaviour, desires, interests, and opinions of nearly all members of society, there are increasing concerns about the loss of privacy and individual autonomy due to increasingly transparent and predictable human beings. The new (but still not fully enacted) European General Data Protection Regulation is viewed as an important step for better protecting personal data in the EU where privacy is seen as a fundamental right of EU citizens.[2]

The objective of this paper is to analyze the privacy concerns in the digital economy from an economics perspective. Economic analyses of privacy issues are a new but in recent years fast developing field with many theoretical and empirical studies that offer many results which can help to shed at least some light on the complex working of the digital economy.[3] What can we learn from economics whether and to what extent we need legal rules helping to protect privacy, and what kind of regulatory instruments might be relevant for policy solutions? From an institutional economics perspective it is not surprising that this Schumpeterian technological and economic revolution (with all the typical phenomena of "disruptive innovations" and "creative destruction") will also require a broad and deep adaptation and evolution of the legal framework for markets and the economy, both in regard to economic efficiency and in regard to privacy concerns. My claim in this paper is that for addressing properly the concerns about privacy in the digital economy, it is not sufficient to look for policy solutions only in

---

[1] For a brief overview about the importance of data and data analytics in the digital economy, see, e.g., *Dapp/Heine*, Big Data. The untamed force, DB research, May 5, 2014.

[2] *European Commission*, Proposal for a Regulation 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 (General Data Protection Regulation), COM(2012) 11 final.

[3] For overviews see *Acquisti,* The Economics of Personal Data and Privacy, 30 Years after the OECD Privacy Guidelines, OECD Conference Centre 2010, and *Acquisti/Wagman/Taylor*, The Economics of Privacy, Journal of Economic Literature 2016 forthcoming, available at SSRN: http://ssrn.com/abstract=2580411.

one field of the law, as, e.g. competition law or data protection, but that an integrated approach from different regulatory perspectives is necessary. In this paper I want to focus on competition policy, consumer policy, and data protection policy as the three main regulatory perspectives that can be deemed relevant for privacy concerns.[4] For all three policies it will be discussed from an economic perspective how these policies might help to remedy market failures in regard to privacy rights and privacy preferences of individuals. This will also include brief discussions of policy proposals that have emerged in these fields of the law. Economic analyses are necessary for a better understanding of the manifold tradeoffs between the benefits and costs of disclosure and nondisclosure of information, both for individual persons and the society.

The paper is structured as follows. Section II provides a brief overview about the economics of privacy and important results about the effects of Big Data and privacy on firms and consumers as well as an analysis of potential market failures in regard to the fulfillment of privacy preferences of consumers. Section III to V analyze step by step the privacy problems from a competition policy, a consumer policy, and a data protection perspective. In each section current policy proposals about remedying privacy problems are discussed as well as the need for further legal developments and research. Some general conclusions follow in section VI.

II. Economics of Privacy and Regulatory Perspectives

Privacy is a difficult and complex concept. It is seen as deeply rooted in human dignity and autonomy, linked to the protection of personal space, and often operationalized as a right to safeguard and control personal information. It can also be interpreted as drawing boundaries between the spheres of the private and the public.[5] However the delimitation between both spheres is also a normative question that can be subject to controversial discussions and might also depend on culture and religion. In the European Union privacy is seen as a fundamental right. Its basic idea is that persons should have control about their personal data.[6] This is closely linked with the notion of "informational self-

[4] See also *Monopolkommission*, Competition policy: The challenge of digital markets, Special Report No. 68, 2015, and *European Data Protection Supervisor,* Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, Preliminary Opinion 2014. Both emphasize the combination of policy instruments from competition, consumer and data protection law.

[5] See as overview *Acquisti/Wagman/Taylor*, (fn.3), 1; seminal contributions are *Warren/Brandeis*, The right to privacy. Harvard Law Review 1890, 193, *Westin*, Privacy and Freedom (1967), and *Schoeman*, Privacy and social freedom (1992).

[6] See Art. 7 and 8 of the Charter for Fundamental Rights, the Directives 95/46/EC ("Data Protection Directive") and 2002/28/EC as well as the planned General Data Protection Regulation (fn.2).

determination" developed by the German Federal Constitutional Court.[7] Economists are well-equipped to analyze privacy issues, because this informational approach to privacy allows them to use information economics with its focus on analyzing the effects of different information distributions (as information asymmetries), and of incentives for producing, disclosing, and signalling information. However, it has to be kept in mind that economic analysis usually focusses only on welfare effects, which might not always grasp sufficiently the normative dimension of privacy as a fundamental right. Therefore tensions and tradeoffs between the protection of privacy (as a legal normative concept) and economic efficiency can emerge.[8]

In the following, a brief overview is presented about important preliminary results of theoretical and empirical economic studies about privacy in the digital economy.[9] From an economic perspective, the value of privacy for individuals can be derived either from their preferences for privacy (privacy as final good) or from other advantages of keeping information private (privacy as an intermediate good), e.g. for not getting harmed or discriminated. Often individuals have incentives for revealing private information, e.g., for using "free" services as a search engine or for getting lower rates on insurance markets (e.g., in regard to the healthiness of their life style). Acquisti shows that both the disclosure and non-disclosure of data can have benefits and costs for the subjects of the data as well as the firms that hold the data.[10] Through voluntary and involuntary revealing of private data, e.g. through tracking websurfing behaviour, Big Data allows firms to have much more information about the preferences and behaviour of their customers. Whereas this enables firms to offer new and better-matching products and services (which increases welfare), there are also serious concerns that this new information distribution can also enable firms to pursue strategies that might harm consumers (according to the old insight that information is power and therefore also might have distributional effects). Therefore it is one of the main research questions whether and under what conditions this different information distribution can have negative effects on consumers and generally on welfare.

One of the crucial differences between online and offline markets is that online markets allow personalised pricing in real time, i.e. that prices through price-setting algorithms can change constantly and that different persons can be offered different prices at the same time. If Big Data leads to sufficient information to predict the willingness-to-pay of individual customers, then personalised pricing might allow first-degree price discrimination with the possibility that firms can appropriate the entire consumer rent by setting prices according to the willingness-to-pay of their individual customers. Therefore

---

[7] Federal Constitutional Court (Bundesverfassungsgericht), Judgement of 15 December 1983, 1 BvR 209/83 and others - Census, BVerfG 65, 1.

[8] For example already *Posner*, The right of privacy, Georgia Law Review 1978, 393, emphasized that privacy (as non-disclosure of relevant information) can lead to economic inefficiencies.

[9] For overviews see *Acquisti/Wagman/Taylor* (fn.3), *Acquisti* (fn.3).

[10] *Acquisti* (fn.3).

one of the first lines of research has focussed on price discrimination. However, the results of theoretical models show the complexity of the effects of more information about customers. In economic models with two periods, in which customers reveal with their buying decisions their willingness-to-pay in a first period, this information (buying history) can be used for personalised pricing in the second period. In such settings economists can show that it depends on a number of conditions whether this additional information leads to higher or lower profits of firms, and harms or even benefits consumers. If the customers are not aware that the firms use the buying history ("naive" customers) and the firms have a monopoly, then this information increases profits by appropriating more (and theoretically all) consumer rents. However, under competitive conditions the same information can lead to more competition between firms for the different customers and therefore lower profits and lower prices. As a consequence, having more information about the customers is not always beneficial for the firms. These models also show that in competitive settings the existence of sophisticated customers, which take into account the future use of revealed information by firms, might lead to higher prices and less welfare due to the costs of the strategic non-revealing of information by these customers. Therefore protecting this private information about willingness-to-pay might not always lead to a better outcome for consumers or increase social welfare.[11] However, the empirical studies about price-discriminating behaviour, e.g. in the airline industry, show so far only a limited application of sophisticated price discrimination strategies on the basis of more data about the customers.[12]

Beyond this price discrimination issue economic studies have addressed a number of other questions in regard to data and privacy in digital markets. Important topics are marketing techniques (with targeted advertising and e-commerce), data intermediaries, and markets for privacy and personal data.[13] What general conclusions can be drawn from this research so far? For all three topics the results sug-

---

[11] See as an overview about the results of these models about behaviour-based price discrimination *Fudenberg/Villas-Boas*, Price Discrimination in the Digital Economy, in: Peitz/Waldfogel, Oxford Handbook of the Digital Economy (2012), 254; important contributions are *Fudenberg/Tirole*, Customer poaching and brand switching, RAND Journal of Economics 2000, 634, *Villas-Boas,* Dynamic competition with customer recognition, RAND Journal of Economics 1999, 604, *Villas-Boas,* Price cycles in markets with customer recognition, RAND Journal of Economics 2004, 486, *Taylor,* Consumer privacy and the market for customer information, RAND Journal of Economics 2004, 631, *Acquisti/Varian*, Conditioning prices on purchase history, Marketing Science 2005, 367; see also *Acquisti/Wagman/Taylor* (fn.3), 14-16. For a deeper analysis of criteria when personalised pricing might be a problem for consumers and welfare see *OFT*, The economics of online personalised pricing (2013).

[12] See, e.g., *Escobari/Rupp/Meskey*, Dynamic Price Discrimination in Airlines, available at ssrn.com/abstract=2248124, 2013, *Mikians et al.*, Crowd-assisted search for price discrimination in e-commerce: First results. Proceedings of the Ninth ACM Conference on Emerging Networking Experiments and Technologies 2013, 1, *Vissers et al.*, Crying wolf? On the price discrimination of online airline tickets. Proceedings of the 7th Workshop on Hot Topics in Privacy Enhancing Technologies 2014, 16.

[13] See *Acquisti/Wagman/Taylor* (fn.3), 17-20.

gest that it depends on the specific conditions of the markets whether economically efficient solutions occur or serious market failures emerge, and whether legal protections of privacy will have positive or negative effects on consumers and welfare. For example, in regard to marketing techniques, privacy protection that prohibits the collection of personally identifiable data and therefore impedes selective targeting of consumers might have positive or negative effects on consumers, depending on their being naive or sophisticated and on the intensity of competition.[14] Many large data holders as Google and Facebook can be viewed as data intermediaries on multi-sided markets. For these markets research has shown that the firms on these markets (intermediaries and advertisers) often do not have optimal incentives for matching products with consumers (suggesting some degree of market failure).[15] The problem why so far no well-functioning markets for privacy and personal data exist that respect the privacy rights and preferences of the individuals will be discussed in more detail below. One of the important lessons from these economic studies is that no general conclusions can be drawn whether privacy protection is generally beneficial or detrimental to individuals or society.[16] This leads to the conclusion that due to the complexity of the effects of information distributions on digital markets, specific economic analyses are necessary for identifying where privacy protection is helpful and how it should be designed.

One of the big puzzles of the privacy in the internet topic is the well-established empirical fact that in surveys a large majority of internet users are very concerned about their private data on the internet,[17] but that an analysis of the actual internet behaviour of many users show that that they often are not cautious about disclosing private information and also do not use enough privacy-enhancing technologies. This privacy paradox has led to a number of empirical studies and different attempts for its interpretation and explanation.[18] It is directly related to the questions about the value of data and the value

---

[14] *Hoffmann/Inderst/Ottaviani*, Hypertargeting, limited attention, and privacy: Implications for marketing and campaigning, Working Paper 2013; other questions refer to the link between unsolicited marketing, spamming, targeted advertising and privacy; see, e.g., *Tucker*, Social networks, personalized advertising, and privacy controls. Journal of Marketing Research 2014, 546.

[15] See in more detail *Acquisti/Wagman/Taylor*, (fn.3), 17-19, with many references.

[16] This is one of the main conclusions of *Acquisti/Wagman/Taylor*, (fn.3), 2, in their broad survery article about the economics of privacy.

[17] See for a US survey that 68% of adults think their online privacy is not enough protected by existing laws *Rainie et al.*, Anonymity, privacy, and security online. Pew Research Center 2013.

[18] The literature about the privacy paradox is huge; see, e.g., *Berendt/Gunther/Spiekermann*, Privacy in e-commerce: stated preferences vs. actual behavior, Communications of the ACM 2005,101, *Dinev/Hart*, An extended privacy calculus model for e-commerce transactions, Information Systems Research 2006, 61, *Norberg/Horne/Horne,* The privacy paradox: Personal information disclosure intentions versus behaviors, Journal of Consumer Affairs 2007, 100; for a very careful overview and analysis of the many (partly also experimental) studies and interpretations of the effects in regard to the information privacy paradox see *Kokolakis*, Privacy attitudes and privacy behavior: A review of

of privacy, i.e. the willingness-to-pay of users for not revealing private information.[19] The studies have led to the following results: (1) Privacy behaviour seems to be very context-specific, i.e. it depends on the specific circumstances, whether users are willing to disclose information, what type of information (health data, location data etc.), and to whom. (2) Privacy preferences are heterogeneous, i.e. users can differ considerably in their preferences for disclosing (what type of) private information and to whom.[20] (3) It is also empirically well-confirmed that many users are not aware of the extent of the collection of data and the extent of their being behaviorally targeted based upon these data.[21] (4) A number of studies have also confirmed the relevance of bounded rationality and behavioral decision-making biases in regard to such privacy decisions.[22] The possible conclusions from this privacy paradox and these studies vary widely. However, the intransparency of the extent of the collection of data and the uncertainty about their future use, which does not allow predictions about the long-term costs of disclosed and collected data, have led to the conclusion that many internet users might have serious problems to protect their privacy according to their preferences.

From an economic policy perspective, we can ask whether digital markets fulfill the privacy preferences of the individuals or whether there might be serious market failure problems that call for regulatory remedies. Especially the examples of Google and Facebook with their often alleged dominant market positions have raised the question whether weak competition might lead to an excessive collection of private data and to an insufficient provision of privacy options for fulfilling the different privacy preferences of users.[23] For example, it can be claimed that a well-functioning market would offer much more different privacy options, i.e. more specific opt-in and opt-out solutions for data collecting as well as an option for using the Google search engine or Facebook also with a monthly subscription

---

current research on the privacy paradox phenomenon, Computers & Security 2015, available at https://www.researchgate.net/publication/280244291.

[19] For studies about the monetary value of privacy and personal data, see *Acquisti/Wagman/Taylor*, (fn.3), 38-39.

[20] For differences in regard to persons, types of data, and data recipients, see *Acquisti/Wagman/Taylor*, (fn.3), 5, *Staiano et al*, Money walks: a human-centric study on the economics of personal mobile data, UbiComp '14 Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing Pages 2014, 583.

[21] *McDonald/Cranor*, Beliefs and behaviors: Internet users' understanding of behavioral advertising, Proceedings of the 2010 Research Conference on Communication, Information and Internet Policy 2010, *Acquisti/Wagman/Taylor* (fn.3), 6.

[22] See *Acquisti*, Privacy in electronic commerce and the economics of immediate gratification, Proceedings of the 5th ACM conference on Electronic commerce 2004, 21, *Acquisti/Grossklag,* What can behavioural economics teach us about privacy? in: Acquisti/Vimercati, Digital Privacy: Theory, Technologies and Practices, (2007), 363, *Borgesius*, Behavioural Sciences and the Regulation of Privacy in the Internet, in: Alemanno/ Sibony, Nudge and the Law (2015), 192, and the survey in *Kokolakis* (fn.18).

[23] See *Monopolkommission* (fn.4), para. 306-311.

fee without the collection of data and/or advertising. A second market failure concern is that the intransparency about the collection and use of private data does not allow the users to make well-informed rational decisions in regard to their privacy behavior on the internet leading to market failures due to information asymmetry and behavioral biases. Other possible market failures refer to externalities in regard to the disclosure and transfer of data[24] and to the lack of properly defined and protected property rights of personal data.[25] In the following, we will discuss step by step competition law, consumer law, and data protection law as policies which might help to remedy market failures in regard to privacy and to protect privacy as a fundamental right.

III. Competition Law

To what extent can competition law help to solve privacy problems on the internet? Competition law has the objective of protecting effective competition, i.e. to protect consumers from harm through anti-competitive behaviour. Both Google and Facebook are viewed as potentially dominant firms, and there is also much discussion about the market power of EBay, Amazon, and Apple.[26] In competition economics the theory of platform (or multi-sided) markets has shown that competition between platforms can be difficult due to often large direct and indirect network effects between different market sides, and economies of scale. Although other factors as multihoming, platform differentiation, and congestion might facilitate competition between platforms, particularly large indirect network effects can lead to a natural monopoly situation with only one dominant platform, which however also can be an efficient solution.[27] In regard to search engines and social networks such a market position might be additionally protected by high entry barriers, especially through the large amount of data collected in the past, which allows for a higher quality of the services of the incumbent platforms.[28] Although it is true that the huge technological progress in digital markets can undermine also very strong market positions of firms, it cannot be denied that due to the network effects and entry barriers it might be very difficult to challenge the market positions of firms like Google and Facebook. Therefore there are serious concerns and discussions about competition problems in the digital economy, how competition

---

[24] For example, negative externalities can emerge through sharing of disclosed data with others, whose effects might not be internalised. See, e.g., *Swire/Litan*, None of Your Business - World Data Flows, Electronic Commerce, and the European Privacy Directive. Washington 1998.

[25] See below section VI.

[26] See *Monopolkommission* (fn.4), para.188-220, 293-305; *Haucap/Heimeshoff*, Google, Facebook, Amazon, eBay: Is the Internet Driving Competition or Market Monopolization?, International Economics and Economic Policy 2014, 49.

[27] *Evans/Schmalensee,* The Industrial Organization of Markets with Two-Sided Platforms, Competition Policy International 2007, 151, and *Monopolkommission* (fn.4), para. 30-63.

[28] *Argenton/Prüfer*, Search Engine Competition With Network Externalities, Journal of Competition Law & Economics 2012, 73.

authorities should deal with them, and whether current competition laws are sufficient or should be amended.[29]

How does this discussion relate to privacy problems? The well-known competition cases, as, e.g., the European Google search engine case or the Google Android investigation do not focus on abusive behaviour in regard to privacy but on exclusionary behaviour in regard to competitors and leveraging market power to other markets, as in the Google search engine case through the alleged favoring of own services in the search results ("search bias").[30] However the negative effects of weak competition between platforms on the privacy of customers are increasingly discussed. A first important step was the recognition that the services of search engines and social networks are not "free" but paid with the data and the privacy of the users.[31] The interpretation of the price as the extent that private data are collected and commercially used allows the application of competition economics in regard to the analysis of data collection as price-setting behaviour and also the application of competition law in regard to data collection behaviour. One important question refers to the problem why we do not observe more competition in which firm compete with offering privacy-friendly solutions.[32] However from a competition economics perspective it is not surprising that the weak competition between platforms with the consequence of potentially dominant firms would allow them to collect more data and offer fewer privacy options than under effective competition. The lack of options to switch to qualitatively similar other search engines or social networks might lead users to accept also very high prices (in form of collected data) and privacy policies that do not match their specific privacy preferences. Therefore the well-known competition problems on the internet can also lead to privacy problems and thus harm consumers.

What solutions are discussed from a competition law perspective? One group of solutions try to solve the problem of weak competition among internet platforms in order to increase the incentives of the firms to offer their services in a more privacy-friendly way, e.g. by being more responsive to the heterogenous privacy preferences of their customers. This might include more choice through product differentiation within and between firms in regard to privacy protection (i.e., offering more privacy options) but also "price" competition in form of less data collection as price for using the "free" services. The option of granting access to the already accumulated data of a dominant platform (as an essential facility) to other competitors for eliminating a huge entry barrier might admittedly help competition but

---

[29] For this discussion see the German *Monopolkommission* (fn.4), and *Bundeskartellamt*, Digitale Ökonomie - Internetplattformen zwischen Wettbewerbsrecht, Privatsphäre und Verbraucherschutz 2015.

[30] See *European Commission*, press release MEMO/15/4781, 15 April 2015, *Körber*, The Commission's "Next Big Thing"?, NZKart 2015, 415, *Monopolkommission* (fn.4), para. 248-257.

[31] *European Data Protection Supervisor* (fn.4), 10.

[32] *European Data Protection Supervisor* (fn.4), 33.

can be seen critically from a privacy protection perspective due to the further spreading of private data.[33] A less problematic solution and often recommended solution is the introduction of a right for data portability of users, which through the reduction of switching costs might lead to more competition between platforms (especially in regard to social networks).[34] Another group of proposals tries to deal with excessive data collection by using the notion of exploitative abuse of dominant firms according to Art. 102 TFEU. From that perspective excessive data collection could be challenged directly as exploitative "price" abuse. Also the non-provision of enough transparency about data collection and insufficient privacy options can be seen as abusive behaviour.[35] The German Monopolkommission discussed whether also the violation of individual rights, both in regard to privacy and in regard to intellectual property, might be an exploitative abusive behaviour according to Art. 102 TFEU.[36] However, the difficulties of applying these solutions in current competition law, esp., also in regard to proving market dominance and establishing clear criteria for exploitative abuse in regard to data, raise serious questions about their implementability.[37] Therefore it is a bold step that the German Bundeskartellamt initiated on March 2, 2016 a proceeding against Facebook, in which it investigates whether its specific terms of service on the use of user data might be an abuse of a dominant position in the market for social networks. The direction of the investigation focusses on the question whether the terms and conditions of Facebook that violate data protection provisions might be an abusive imposition of unfair conditions on users.[38]

IV. Consumer Law

From an economic perspective it is the task of consumer policy to remedy market failures through information and rationality problems of consumers. Both information economics and behavioral economics offer a wide range of theoretical or empirical insights why and under what conditions consumers might make wrong decisions due to information problems and behavioral biases. Consumer edu-

---

[33] For such a proposal see *Argenton/Prüfer* (fn.28); see also *Monopolkommission* (fn.4), para. 275-280.

[34] *Monopolkommission* (fn.4), para. 105-106. The new General Data Protection Regulation would facilitate data portability.

35 Monopolkommission (fn.4), para. 326-329, *Gebicka/Heinemann*, Social Media & Competition Law, World Competition 2014, 149.

[36] *Monopolkommission* (fn.4), para. 514-528.

[37] Increasingly discussed are also the possibilities how to take into account large data pools in merger proceedings, and the competition problems that might arise, because firms that violate privacy rights or intellectual property rights might gain an unfair competitive advantage (see *Monopolkommission* (fn.4), para. 523-525). For a proposal to solve gaps in regard to the control of mergers in the digital economy with low turnovers but large valuable data pools (Facebook/WhatsApp) see *Monopolkommission* (fn.4), para. 109, 453-463.

[38] Bundeskartellamt, press release March 2, 2016.

cation, nudging instruments (as default rules), labelling and information disclosure duties, as well as minimum standards for products, services, and qualifications are part of the toolbox of consumer policy for solving these market failure problems.[39] Since intransparency about the collecting of data and uncertainty about the use of these data and the potential long-term future costs for the users are one of the major reasons for privacy concerns on the internet, consumer policy might be very suitable for solving privacy problems of internet users. Since European consumer law has the objectives of protecting the health, safety, and economic interests of consumers, it also protects the privacy of consumers as part of their economic interests and safety but also as their fundamental right.[40]

The difficulties for internet users of coping with privacy due to information problems and behavioral biases have already been discussed in the context of the privacy paradox in section II. One part of the problem is that often the users are intentionally kept uninformed or misled about the extent of the tracking of their behaviour. If the users do not know how their data are collected and how the data holders use these data, then even sophisticated consumers cannot protect themselves against these breaches of privacy. This leads to the questions to what extent secret collecting of data (e.g. through tracking with cookies and web bugs) should be prohibited, and if allowed whether there should be a duty for informing users of a service or a website about the data collection.[41] Another part of the problem is that there are a lot of empirical studies and much critical discussion about the question whether the (in the meantime far-spread) solution of "notice and consent" works, i.e. that the users are informed about the "privacy policies", and implicitly consent to them by using the service or the website. These studies show the problems and limitations of these information solutions. The main problems are that the privacy policies are often vague and unclear in regard to the collection and use of data, that it is too costly to read the privacy policies (due to their length and often incomprehensible legal language), and that there are a number of behavioral decision-making problems, as, e.g., framing effects, myopia, and status quo bias.[42] Therefore many scholars have serious doubts about the capa-

---

[39] For consumer policy and its toolbox of instruments see *Luth*, Behavioral Economics in Consumer Policy. The Economic Analysis of Standard Terms in Consumer Contracts (2010), *OECD*, Consumer Policy Toolkit 2010, and for EU consumer law *Weatherill*, EU Consumer Law and Policy, 2. ed. (2013).

[40] See also *European Data Protection Supervisor* (fn.4), 23-26.

[41] See for these questions the so-called EU ePrivacy Directive (2002/58/EC) and EU Cookie Directive (2009/136/EC) which permit the use of cookies if the users give their opt-in consent, whereas in the US the Do-not-track proposal of the FTC (Federal Trade Commission) in 2012 follows an opt-out approach. See *FTC*, Protecting Consumer Privacy in an Era of Rapid Change, FTC Report March 2012, and for the EU *Luzak*, Privacy Notice for Dummies? Towards European Guidelines on How to Give “Clear and Comprehensive Information” on the Cookies’ Use in Order to Protect the Internet Users’ Right to Online Privacy, Journal of Consumer Policy 2014, 547.

[42] See, e.g., the overviews in *Acquisti/Wagman/Taylor*, (fn.3), 40, *Borgesius* (fn.22), *Bechmann,* Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook, Journal of Media Business Studies 2014, 21, *Luzak* (fn.41) for the specific problem of consent to cookies, and *McDon-*

bility of such transparency solutions for solving the privacy problems, because they might not fulfill the requirements for leading to well-informed choices by consumers.[43]

In the recent literature a large number of solutions have been discussed. Giving not enough clear and intelligible information about the collection and use of data can be an unfair commercial practice, violate consumer rights, or can be misleading advertising, e.g. if a service is described as "free" (despite paying with private data) - in addition to violating data protection laws. Therefore different consumer law regulations can be used for requiring much more and detailed information about the extent but also the specific use of data, i.e. minimum standards for information and its intelligibility can be defined.[44] Also standard form contract law can be used for monitoring and limiting the extent that service providers can get general consent to the use of private data through the consent to the privacy terms in standard form contracts.[45] A closely linked proposal refers to the requirement to offer privacy-friendly default rules in these privacy policies in order to help users through nudging to make better choices in regard to the protection of their privacy.[46] One step further go proposals about an obligation to offer certain internet services (search engine, social network) with much more privacy options, as, e.g., also with a subscription fee but without the collection of private data (or without advertising).[47] Then users would have much more choice to use a service with or without the collection of data, or with or without advertising, and different monetary payments. This might lead to a better fulfillment of heterogenous privacy preferences. Other solutions are the use of more opt-in instead of opt-out solutions as well as the introduction of a right to data portability for weaking the lock-in of consumers.[48]

It is particularly interesting that the interfaces between competition and consumer law are increasingly discussed in regard to privacy problems on the internet. Asking for a sophisticated combination of competition and consumer policy solutions can also be supported from an economic perspective, because the two different market failures, competition problems on one hand and information and rationality problems on the other hand, can reinforce themselves mutually. Weak competition between plat-

---

ald/Cranor, The cost of reading privacy policies. I/S: A Journal of Law and Policy for the Information Society 2008, 540, for the costs of reading privacy policies.

[43] See, e.g., *Solove*, Introduction: Privacy self-management and the consent dilemma. Harvard Law Review 2013, 1880, *European Data Protection Supervisor* (fn.4), *Luzak* (fn.41), *Borgesius* (fn.22), *Monopolkommission* (fn.4) 308-310. For the legal requirements of "informed consent" in the EU, see *Luzak* (fn.41), 548-549, and *Borgesius* (fn.22), 182-188.

[44] See in more detail *European Data Protection Supervisor* (fn.4), 24-25.

[45] *Monopolkommission* (fn.4) para. 339-341.

[46] For nudging solutions see *Wang et al.*, The second wave of global privacy protection: From Facebook regrets to Facebook privacy nudges. Ohio State Law Journal 2013, 1307, *Borgesius* (fn.22), 200-201, and *Monopolkommission* (fn.4), para. 283, in regard to privacy-friendly default rules.

[47] *Monopolkommission* (fn.4), para. 338, *European Data Protection Supervisor* (fn.4) 35.

[48] *Monopolkommission* (fn.4), para. 103-106.

forms can reduce the competitive pressure for disclosing information about the collection and use of data, and, vice versa, the intransparency and lack of information of consumers can dampen the intensity of competition due to a lack of comparability. An integrated competition and consumer law strategy can include also the use of typical consumer policy solutions in competition law remedies, as, e.g., minimum options for privacy (by offering users a paid service with minimised collection and retention of personal data), proportionate limits to the retention of customer data, or ensuring data portability between service providers.[49] At the same time a stricter application of consumer policy instruments might be necessary on those digital markets, in which there are simultaneously serious competition problems.

V. Data Protection and Privacy Laws

Crucial for privacy on the internet are certainly also data protection and privacy laws that directly protect the personal data of citizens. The widely agreed on but still not enacted new EU General Data Protection Regulation has the task of enforcing the fundamental right of EU citizens for the protection of personal data and facilitating the creation of the European internal market by overcoming the fragmentation of national data protection laws in the EU.[50] Basic principles of the European data protection law are the principles of consent, data minimization, purpose limitation, the rights of data subjects (information, access, rectification, right to be forgotten and erasure, data portability) as well as restrictions for profiling. However, the proposed regulation also stipulates that data protection is not an absolute right, but must be considered in relation to its function in society, and must be balanced with other fundamental rights.[51] One of the huge challenges for the protection of privacy in the world-wide internet is that the EU and the US have very different policy approaches in regard to privacy and data protection. Whereas in the US the collection, trade, and use of personal data is widely allowed, the EU is much more restrictive, to what extent what kinds of data are allowed to be collected, and how they can be stored, processed, and used for what kind of purposes.[52] Despite concerns about the compliance costs of data protection laws and the impact of strict data protection for the international competitiveness of European firms, there seems to be a broad consensus in both the public and academic

---

[49] *European Data Protection Supervisor* (fn.4), 32, *Monopolkommission* (fn.4), para. 336-342.

[50] *European Commission* (fn.2).

[51] *European Commission* (fn.2), Recital 139; for the principles see *European Data Protection Supervisor* (fn.4), 11-16, and the references in fn.52.

[52] For the different approaches to data protection and privacy in the EU and the U.S., see *Rubinstein*, Big Data: The end of privacy or a new beginning, International Data Privacy Law 2013, 74, *Tsesis*, The right to erasure: Privacy, data brokers, and the indefinite retention of data, Wake Forest Law Review 2014, 433, *Gautam*, 21st century problems: Will the European Union data reform properly balance its citizens' business interests and privacy?, Southwestern Journal of International Law 2015, 195.

debate that the new European Data Protection Regulation will be a huge progress and its implementation will help protecting the privacy of the EU citizens.[53]

How can data protection laws be interpreted from an economic perspective? What kind of market failure do they try to remedy? Since data protection laws in Europe were initially seen as a defence against privacy violations of the state, they are rooted mainly in public law, and were only later extended to the collection and processing of personal data in business contexts. From an economic perspective data protection laws can be linked to two kinds of market failure and the additional normative objective of protecting privacy as a fundamental right. Many data protection problems in regard to privacy on the internet are the same we already discussed in regard to consumer law, namely market failures due to information and rationality problems of consumers and internet users. Therefore it is not surprising that many issues that are brought up and legally challenged by data protection supervisors use reasonings that are very similar to those in consumer policy. Therefore it is not surprising that to a large extent also the same policy solutions are discussed as, e.g., more transparency about the collection and use of data or limiting the collection of data, offering more privacy options, or rights to facilitate the withdrawal of data or data portability. Since data protection law can draw normatively more directly on privacy as a fundamental right, it might be sometimes easier to use data protection law instead of consumer law for implementing these policy solutions. In the following, we will focus on another approach from an economics perspective, namely analyzing personal data and privacy from a property rights perspective. Here market failures on digital markets can occur, because the technologial progress through digitalisation might require the (re)definition and (re)specification of property rights on (personal) data for (1) protecting the fundamental right to privacy (e.g., against new kinds of privacy violations as intrusive surveillance practices), and (2) for enabling well-functioning markets for (personal) data in the digital economy.

The economic theory of property rights asks about the optimally specified bundle of rights in regard to an object, as, e.g., personal data.[54] From this perspective, the question is who has the right to collect what kind of data and for what use, to process these data (and how), and to what extent firms are allowed to trade these data and share them with others. And to what extent do these firms need to inform the persons and/or need their consent? Do they need their explicit consent in form of an opt-in solution or are also opt-out solutions sufficient, i.e. that as default rule the firms can collect, use and transfer the data as long as the individuals do not explicitly contradict. Do the individuals have a right to information about the data firms have collected about them, and do they have a right to correct wrong information and even have a right to withdraw the data or have them deleted? Through answering all these questions data protection laws can be interpreted as defining, specifying, and allocating

[53] See, e.g. also the German *Monopolkommission* (fn.4), para. S13.
[54] For property rights theory see *Furubotn/Richter*, Institutions and Economic Theory 2010, 79.

property rights on personal data, and whether and under what conditions those rights can be transferred and traded. Therefore the different approaches to data protection and privacy in the EU and the US can be interpreted as different definitions and allocations of property rights about personal data and the extent of their tradeability. Whereas a traditional law and economics approach would ask for the economically efficient (i.e. welfare-maximizing) specifications of these property rights, the normative decision to view privacy also as a fundamental right of individuals might lead to a stronger protection of privacy and personal data than what can be derived from an economic efficiency standard. This also can lead to tradeoffs between privacy protection and welfare maximization.

So far the analysis of data protection and privacy laws from a law and economics perspective is still in its infancy. Although some of the studies in the economics of privacy literature can be interpreted that way, economic studies about specific data protection laws as, e.g., the new European Data Protection Regulation are still missing.[55] However, for the US, where often also on the state level specific privacy laws were enacted for certain sectors as the health sector or credit markets, a number of studies exist that clearly show the often difficult tradeoffs that have to be considered in regard to the design of privacy laws. Empirical studies in US credit markets seem to confirm the theoretical prediction that tighter privacy laws, which set more restrictions for financial institutions to obtain and trade information about borrowers and credit applicants, impede the screening of consumers, and can lead to higher prices for mortgages, lower rejection rates and higher default rates.[56] The tradeoffs in the health sector are even more complex. Although health data are very sensitive personal data requiring a strict privacy protection, the obtaining, transfer and processing of health data, e.g., also through electronic medical records, might be crucial for the health of the patients themselves but also for medical research and innovations as well as for saving costs in the health sector. One of the problems is that better knowledge about health risks, e.g., through genetic testing, might allow better treatment but also carries the risk for patients for being discriminated by health insurance companies or employers if nondisclosure is not ensured.[57] Privacy laws have to navigate these and other tradeoffs in a sophisticated way for finding the right balance between the benefits and costs of protecting privacy. One much discussed general possibility for helping to solve this problem are privacy-enhancing technologies, which through anon-

---

[55] Exceptions are studies about compliance costs (e.g., *London Economics*, Implications of the European Commission's proposal for a general data protection regulation for business 2013).

[56] See, e.g., *Jentzsch*, The Regulation of Financial Privacy: The United States vs. Europe. European Credit Research Institute 2003, *Jappelli/Pagano*, Information sharing, lending and defaults: Cross-country evidence. Journal of Banking and Finance 2002, 2017, *Kim/Wagman,* Screening incentives and privacy protection in financial markets: A theoretical and empirical analysis. RAND Journal of Economics 2015, 22.

[57] See *Acquisti/Wagman/Taylor* (fn.3), 29-32, *Adjerid et al*, Impact of health
disclosure laws on health information exchanges, NBER Workshop on the Economics of Digitization 2013, *Miller/Tucker*, Privacy protection, personalized medicine and genetic testing 2014, available at SSRN: http://ssrn.com/abstract=2411230.

ymization try to combine the analysis of huge data pools with protecting the privacy of individual persons.[58] The experiences with the health and credit sector show that it might be necessary to develop sector-specific rules for the application of data protection and privacy laws.

From a property rights perspective it can also be suggested that a solution to the question of privacy and the fulfillment of different privacy preferences of individuals can be sought through propertization of personal data. Although personal data are protected under data protection laws, so far it is entirely unclear whether persons own their personal data in the sense of property and what ownership might mean in that respect.[59] The idea of a market for personal data would be that individuals based upon their own preferences could decide what kind of personal data they want to sell or license (and under what restrictions). This also would allow individuals to offer their personal data for money on data markets instead of letting large tech companies as Google or Facebook collect their personal data in exchange for the use of "free" services as social networks or search services.[60] An early discussion about this idea of propertization has shown that also with such an approach difficulties and market failure problems might arise which would require regulatory solutions.[61] However in my view such an approach would be very worthwhile to pursue in the future. But it might be helpful to think less in terms of markets for selling personal data and more in terms of markets for licensing the use of personal data. Such licensing agreements would also allow a much more precise specification for what kinds of uses and to whom the rights to use the data should be sold (and for how long). This idea of markets for licensing personal data is closely linked also to other new discussions in the digital economy, as, e.g., about the licensing of copyright-protected digital goods, which in the long run might replace the "sale" of digital goods as music and books.[62] Another discussion refers to proposals for creating new

---

[58] See *London Economics*, Study on the economic benefits of privacy-enhancing technologies (PETs), 2010. However, in the meantime, there is also considerable skepticism about anonymization as a solution; see *Barocas/Nissenbaum*, Computing Ethics. Big Data's end run around procedural privacy protections, Comunications of the ACM 2014, 31.

[59] *Monopolkommission* (fn.4), para. 88-89.

[60] For a new start-up industry which offers services to empower consumers to take control and sell their data, see *Chahal*, Taking back control: the personal data economy, available at: www.marketingweek.com/2014/03/12/taking-back-control-the-personal-data-economy, and *Mun et al*, Personal data vaults: A locus of control for personal data streams, ACM CoNext 2010, available at: remap.ucla.edu/jburke/publications/Mun-et-al-2010-Personal-Data-Vaults.pdf.

[61] For these early discussions see especially *Laudon*, Markets and privacy. Communications of the ACM 1996, 92, *Samuelson*, Privacy as intellectual property. Stanford Law Review 2000, 1125, and *Schwartz*, Property, Privacy, and Personal Data. Harvard Law Review 2004, 2056; *Acquisti/Wagman/Taylor*, (fn.3), 41, are skeptical.

[62] For the discussion about the tradeability of copyright-protected digital goods (exhaustion) see *Rubí Puig*, Copyright exhaustion rationales and used software. A Law and Economics approach to Oracle v. UsedSoft, jipitec 2013, 159, and *Rub*, Rebalancing copyright exhaustion, Emory Law Journal 2015, 741.

exclusive rights for automatically generated data.[63] However in regard to creating well-functioning markets for (the use of) personal data much more economic and legal research is necessary.

VI. Conclusions

The technological revolution through the digital economy with its manifold possibilities and dangers is still at the beginning. But it seems to be clear that the amount of generated data will increase exponentially and that it is no more a technological problem to collect comprehensive data about the behavior, characteristics, interests, and opinions of nearly all citizens of a society. The "internet of things", the use of sensor data, and the increasing use of surveillance in public places will accelerate this development. Therefore the need of legal protection of the privacy of individual persons will increase dramatically, both in regard to the state and in regard to private parties in the market context of the digital economy. Since many of the current rules do not reflect these new technological possibilities, a broad adaptation of legal rules is necessary for dealing with the new possibilities and problems of the digital economy. The protection of privacy as a fundamental right can be derived from the basic values of autonomy and human dignity. However also from an economic perspective, it can be shown that the protection of privacy and personal data should be strengthened for solving serious market failure problems in regard to privacy. So far economic research has identified competition problems, information and rationality problems, externalities, and the lack of properly specified property rights about personal data as important market failure problems which call for an adaptation of legal rules.

From an economic perspective, it is crucial to understand the manifold and complex effects and trade off problems in regard to information and privacy. In section II we have seen that the impact of having more information about customers depends very much on the specific conditions of digital markets, and therefore legal rules for protecting privacy might have very different and sometimes counterintuitive effects. Therefore data protection rules should be applied in a specific way to different digital markets, and often only after an economic analysis of the expected effects. Most important is to find the right balance between the huge potential advantages of analyzing large sets of collected data and protecting the privacy of individual persons. A very difficult problem is to develop legal rules and regulatory solutions for the protection of privacy in these highly innovative digital markets without impeding too much further innovation and endanger the many (so far still unknown) future opportunities of the digital economy. Therefore it can be expected that also a lot of regulatory errors will be made, both in regard to under- and overregulation.

---

[63] See *Dorner*, Big Data und „Dateneigentum“, Grundfragen des modernen Daten- und Informationshandels, Computerrecht 2014, 617, *Zech*, Daten als Wirtschaftsgut - Überlegungen zu einem „Recht des Datenerzeugers“, Computerrecht 2015, 137.

The digitalisation of the economy requires the adaptation of a wide array of different legal rules and policies. This article has focussed on competition, consumer, and data protection law. However, also other fields of law are relevant as, e.g., media law and intellectual property law. For example, the German Monopolkommission emphasized the danger of abusive behavior of dominant internet firms in regard to the violation of intellectual property rights, e.g. through scraping content from websites, and recommended clarifications in copyright law.[64] This article claims that it is necessary to develop a sophisticated integrated approach of the proper legal rules in competition, consumer, and data protection law (and also intellectual property) for developing a well-functioning legal order for protecting privacy in the digital economy. Therefore the interrelations between competition, consumer, and data protection laws are particularly worthwhile for further research. This requires joint research of specialised lawyers in competition, consumer and data protection law as well as interdisciplinary research of lawyers and economists. However it also requires the collaboration of the enforcement agencies in these different policy areas. Therefore competition authorities, consumer protection agencies, and data protection supervisors have to find a common strategy how to deal with privacy issues and protect consumers and implement them in a coordinated way.

[64] *Monopolkommission* (fn.3), para. 284-287.