Contracting Around Privacy

The (Behavioral) Law and Economics of Consent and Big Data

by **Yoan Hermstrüwer**, Senior Research Fellow at the Max Planck Institute for Research on Collective Goods in Bonn, Germany. His research covers (behavioral) law and economics, cyberlaw, constitutional law, financial law, international economic law and empirical legal studies (hermstruewer@coll.mpg.de).

Abstract: European privacy law rests on the implicit assumption that consent to the processing of personal data and the analysis of Big Data is a purely individual choice. Accordingly, privacy lawyers mainly focus on how to empower users to make free and informed choices, for instance through debiasing and nudging. However, a game theoretical analysis suggests that strategic considerations may be a driving force of consent under certain conditions. In environments relying on the use of Big Data, consent is likely to impose negative privacy externalities on other users and constrain their freedom of choice. By contrast, a behavioral economic analysis suggests that users are subject to bounded rationality and bounded willpower. While nudges, like default options, can enable users to make protective privacy choices in some cases, correcting cognitive deficits might facilitate market failures and accelerate the erosion of privacy in other cases. This counterintuitive conclusion shows that legal rules on consent and privacy contracts should be grounded on an assumption of 'mixed rationalities', i.e. on insights from both standard economics and behavioral economics. Hence, a sharper distinction between 'paternalistic nudging' and 'non-paternalistic soft regulation' to counter market failures is warranted.

Keywords: Consent; monetizing personal data; big data; EU privacy law; EU-GDPR; behavioral law and economics; game theory; nudging, libertarian paternalism; constitutional law

Recommended citation: Yoan Hermstrüwer, Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data, 8 (2017) JIPITEC 9 para 1.

A. Introduction

1 Personal data has become one of the most important currencies in digital economies.[1] This currency seems to be inherently inclusive and egalitarian, since there is no need to be wealthy in order to pay with data. Digital services like Facebook, Google, Instagram or Snapchat, largely rely on this *pay-with-data* business model and the use of Big Data. However, monetizing personal data might well give rise to a society where, overall, publicity trumps privacy. On both sides of the Atlantic, the debate about what legislators should do to cope with the tendency to contract around privacy and the continuous erosion of privacy has just begun.

2 One of the biggest problems is that privacy law does not really dovetail with the concept of contract and the idea of personal data as money.[2] While there is a growing consensus that privacy can be waived and even monetized, it is less clear under which conditions such a 'contract around privacy' shall be considered valid. In the draft of a Directive on

1 This article draws on Hermstrüwer, Informationelle Selbstgefährdung (2016).

2 *Ben-Shahar/Strahilevitz*, Contracting over Privacy: Introduction, Journal of Legal Studies 45 (2016), S1 (S5-S10); *Hermstrüwer*, Informationelle Selbstgefährdung (2016).

certain aspects concerning contracts for the supply of digital content, the European Commission has proposed a new legal regime for contracts "where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data".[3] The EU General Data Protection Regulation (EU-GDPR), which was recently adopted as a substitute for the EU Data Protection Directive, relies on consent as the prime mechanism to 'pay' with personal data.[4] According to Art. 4 § 11 EU-GDPR, consent "means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". How can privacy law enable people to make such an autonomous choice?

3 The academic and political struggle over appropriate tools to empower people to protect or waive their privacy has been fought from two different angles: the traditional data protection approach and the market-oriented approach. The data protection approach is firmly anchored in the tradition of public law doctrine and claims that stricter government interventions to protect privacy are needed.[5] The market-oriented approach basically claims that the market will yield an optimal level of privacy, be it through competition, self-regulation, or learning and evolutionary forces.[6]

4 In this article, I argue that to a certain extent both approaches go astray. As it seems, neither policymakers nor legislators have sufficiently taken account of the cognitive and motivational forces driving privacy choices. The result of this reluctance to take account of economics and psychology is a mismatch between the regulatory problem and the legal tools introduced to solve it. Consequently, the literature regarding the role that the behavioral sciences could play in the design and implementation of EU privacy law remains rather scarce.[7] To understand the regulatory problem associated with contracts involving consent to the disclosure of personal information, I argue that it is crucial to understand the behavioral and social forces that push people to disclose personal information in the first place. A cautionary note is warranted, however; the objective of my analysis is not to identify the criteria for optimal contract design, nor to develop a full-fledged doctrinal framework for consent and Big Data embedded in behavioral law and economics. Rather, my objective is to identify some of the 'sweet spots' where the law could step in to regulate privacy choices and consent, given certain more or less specific objectives that EU privacy law aims to accomplish.

5 In Section B, I explore the factors driving consent in an analytical framework set out by rational choice theory and game theory. This approach allows us to understand some of the strategic reasons pushing users to disclose or withhold personal information in interactions with companies or other users. In Section C, I shed light on the so-called privacy paradox and the behavioral economics of privacy. Without a good grasp of this paradox, lawmakers and legal practitioners are likely to make ill-informed choices that may well cause backfire effects in some cases. In Section D, I show that a behaviorally informed privacy law does not necessarily imply libertarian paternalism. EU privacy law and constitutional law should take account of the distinction between paternalistic nudging and non-paternalistic soft regulation of market failures. In Section E, I present my conclusion.

B. The Strategic Rationality of Consent

6 Rational choice theory assumes that individuals are rational actors with a set of stable and exogenously given preferences.[8] Rational actors are able to process an indefinite amount of information and will always make their choices such as to maximize their utility. Standard game theory builds on the rational choice paradigm and analyzes strategic interactions between actors.[9] Under a game theory approach,

3 Art. 3 § 1 of the Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content [Brussels, 9.12.2015, COM(2015) 634 final].

4 Regulation EU 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

5 *Solove*, Privacy Self-Management and the Consent Dilemma, Harvard Law Review 126 (2013), 1880; *Weichert*, Wider das Verbot mit Erlaubnisvorbehalt im Datenschutz?, Datenschutz und Datensicherheit 2013, 246.

6 *Tene/Polonetsky*, Big Data for All: Privacy and User Control in the Age of Analytics, 11 Northwestern Journal of Technology and Intellectual Property 11 (2013), 239 (242), favoring a relaxation of the consent requirement; for a traditional view *Posner*, The Right of Privacy, Georgia Law Review 12 (1978), 393; *Stigler*, An introduction to privacy in economics and politics, Journal of Legal Studies 9 (1980), 623; *Posner*, The Economics of Privacy, American Economic Review 71 (1981), 405.

7 But see *Borgesius*, Behavioural Sciences and the Regulation of Privacy on the Internet, in Alemanno/Sibony (Eds.), Nudge and the Law: A European Perspective (2015), 179.

8 *Becker*, The Economic Approach to Human Behavior (1976), 14.

9 *Rebonato*, Taking Liberties: A Critical Examination of Libertarian Paternalism (2012).

whether a person gives their[10] consent depends on the choices or, more precisely, the strategies chosen by companies and other users. Consent has the features of a choice in a strategic game. Game theory shows that under certain conditions, rational actors will have a strategic incentive to disclose personal information and give their consent. The upshot is that the erosion of privacy does not necessarily result from the bounded rationality of users. Rather, consenting to the processing of personal information might often be the result of a rational calculus. On a *positive* view, this shows that countering bounded rationality could facilitate strategic choices for sophisticated users and accelerate the erosion of privacy. On a *normative* view, it shows the limits and potential drawbacks of debiasing instruments in the field of privacy law.

I. Consent and Default Rules

7 According to the Coase theorem, the initial allocation of a right or good is irrelevant for its final allocation in the absence of transaction costs.[11] The right or good will eventually end up in the hands of the person who values it most. Each transaction entails a pareto-superior allocation. The process ends once a pareto-optimal allocation is accomplished; and in principle, the same holds for the process of bargaining over the allocation of personal information. The main contribution of the Coase theorem is not that markets will work in theory, but that transaction costs matter. When transaction costs are high – as is usually the case – parties will not contract around inefficient default rules (contractual standard settings).[12] Therefore, the law should use instruments to reduce transaction costs when the legislator aims to foster efficiency (welfare approach) or to increase transaction costs when the legislator aims to limit transactions for whatever reason. What does this mean for situations where users and companies can bargain over the allocation of personal information?

8 On the one hand, privacy law can attempt to minimize the transaction costs associated with the transfer of personal information. This objective can be achieved through default rules. As regards consent and contract formation, privacy law distinguishes between two different types of default rules: opt-in rules and opt-out rules. Traditionally, law and economics scholars claim that default rules should mimic the terms that a majority of parties would have agreed on without transaction costs (*majoritarian defaults*).[13] A majoritarian default simply minimizes the number of parties that have to contract around a default rule to reach an efficient agreement. The theory of majoritarian defaults results from a simple transaction cost analysis of incomplete contracts.

9 The problem of this approach is that it assumes a symmetric distribution of transaction costs between the majority and the minority.[14] When it comes to the design of consent options in privacy law, such an asymmetric distribution of costs is not unlikely. Digital platforms can lower their transaction costs by offering a standardized menu of default rules in their privacy settings. Their transaction costs should be low because they do not have to bargain over privacy with each and every user. On the user side, however, one should expect a huge disparity of transaction costs. Suppose that most users do not care for privacy, while a minority of users has strong privacy preferences. If the number of default rules in the standardized privacy settings is large, like on Facebook or Google, the minority of privacy sensitive users will incur high transaction costs since they will have to alter most of the standardized privacy settings. The inverse problem arises when the majority of users have strong privacy preferences.[15] In this case, the small group of users with weak privacy preferences is likely to incur high transaction costs if the default rules restrict the processing of personal information. Without concrete empirical evidence on the distribution of transaction costs, legislators can only speculate about the adequate allocation of rights. This shows that the *privacy by default* principle enshrined in Art. 25 § 2 EU-GDPR cannot clearly be justified according to the logic of majoritarian defaults.

10 On the other hand, default rules may also be justified on strategic grounds to counter the risk of a specific kind of market failure. In some cases, the bargaining parties will refrain from contracting around a default rule even when the transaction costs are low. Parties might prefer to stick with the status quo because contracting around the default rule would require one of the parties to disclose private information.[16] Disclosure of this information might enable the

10 For the sake of linguistic neutrality, I avoid the generic 'he' or 'she' and use the *singular they* as far as possible. See *Baron*, Gender politics of the generic "he", OUPblog, January 6, 2016, *available at* <https://blog.oup.com/2016/01/gender-politics-generic-he/>.

11 *Coase*, The Problem of Social Cost, Journal of Law and Economics 3 (1960), 1.

12 *Korobkin*, The Status Quo Bias and Contract Default Rules, Cornell Law Review 83 (1998), 608 (614-615).

13 See *Ayres/Gertner*, Majoritarian vs. Minoritarian Defaults, Stanford Law Review 51 (1999), 1591 (1592).

14 *Ayres/Gertner*, Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules, Yale Law Journal 99 (1989), 87 (93).

15 *Willis*, Why Not Privacy by Default?, Berkeley Technology Law Journal 29 (2014), 61 (64).

16 *Korobkin*, The Status Quo Bias and Contract Default Rules, Cornell Law Review 83 (1998), 608 (617-618).

uninformed party to exploit this information to their benefit and increase their gains from the contract.[17] Building on this analysis, default rules can be set in a way that the parties – specifically the informed party – would not want (*penalty defaults*).[18] Penalty defaults follow the logic of signaling games in that they force the informed party to reveal information regarding their own attributes (type).[19] They are designed to give the informed party an incentive to disclose private information. Accordingly, an opt-in rule that requires consent sets an incentive for companies to reveal more or more specific information about the characteristics of the service and the respective privacy policies.[20] An opt-in rule will force companies to convince users to opt in and give their consent. Through the lens of the theory of penalty defaults, an opt-in rule may be justified as a rule to solve information asymmetries and counter market failures. On this view, it should not be conceived of as a policy default that aims at exploiting users' status quo bias and reducing the overall amount of positive consent decisions. Hence, the theory of penalty defaults might provide a better normative rationalization of Art. 25 § 2 EU-GDPR than justifications on the grounds of libertarian paternalism.

II. Consent and Collective Privacy

11 In a libertarian society, users have the right to disclose as much personal information as they like. The problem of this individualistic conception of privacy is that it misses a crucial feature of modern data analytics (Big Data) and the behavioral forces underlying the diffusion of personal information in networked environments. To understand the problem, it is helpful to consider a social network like Facebook or any other service building on network externalities. In these networks, algorithms are used to analyze large datasets consisting of personal and anonymized data.[21] For these algorithms to allow good predictions about personal traits and behaviors, the network operator needs two things: sound knowledge about the social graph and large amounts of data. The social graph describes the social ties between users.

12 Now suppose that Angela is best friends with Bartleby and that Angela has willingly revealed information about her sexual orientation, while Bartleby has refrained from doing so, since he 'would prefer not to'.[22] Empirical evidence suggests that it is possible to predict the probability of Bartleby's sexual orientation with a simple logistic regression that depends on one parameter, i.e. the number of friends with a known sexual orientation.[23] This kind of prediction is not deterministic but probabilistic. However, if the data set is large enough, regressions will usually generate a better prediction than the toss of an even-sided coin. Other traits such as ethnicity, political preferences, religious affiliation, addictive behaviors and even emotions can be inferred from seemingly unrelated data using psychometric methods.[24] The more information a user feeds into the algorithms, the easier it becomes to predict outcomes. Moreover, with every piece of information that people willingly reveal about themselves, they increase the probability of revealing personal information about other users regardless of their (the other users') consent. Technically speaking, consenting to the processing of personal information about oneself imposes negative privacy externalities on other users.[25] This shows that privacy in networked environments has the features of a social dilemma.[26]

13 The easiest way to conceptualize the problem that users face when confronted with the option to disclose personal information or withhold it, is a simple prisoners' dilemma (Figure 1).[27] Suppose that users have the opportunity to give their consent (Defect = D) or refuse their consent (Cooperate = C). Further, suppose that each user has an incentive to disclose certain types of information about herself – say because she obtains a monetary or social reward

17 *Ayres/Gertner*, Majoritarian vs. Minoritarian Defaults, Stanford Law Review 51 (1999), 1591 (1591).

18 *Ayres/Gertner*, Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules, Yale Law Journal 99 (1989), 87 (91).

19 The idea of signaling games is often attributed to *Spence*, Job Market Signaling, Quarterly Journal of Economics 87 (1973), 355.

20 *Kesan/Shah*, Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics, Notre Dame Law Review 82 (2006), 583 (633); *Willis*, Why Not Privacy by Default?, Berkeley Technology Law Journal 29 (2014), 61 (82).

21 *Mayer-Schönberger*, Big Data: A Revolution That Will Transform How We Live, Work, and Think (2013); *Fairfield/Engel*, Privacy as a Public Good, Duke Law Journal 65 (2015), 385 (389-390).

22 This is an allusion to *Herman Melville*, Bartleby, the Scrivener: A Story of Wall Street [The Piazza Tales, 1856].

23 *Jernigan/Mistree*, Gaydar: Facebook friendships expose sexual orientation, First Monday 14 (2009).

24 *Kosinski/Stillwell/Graepel*, Private traits and attributes are predictable from digital records of human behavior, PNAS 110 (2013), 5802 (5803). The rumor goes that Cambridge Analytica helped Donald Trump to win the US presidential election in 2016 by targeting thousands of users through psychometrics.

25 *MacCarthy*, New Directions in Privacy: Disclosure, Unfairness and Externalities, I/S: A Journal of Law and Policy for the Information Society 6 (2011), 425 (447).

26 See also *Regan*, Legislating Privacy: Technology, Social Values, and Public Policy (1995), 227; *Fairfield/Engel*, Privacy as a Public Good, Duke Law Journal 65 (2015), 385 (397).

27 For a more complex model see *Hermstrüwer*, Informationelle Selbstgefährdung (2016), 167-169.

– but that she does not want others to intrude on her privacy and disclose information about her.

		User 2 C	User 2 D
User 1	C	3 , 3	0 , 5
	D	5 , 0	1 , 1

Figure 1: Prisoners' dilemma

14 From a rational choice perspective, it is rational for every user to give their consent if the benefits of consent exceed its costs. In the prisoners' dilemma depicted above, consent is the best response to any given strategy of the other user.[28] In this simple game, consent (D) strictly dominates the refusal of consent (C), which means that each user will disclose personal information. Consent is the dominant strategy equilibrium in this game.

15 To understand the role of companies and the broader dimension of the social conflict over privacy, the interaction between users and companies may be conceived of as a one-sided hawk/dove game (Figure 2).[29] Suppose that companies can choose between an aggressive strategy of gathering data (Hawk = H) or a tame strategy of offering users a decent level of privacy protection (Dove = D). Further suppose that users can choose between consent (D) and the refusal of consent (H) and that companies have understood the social dilemma between users described above.

		Companies D	Companies H
Users	D	2 , 1	1 , 4
	H	4 , 0	0 , 2

Figure 2: One-sided hawk/dove game

16 If companies anticipate that only few users will refuse to give their consent or refrain from using their services, they will always opt for the aggressive strategy and impose take-it-or-leave-it options on users. From this point of view, refusing consent and the disclosure of personal information is not a credible threat against companies. Companies will anticipate that the group of users refusing consent will not be large enough to negatively affect their gains. Users can refuse consent but this choice excludes them from the use of digital services if no privacy-friendly alternatives are offered on the market. The important aspect of this game is that it combines elements of a cooperation game and a coordination game. As a consequence, the choice over the disclosure or non-disclosure of personal information may be described as a decision in a mixed-motive game in which users have to cooperate and coordinate to reach a socially optimal level of privacy. What does this analysis tell us about privacy law?

17 First, it shows that the individualistic conceptualization of privacy goes astray. The decision to give consent and disclose personal information will often be influenced by other users' behavior and result from strategic incentives in a situation with the features of a social dilemma. The refusal of consent is a dominated strategy that rational users will have no incentive to choose whatsoever. On this view, full and informed consent might be considered the reason for the erosion of privacy and not the solution to the very problem. The counterintuitive result for lawmakers and privacy lawyers is that empowering users to make more rational choices is likely to accelerate the erosion of privacy. This result holds regardless of individual privacy valuations.

18 Second, in larger networked environments the social dilemma will have the features of a public goods game. Users might have an incentive to free-ride on other users' efforts to protect their privacy and persist on disclosing personal information about themselves. In the end, consent is rational from an individual perspective but it produces a suboptimal level of privacy for all users. The individual freedom of users to give their consent comes at a cost, namely a reduction of the level of collective privacy. This leads to a crucial insight for legislators and privacy lawyers: Privacy law can either guarantee the freedom of consent or a (pareto-)optimal level of privacy, but not both.

19 This analysis prompts three conclusions regarding privacy regulation. First, experimental evidence on public goods games suggests that many people are conditional cooperators.[30] If people believe that

28 *Rasmusen*, Games and Information. An Introduction to Game Theory, 4. Ed. (2007), 20; *Baird/Gertner/Picker*, Game Theory and the Law (1994), 11-14.

29 For this conceptualization of the problem *Warner/Sloan*, Behavioral Advertising: From One-Sided Chicken to Informational Norms, Vanderbilt Journal of Entertainment and Technology Law 15 (2012), 49 (61-65). *Hetcher*, Norms in a Wired World (2004), 298-301, assumes a prisoners' dilemma and the evolution towards cooperative norms between companies and users in the long run.

30 *Fischbacher/Gächter/Fehr*, Are people conditionally cooperative? Evidence from a public goods experiment, Economics Letters 71 (2001), 397; *Chaudhuri*, Sustaining Cooperation in Laboratory Public Goods Experiments: A Selective Survey of the Literature, Experimental Economics

others will not exploit them or free-ride on their efforts, they are likely to resist the temptation of playing an uncooperative strategy. Increasing the visibility of other users' refusal to consent might be used as a tool to trigger reciprocation and cooperation among users. Second, theories of expressive law suggest that law can be used to communicate normative expectations and thereby change behavior without the threat of a sanction.[31] Expressive law can either induce a change of preferences or push people to select certain equilibria in strategic interactions. In the latter case, the law can be used to set what game theorists call a focal point. In principle, communication of the rule sets a focal point and helps solve the coordination problem.[32] For instance, increasing the salience of legal rules on right-hand or left-hand traffic is likely to make the preferred outcome focal. Empirical evidence suggests that focal points can facilitate equilibrium selection not only in pure coordination games but also in mixed-motive games.[33] Therefore, making opt-in rules very salient could set a focal point and help users solve some of the strategic problems associated with consent. Opt-in rules can be considered as third-party expression of normative (legislative) expectations as to the socially desirable level of privacy. They might help users to form an expectation of the behavior of other users. Third, empowering users to make informed and unrestricted choices about the disclosure of personal information is likely to accelerate the erosion of privacy in networked environments instead of slowing it down. The legal requirements set by Art. 7 § 1 EU-GDPR (free and informed consent) are based on a purely individualistic conception of privacy.

20 In sum, the EU-GDPR takes no account of collective privacy and the strategic incentive problems resulting from the analysis of Big Data. To solve the privacy problem, legislators and privacy lawyers might consider structural similarities with other public goods problems, such as the protection of the environment or the stability of the financial system.

III. Consent and Unraveling

21 Privacy lawyers often assume that refusing consent will offer sound protection of individual privacy.[34] Each user, the argument goes, can freely decide whether to disclose or withhold personal information. I have already explained why this argument is flawed once we consider the strategic incentives of users in environments with the features of a social dilemma and a one-sided hawk/dove game. But another problem might occur when consent is incentivized, the company creating the incentive holds a monopoly, and the group of users is heterogeneous.

22 For example, consider an insurance company that offers a rebate if the user consents to the disclosure of a specific piece of 'high-value' personal information – such as information about good health – and discriminates between different types of users.[35] In a pool of heterogeneous users, the user with the best health information has the strongest incentive to reveal this information and consent to its processing because they would like to obtain a favorable (cheaper) service. Once this user has consented, the pool of remaining users shrinks. The user who had the second-best personal traits now has the best personal traits in the pool of remaining users and therefore has the strongest incentive to give consent. This user would want to avoid a negative inference about their health status from a refusal of consent and therefore disclose personal information. An unraveling process has now been set in motion. This process follows the logic of signaling games where the disclosure of high-value information facilitates an inference about low-value information for those refusing to disclose personal information.[36] Without further constraints and with a tool to verify personal information, the unraveling process ends when every user has consented to the disclosure and processing of personal information.[37]

23 This unraveling may concur with price discrimination where the company aligns the price of the service with the individual willingness to

14 (2011), 47 (49).

31 *Lessig*, The New Chicago School, Journal of Legal Studies 27 (1998), 661; *McAdams*, A Focal Point Theory of Expressive Law, Virginia Law Review 86 (2000), 1649.

32 For an investigation of salience see *Mehta/Starmer/Sugden*, The Nature of Salience: An Experimental Investigation of Pure Coordination Games, American Economic Review 84 (1994), 658.

33 *McAdams/Nadler*, Testing the Focal Point Theory of Legal Compliance: The Effect of Third-Party Expression in an Experimental Hawk/Dove Game, Journal of Empirical Legal Studies 2 (2005), 87.

34 *Mayer-Schönberger*, Delete: The Virtue of Forgetting in the Digital Age (2009), 128-134.

35 The basic idea goes back to *Grossman*, The Informational Role of Warranties and Private Disclosure About Product Quality, Journal of Law and Economics 24 (1981), 461. See also *Fishman/Hagerty*, Mandatory Versus Voluntary Disclosure in Markets with Informed and Uninformed Customers, Journal of Law, Economics, and Organization 19 (2003), 45. For many more examples see *Peppet*, Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future, Northwestern University Law Review 105 (2011), 1153.

36 *Stigler*, An Introduction to Privacy in Economics and Politics, Journal of Legal Studies 9 (1980), 623.

37 *Baird/Gertner/Picker*, Game Theory and the Law (1994), 90.

pay.[38] However, both processes do not necessarily coincide. It is important to note that unraveling is efficiency-enhancing since users will be required to pay a price that reflects their individual (health) risk. Privacy has the opposite effect and entails a redistribution of resources between users and cross-subsidization of types with low-value information. Efficiency-minded users might therefore prefer a certain degree of unraveling, while users with a preference for redistribution might have a taste for privacy. However, whether an unraveling occurs in real markets will depend on a variety of additional factors.

24 First, if the company sets a certain quality threshold and only offers a rebate for personal information above this threshold – e.g. for doing sports three times a week – only users with information above this threshold will give their consent. This might eventually lead to a separating equilibrium with a pool of consenting users and a pool of non-consenting users.[39] In this case, unraveling is mitigated. Second, if the costs of consent are high, only few users will give their consent. Non-consenting users will be pooled together and include users with high-value and low-value information. It will then be difficult to make a sound inference from a refusal of consent. High costs of consent may therefore lead to a pooling equilibrium and limit unraveling.[40] Third, bounded rationality in the sense of limited depth of reasoning (level-k reasoning) and limited anticipation of other users' behavior may also slow down the unraveling process.[41] Only entirely rational players who form correct beliefs about other players' beliefs (about their own beliefs and so on) will eventually set in motion a perfect unraveling process. Finally, a simple privacy framing (e.g. mentioning that the choice relates to the 'health status' of 'workers' in a 'labor market') may be enough to trigger privacy concerns and reduce the propensity to consent.[42] Salient information about the risks of consent and the processing of personal information could therefore mitigate unraveling.[43]

25 Generally, this analysis shows that privacy law has rent-shifting effects.[44] User welfare depends on the distribution of user types and on the identity and distributional preferences of those who benefit or lose from privacy-protective rules. From a doctrinal point of view, it shows that conventional legal doctrines concerning the freedom of consent do not capture the behavioral pressure associated with unraveling. The implicit behavioral assumption of many privacy laws is that the freedom to consent is not constrained as long as users are formally offered an option to refuse consent and use the service without disclosing personal information. Under Art. 7 § 4 EU-GDPR, for instance, the assessment whether consent is freely given should take account of whether the performance of a contract is conditional on consent. However, as the unraveling analysis shows, consent may significantly increase the pressure to consent on other users. Once unraveling is triggered, consent imposes a negative externality on others in that it increases their (expected) cost of refusing consent. Unraveling might therefore occur irrespective of a conditionality link between contract performance and consent. This prompts two observations as to the adequacy of legal instruments used to protect privacy.

26 On the one hand, there are many situations where the most effective instrument to mitigate unraveling will be a legal prohibition of the processing of personal information. Art. 9 § 1 EU-GDPR contains such a prohibition for genetic data, biometric data, health data and data concerning sex life and sexual orientation. This prohibition is based on the conventional idea that specific categories of personal information should benefit from stronger protection than others. It does not however, take account of the structural risk of unraveling. If privacy law aims at securing the freedom of consent, it might make more sense to identify situations bearing a high unraveling risk and determine the level of privacy protection according to this risk instead of relying on a classification of specific categories of personal information deemed to be sensitive.

27 It is important to note that the legal justification for this kind of prohibition is not paternalistic. Rather, prohibitions of processing will have the effect of countering negative externalities (i.e. behavioral pressures generated by consent) and

38 For an analysis see *Strandburg*, Free Fall: The Online Market's Consumer Preference Disconnect, University of Chicago Legal Forum (2013), 95 (134-141).

39 For further explanations of this equilibrium concept see *Rasmusen*, Games and Information. An Introduction to Game Theory, 4. Ed. (2007), 320-324; *Baird/Gertner/Picker*, Game Theory and the Law (1994), 80-89.

40 *Posner*, Privacy, in: Newman (Ed.), The New Palgrave Dictionary of Economics and the Law 3 (1998), 103; *Benndorf/Kübler/Normann*, Privacy concerns, voluntary disclosure of information, and unraveling: An experiment, European Economic Review 75 (2015), 43 (48-52).

41 *Benndorf/Kübler/Normann*, Privacy concerns, voluntary disclosure of information, and unraveling: An experiment, European Economic Review 75 (2015), 43 (51-52). Inequality aversion could also reduce unraveling.

42 *Benndorf/Kübler/Normann*, Privacy concerns, voluntary disclosure of information, and unraveling: An experiment, European Economic Review 75 (2015), 43 (50).

43 However, salient consent options may push users to comply with social norms, see *Hermstrüwer/Dickert*, Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten, MPI Collective Goods Preprint, No. 2013/15 (<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2311201>).

44 *Jentzsch*, Secondary use of personal data: a welfare analysis, European Journal of Law and Economics (2014), 1 (21).

could be justified on non-paternalistic grounds. An unraveling-based legal rule should also consider whether users can influence personal information. Unraveling might have antisocial effects when personal information is impossible or costly to influence. In this case, privacy law might be used as a social policy tool to increase redistribution and reduce unraveling pressures on those who should benefit from redistribution. Finally, prohibitions could be based on the objective to reduce chilling effects.[45] Such chilling effects might occur where users are offered valuable rewards for high-value information and where they have an incentive to adapt their behavior to generate such information, e.g. do more sports when consent to the processing of information regarding intense sports activities is incentivized. The normative assessment of a chilling effect depends on whether a deviation from the expectation set by the data-intensive service is qualified as 'good'. Courts could operate this assessment on a case-by-case basis and use the unraveling argument as a justification for sectoral restrictions.

28 On the other hand, the unraveling argument shows that a correction of rationality deficits (*debiasing*) will not necessarily lead to an increase of privacy.[46] Improving users' capacity to engage in level-k reasoning and anticipate other users' behavior would probably foster unraveling. Providing users with better information about the inner-workings of algorithms and data-intensive services might not always be compatible with the objective of increasing the level of privacy. This prompts an argument that runs counter to the regulatory approach supported by some libertarian paternalists: If the social value to be protected is privacy according to the policy objectives formulated by the European legislator, reducing bounded rationality is likely to be the wrong intervention. The potential downside of such an approach is that some unsophisticated users would have to cope with the bounds of their rationality on their own.

C. The Behavioral Rationality of Consent

29 Instead of building an axioms known from decision theory, behavioral economists draw into question these very assumptions (money maximization[47], stability and exogeneity of preferences, optimal evaluation and processing of information).[48] Analyzing the trade-offs associated with protecting or sharing personal information, behavioral economists have determined bounds to rationality, self-interest and willpower.[49] These bounds provide some explanations of the factors pushing users to disclose personal information and give their consent. The starting point of the analysis is what has been called the privacy paradox: While many people claim that they do care very much about their privacy, they willingly reveal large amounts of personal information. This observation is corroborated by empirical evidence showing that there is a significant gap between expressed preferences and revealed preferences for privacy.[50] According to the theory of revealed preferences, observed privacy choices can be seen as a straightforward expression of true privacy preferences. Accordingly, the privacy paradox is seen as an artifact of a comparison of two very different things: attitudes and behavior.

30 This approach, however, neglects psychological evidence on preference uncertainty, i.e. the fact that some people hold weak preferences or do not fully understand their preferences.[51] Furthermore, behavioral economics casts doubt on the relationship between choice, self-interest, utility and welfare.[52] Empirical evidence suggests that people are reluctant to offset the monetary benefits of consent with the

45 For a discussion of chilling effects in the context of privacy *Richards*, The Dangers of Surveillance, Harvard Law Review 126 (2013), 1934 (1949-1952).

46 For a general discussion of debiasing *Jolls/Sunstein*, Debiasing through Law, Journal of Legal Studies 35 (2006), 199.

47 It is important to note that utility maximization is not excluded under the assumption of non-standard preferences, see *Bernheim/Rangel*, Behavioral Public Economics: Welfare and Policy Analysis with Non-Standard Decision-Makers, in Diamond/Vartiainen (Eds.), Behavioral Economics and Its Applications (2007), 7.

48 *Jolls/Sunstein/Thaler*, A Behavioral Approach to Law and Economics, Stanford Law Review 50 (1998), 1471 (1476); for a critical assessment *Posner*, Rational Choice, Behavioral Economics, and the Law, Stanford Law Review 50 (1997), 1551.

49 *Acquisti/Brandimarte/Loewenstein*, Privacy and human behavior in the age of information, Science 347 (2015), 509; *Acquisti/Taylor/Wagman*, The Economics of Privacy, Journal of Economic Literature 54 (2016), 442; *Acquisti*, Nudging Privacy: The Behavioral Economics of Personal Information, IEEE Security & Privacy, November/December 2009, 82; *Acquisti/Grossklags*, Privacy and Rationality in Individual Decision Making, IEEE Security & Privacy, January/February 2005, 26.

50 *Berendt/Günther/Spiekermann*, Privacy in E-Commerce: Stated Preferences vs. Actual Behavior, Communications of the ACM 48 (2005), 1; *Norberg/Horne/Horne*, The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, Journal of Consumer Affairs 41 (2007), 100.

51 *Lichtenstein/Slovic*, The Construction of Preference: An Overview, in Lichtenstein/Slovic (Eds.), The Construction of Preference (2006), 1.

52 For an analysis of this problem generally *Sen*, Rationality and Freedom, 2002, 27; *Kőszegi/Rabin*, Mistakes in Choice-Based Welfare Analysis, American Economic Review 97 (2007), 477; *Bernheim/Rangel*, Beyond Revealed Preference: Choice-Theoretic Foundations for Behavioral Welfare Economics, Quarterly Journal of Economics 124 (2009), 51.

costs incurred by a loss of privacy.[53] As it seems, most people carry the costs and benefits of consent in different mental accounts (mental accounting). While there is a general reluctance to pay for privacy, this does not mean that users are never willing to incur costs for data protection.[54] Rather, it suggests that privacy preferences or, more generally, privacy behaviors are context-dependent and determined by the psychological processes underlying choices.[55] The obvious challenge for privacy law results from the fact that it cannot capture and regulate every context feature that might push users to disclose personal information. One possible solution to this challenge is to determine some of the structural features that are to a large extent context-independent. From a regulatory and legal perspective, it is critical to understand the reasons that might explain the structural factors driving the privacy paradox. Without such an understanding, privacy law is likely to use the wrong instruments to empower people to make free and informed privacy choices. The features determined in the following sections are derived from empirical studies of privacy choices. While these studies should be taken with due caution, they still provide important insights about the behavioral factors that privacy law should take account of.

I. Impact of Information

31 Perhaps the most obvious explanation for the privacy paradox can be found in information asymmetries between users and companies. Empirical evidence suggests that many users simply do not know when, how, and to what extent personal information is gathered by companies. Further evidence shows that only up to 1 % of users actually open the End User Licensing Agreement to have a glance at it when downloading software.[56] In a natural experiment conducted by GameStation, for instance, a large fraction of users agreed to sell their immortal soul when placing an order online.[57] This kind of behavior is not necessarily due to bounded rationality – regardless of whether users believe in the immortality of their soul or not. On the contrary, it is rational to refrain from reading privacy policies if the costs of reading exceed the expected benefits of ignorance (rational ignorance).[58] Some authors have estimated that it would take every user 76 days per year to entirely read the relevant privacy policies, resulting in an overall cost of 781 billion USD.[59] Consequently, users might simply rely on courts to assess the validity of privacy policies, which eventually further decreases incentives of users to read privacy policies and hampers informed consent.

32 The new EU privacy regime does not solve the problem of information asymmetries. Art. 12 § 1 EU-GDPR requires companies to provide information to users "in a concise, transparent, intelligible and easily accessible form, using clear and plain language". However, it is difficult to imagine how these transparency requirements could reasonably be met under a regime that also sets high quantitative thresholds with respect to information for users. In principle, Art. 14 EU-GDPR requires information about: the identity and the contact details of the controller; the contact details of the data protection officer; the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; the categories of personal data concerned; the recipients or categories of recipients of the personal data; the intention to transfer personal data to a recipient in a third country or an international organization; the period for which the personal data will be stored; the legitimate interests pursued by the controller or by a third party; the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability; the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; the right to lodge a complaint with a supervisory authority; the source the personal data originates from and whether it came from publicly accessible sources; the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such

53 *Acquisti/Grossklags*, Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting, in: Camp/Lewis (Ed.), The Economics of Information Security, 2004, 165.

54 *Tsai et al.*, The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, Information Systems Research 22 (2011), 254.

55 *Acquisti/Taylor/Wagman*, The Economics of Privacy, Journal of Economic Literature 54 (2016), 442 (476-478); *Adjerid/Soman/Acquisti*, A Query-Theory Perspective of Privacy Decision Making, Journal of Legal Studies 45 (2016), S97.

56 *Bakos/Marotta-Wurgler/Trossen*, Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts, Journal of Legal Studies 43 (2014), 1.

57 7,500 Online Shoppers Unknowingly Sold Their Souls, April 15, 2010, <http://www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls.html>: „By placing an order via this Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant Us a non transferable option to claim, for now and for ever more, your immortal soul. Should We wish to exercise this option, you agree to surrender your immortal soul [...]".

58 *Ben-Shahar/Schneider*, The Failure of Mandated Disclosure, University of Pennsylvania Law Review 159 (2011), 647; *Wilkinson-Ryan*, A Psychological Account of Consent to Fine Print, Iowa Law Review 99 (2014), 1745.

59 *McDonald/Cranor*, The Cost of Reading Privacy Policies, I/S: A Journal of Law and Privacy for the Information Society 4 (2008), 540.

processing for the data subject. This kind of notice policy is likely to facilitate the exploitation of two effects: attribute substitution and limited attention spans.

33 On the one hand, empirical evidence suggests that users confronted with lengthy privacy policies have a tendency to use cognitive rules of thumb (heuristics) when making their privacy choices. When the relevant information is not available due to a lack of transparency or high transactions costs, users tend to rely on available information and use it as a substitute for the unavailable information (attribute substitution). Such heuristics may sometimes improve decision making.[60] In the field of privacy however, heuristics seem to impair the quality of choices. Empirical evidence shows that privacy policies are often interpreted as a cue signaling a high level of privacy protection regardless of their content.[61] Similarly, users tend to interpret privacy seals as a guarantee of confidential communication,[62] and ignore salient warnings about dangerous malware when downloading software.[63] Invoking formal privacy policies however, can also reduce trust in the company.[64] This shows that privacy policies are likely to trigger effects that run counter to their regulatory objectives.

34 On the other hand, lengthy privacy policies and large quantities of information increase the complexity of privacy choices. The more information a user is confronted with, the more difficult it becomes to select the relevant information (*information overload*) and make a truly informed but 'frugal' choice. Whether consent is given in light of relevant information, heavily depends on the *cognitive load*, i.e. the level of cognitive effort required by the working memory. Short distractions (a couple of seconds) after presenting a privacy policy significantly lower the perception of risks thereby increasing the propensity to give consent.[65] Limited attention spans provide a further plausible explanation for the ineffectiveness of lengthy privacy policies, especially when user attention is focused on the content features of the service and not its privacy features.

35 At first sight, these findings prompt the conclusion that reducing information, simplifying information formats, and forcing users to focus on privacy policies might improve privacy choices.[66] But again empirical evidence shows that reducing complexity is itself a complex endeavor. Information presented as a 'privacy nutrition label' or in a short table format with clearly structured information seems to facilitate the correct assessment of the level of privacy protection as compared to full-text formats.[67] However, even when confronted with table formats, users have difficulties altering default options in a way that reflects their stated privacy preferences.[68] In a similar vein, a more recent study shows that warning boxes that alert users about the worst-case scenario do not have a significant effect on the comprehension of privacy losses and the propensity to share personal information.[69]

36 In general, providing information to users seems to have a limited impact on privacy choices. The warning effect seems to be particularly weak when the incentives to give consent are salient. A study investigating the effects of monetizing personal information on a duopolistic market shows that a privacy-friendly company has a significantly higher market share (83%) than a privacy-unfriendly company if the information about the level of data protection is salient.[70] Once the privacy-unfriendly company offers a 50 cent discount, the market share of the privacy-friendly company shrinks to between 31 and 13%.[71] These findings are in line with several other studies showing that the willingness to pay for

60 *Gigerenzer/Todd/ABC Research Group*, Simple Heuristics That Make Us Smart (2000); for an investigation of the power of heuristics in the creation and implementation of law *Gigerenzer/Engel (Eds.)*, Heuristics and the Law (2006).

61 *Turow et al.*, The Federal Trade Commission and Consumer Privacy in the Coming Decade, I/S: A Journal of Law and Policy for the Information Society 3 (2008), 723 (730).

62 *Moores*, Do consumers understand the role of privacy seals in e-commerce?, Communications of the ACM 48 (2005), 86; for a recent analysis *Marotta-Wurgler*, Self-Regulation and Competition in Privacy Policies, Journal of Legal Studies 45 (2016), S13 (S17-S30).

63 *Good et al.*, User Choices and Regret: Understanding Users' Decision Process about Consensually Acquired Spyware, I/S: A Journal of Law and Policy for the Information Society 2 (2006), 283 (299).

64 *Martin*, Do Privacy Notices Matter? Comparing the Impact of Violating Formal Privacy Notices and Informal Privacy Norms on Consumer Trust Online, Journal of Legal Studies 45 (2016), S191.

65 *Adjerid et al.*, Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency, Proceedings of the Ninth Symposium on Usable Privacy and Security, 2013, 1 (9).

66 See generally *Ayres/Schwartz*, The No-Reading Problem in Consumer Contract Law, Stanford Law Review 66 (2014), 545 (580-587).

67 *Kelley et al.*, A "Nutrition Label" for Privacy, Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 2009, 1 (9).

68 *Kelley et al.*, A "Nutrition Label" for Privacy, Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 2009, 1 (10-11).

69 *Ben-Shahar/Chilton*, Simplification of Privacy Disclosures: An Experimental Test, Journal of Legal Studies 45 (2016), S41.

70 *Jentzsch/Preibusch/Harasser*, Study on monetising privacy, An economic model for pricing personal information, Report for the European Network and Information Security Agency, 2012, 1 (34-36).

71 *Jentzsch/Preibusch/Harasser*, Study on monetising privacy, An economic model for pricing personal information, Report for the European Network and Information Security Agency, 2012, 1 (36-37).

privacy is generally very low.[72]

37 Perhaps the more significant conclusion relates to the recent proposal to legally compel companies to offer users the choice between a privacy-unfriendly 'free option' and a privacy-friendly 'paid option'.[73] Such a choice, even when bundled with salient information, is likely to appeal to a minority of privacy-sensitive users who are not better informed through additional information. For the majority of users, the temptation of the 'free option' would probably trump the impact of additional information especially when the language used is vague.[74] In sum, it seems that until now there are no good instruments to mitigate the problem of information asymmetries or react to user over-optimism. As long as the EU-GDPR does not specify the requirements as to information formats – for instance pictograms or *one-pagers* –[75] it is unlikely to enable users to make informed privacy choices.

II. Impact of Framing

38 The framing of consent options has been shown to have a significant impact on privacy choices. Generally, people have a tendency to stick with tracking defaults set by digital platforms.[76] The disclosure of personal information is likely to be the product of status quo bias or lacking awareness of exit options. The European legislator has been aware of this problem. Consequently, the EU-GDPR contains a general principle requiring privacy-protective default options. According to Art. 25 § 2 EU-GDPR, companies "shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed". This *privacy by default* principle "applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility".

39 Nevertheless, it is not clear what *privacy by default* precisely means and to what extent it captures the behavioral problems that users are confronted with. While Recital 32 EU-GDPR specifies that a clear affirmative act "could include ticking a box when visiting an internet website", it also allows any other "statement or conduct which clearly indicates [...] the data subject's acceptance" of the processing of personal information. Only "silence, pre-ticked boxes or inactivity" should not be considered as valid consent. In sum, EU privacy law contains two different consent models: explicit consent and implicit (not tacit) consent. Implicit consent might capture cases where users, for instance, type personal information into a web form that uses the HTML standard or JavaScript and contains a privacy notice stating that any such information will be processed. Each consent model relates to empirical findings in behavioral economics.

40 *Explicit consent* and *privacy by default* raise a number of behavioral problems. The initial allocation of a privacy right or a right to consent has a significant impact on the valuation of privacy and the final allocation of personal information even when transaction costs are very low. Obviously, this is not in line with the predictions of the Coase theorem. Consider a group of people that are provided with a high level of privacy and offered the choice to *accept* 2 USD (willingness to accept) for a lower level of privacy, and a group of people that are provided with a low level of privacy and offered the choice to *pay* 2 USD (willingness to pay) for a higher level of privacy.[77] The fraction of people accepting the offer is significantly higher in the former group than in the latter, which indicates that the willingness to pay for strong privacy is significantly lower than the willingness to accept money for weak privacy.[78] This effect is usually associated with *endowment effects*, i.e. the fact that people have a higher valuation for objects they possess than for objects they do not

72 *Rose*, Data Users versus Data Subjects: Are Consumers Willing to Pay for Property Rights to Personal Information?, Proceedings of the 38th Hawaii International Conference on System Sciences, 2005, 1; *Hann et al.*, Overcoming Online Information Privacy Concerns: An Information Processing Theory Approach, Journal of Management Information Systems 24 (2007), 13 (28); *Carrascal et al.*, Your Browsing Behavior for a Big Mac: Economics of Personal Information Online, Proceedings of the 22nd International Conference on World Wide Web, 2013, 189; *Beresford/Kübler/Preibusch*, Unwillingness to pay for privacy: A field experiment, Economics Letters 117 (2012), 25.

73 For a brief discussion *Borgesius*, Behavioural Sciences and the Regulation of Privacy on the Internet, in Alemanno/Sibony (Eds.), Nudge and the Law: A European Perspective (2015), 179 (201-202).

74 For an assessment of vagueness see *Reidenberg et al.*, Ambiguity in Privacy Policies and the Impact of Regulation, Journal of Legal Studies 45 (2016), S163.

75 A condensed information format (one-pager) has been proposed on the German 2015 IT summit in cooperation with the Federal Ministry of Justice and Consumer Protection (<http://www.bmjv.de/SharedDocs/Pressemitteilungen/DE/2015/11192915_Vorstellung_OnePager.html>).

76 *Sunstein*, The Storrs Lectures: Behavioral Economics and Paternalism, Yale Law Journal 122 (2013), 1826 (1893).

77 *Acquisti/John/Loewenstein*, What Is Privacy Worth?, Journal of Legal Studies 42 (2013), 249 (260-262).

78 *Acquisti/John/Loewenstein*, What Is Privacy Worth?, Journal of Legal Studies 42 (2013), 249 (264-268). The results suggest that this effect (WTA-WTP ratio: 5/1) is stronger than with normal goods (WTA-WTP ratio: 2,5/1). See also *Grossklags/Acquisti*, When 25 cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information, Proceedings of the Sixth Workshop on the Economics of Information Security (WEIS 2007), 1.

possess.[79] A related explanation builds on *prospect theory* and states that losses loom larger than equal gains (*loss aversion*), even when no risk is involved.[80]

41 The analysis becomes slightly more complicated when considering the design of choice frames without strong monetary incentives. Consider the case in which users are presented either with the option *"I would like to benefit from targeting. I give my consent...☐"* or the option *"I would like to refuse targeting. I do not give my consent...☐"*. While the former is framed as an opt-in (*gains frame*), the latter is framed as opt-out (*loss frame*). Empirical evidence suggests that the willingness to give consent is significantly higher with an opt-out than with an opt-in in similar cases.[81] This effect, however, changes when users are presented with the same options – the only difference being that the respective box is pre-ticked: *"...☑"*. In this case, consent rates are relatively similar across both reverse default options and take an intermediate value between those yielded by the regular default options.[82] A possible explanation is that pre-ticked boxes raise people's awareness that a choice is being made and that they should actively think about whether to stick with the status quo. Assuming that these results can be generalized, the EU-GDPR seems to have found a decent solution to the behavioral problems of default options with respect to consent. However, some problems remain.

42 First, it is not clear whether and to what extent *privacy by default* and the prohibition of pre-ticked boxes apply to other privacy choices than consent, such as the withdrawal of consent or deletion. As it seems, companies may well be allowed to use loss frames and pre-ticked boxes in the design of withdrawal options (*"I do not withdraw my consent...☐"* or *"...☑"*). Companies could use these loopholes to lower withdrawal rates and use confusing default options once consent has been given. Instead of primarily regulating choices over the initial collection of personal information (i.e. consent), it would probably make sense if EU privacy law held a stronger grip on choices over downstream uses. This may become particularly important for Big Data analytics. In some cases, Big Data analytics can generate personal information that did not exist when the user gave their consent. Some users will not want the newly generated information to be used, whereas some of them would not have given their consent initially had they known that Big Data analytics would generate this piece of information out of an innocuous piece of information. Downstream control like withdrawal and deletion then becomes crucial. In a similar vein, a strict implementation of *privacy by default* sets an incentive for companies to engage in more aggressive data gathering strategies, for instance extending the scope of processing purposes. Somewhat relaxing the requirements for initial consent and requiring a specific and properly framed consent renewal for the use of newly generated personal information might mitigate this problem to a certain extent.

43 Second, the problem of most investigations of default options is that they do not consider the effects of cumulative choice options. Digital platforms collect all kinds of personal information for a variety of purposes. This entails a high number of choice options. Some time ago, Facebook allegedly offered users up to 50 settings with 170 choice options scattered all over the network.[83] The higher the number of control options and default rules, the more time consuming and costly it becomes for users to think about these options and change them. An extensive scope of *privacy by default* might therefore lead to a situation where defaults have the same effects as an unchangeable fixed option. This becomes a problem when the bulk of default settings contain options set in a way that do not reflect users' privacy preferences. Furthermore, a high number of default options might also make it difficult to assess how defaults should be altered. Empirical evidence suggests that users have difficulties understanding the meaning of an opt-out (that stops tracking or targeted ads), which eventually induces them to opt-out even though it does not reflect their true privacy preferences.[84] Privacy-sensitive users have been shown to set defaults to delete cookies and thereby also delete opt-out cookies, thus diminishing their level of privacy protection instead of increasing it.[85] This shows that providing users with granular

79 *Kahneman/Knetsch/Thaler*, Experimental Tests of the Endowment Effect and the Coase Theorem, Journal of Political Economy 98 (1990), 1325; *Kahneman/Knetsch/Thaler*, Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias, Journal of Economic Perspectives 5 (1991), 193; *Plott/Zeiler*, The Willingness to Pay-Willingness to Accept Gap, the „Endowment Effect", Subject Misconceptions, and Experimental Procedures for Eliciting Valuations, American Economic Review 95 (2005), 530.

80 *Kahneman/Tversky*, Prospect Theory: An Analysis of Decision Under Risk, Econometrica 47 (1979), 263; *Tversky/Kahneman*, Loss Aversion in Riskless Choice: A Reference-Dependent Model, Quarterly Journal of Economics 106 (1991), 1039 (1047); for a critical summary see *Barberis*, Thirty Years of Prospect Theory in Economics: A Review and Assessment, Journal of Economic Perspectives 27 (2013), 173.

81 *Johnson/Bellman/Lohse, Defaults*, Framing, and Privacy: Why Opting In-Opting Out, Marketing Letters 13 (2002), 5 (7) (opt-out: 96.3 % consent rate / opt-in: 48.2 % consent rate).

82 *Johnson/Bellman/Lohse, Defaults*, Framing, and Privacy: Why Opting In-Opting Out, Marketing Letters 13 (2002), 5 (9) (around 70 % consent rate).

83 *Tucker*, Social Networks, Personalized Advertising, and Privacy Controls, Journal of Marketing Research 51 (2014), 546 (549).

84 *Leon et al.*, Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising, CHI 2012, 1 (1).

85 *Leon et al.*, Why Johnny Can't Opt Out: A Usability Evaluation

control through an extensive use of default options is likely to backfire.

44 Some of these behavioral problems could be solved through the use of technical privacy assistants or privacy bots that help users with default configurations for different types of personal information. These assistants might offer a few general settings (for average users) and a range of more specific settings (for more sophisticated users) that would eventually be applied to all services – browsers, search engines and platforms – and hence reduce the burden of opt-in choices. Without such a technological solution, *privacy by default* would require consent before the use of each single service on a case-by-case basis. This would increase the cost of the consent procedure and eventually deter users from making a deliberate privacy choice in every single case.

45 Third, privacy-protective default options could have drawbacks on the level of competition. On the one hand, privacy-protective defaults and restrictions of information flows in general might create incentives for firms to merge or build technological barriers against switching to facilitate the exchange of information within the firm or lock-in users.[86] This is not an insurmountable problem per se because competition authorities can assess these effects in their merger control procedures. However in the past, competition authorities like the European Commission have been reluctant to operate an in-depth analysis of the interaction between privacy and the level of competition in these procedures, like the *Google/DoubleClick* merger.[87] On the other hand, privacy-protective defaults might preclude small or specialized services from entering the market and bolster the position of incumbent generalist services (GoogleNews, Visa).[88] This in turn might bolster the position of generalist services and deprive users of higher-quality services. These findings prompt the conclusion that reducing the cost of consent through a single interface of privacy settings for every service used (a kind of 'flat privacy option') and somewhat relaxing the requirement of case-by-case ex ante consent might actually foster competition and increase the level of privacy.

46 The protection of privacy becomes even thornier in case of *implicit consent*. Under the rational choice paradigm, users should minimize the time spent on and the risks associated with the disclosure of personal information. Recent findings cast doubt on this hypothesis and show that users willingly provide personal information even when doing so is optional.[89] However, this over-disclosure effect seems to be weaker when companies additionally require some types of personal information through mandatory fields. Voluntary over-disclosure might be driven by social norms (visibility of other users' disclosure behavior), reciprocity towards the service and monetary rewards. This indicates that companies might have an incentive not to condition the use of their service on consent. Instead they might simply make consent optional, increase the visibility of other users' behavior and set incentives for disclosure, thereby escaping the prohibition enshrined in Art. 7 § 4 EU-GDPR and maximizing the inflow of personal information. Implicit consent is likely to be the prime channel for information disclosure, but the EU-GDPR says very little about how to mitigate the awareness and attention problems that might be associated with implicit choice.

III. Impact of Time

47 One of the least understood factors that might influence users' privacy choices and explain the privacy paradox is time. Generally, behavioral economics shows that people are subject to bounded willpower when making intertemporal choices.[90] This means that people have a tendency to procrastinate and opt for immediate benefits. For instance, many people prefer a payment of 110 Euros 'a year and a week from now' over a payment of 100 Euros 'a year from now', while favoring a payment of 100 Euros 'now' over a payment of 110 Euros 'a week from now'.[91] While this kind of present bias or myopia is

of Tools to Limit Online Behavioral Advertising, CHI 2012, 1 (9).

86 See *Picker*, Competition and Privacy in Web 2.0 and the Cloud, Northwestern University Law Review Colloquy 103 (2008), 1 (10).

87 Commission decision of 11/03/2008 declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement (Case No COMP/M.4731 – Google/ DoubleClick), C(2008) 927 final; see also *Edwards*, Stepping Up to the Plate: the Google-DoubleClick Merger and the Role of the Federal Trade Commission in Protecting Online Data Privacy, Working Paper (2008), 1 (<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370734>); *Rodrigues*, Privacy on Social Networks: Norms, Markets, and Natural Monopoly, in: Levmore/Nussbaum (Eds.), The Offensive Internet, 2010, 237.

88 *Campbell/Goldfarb/Tucker*, Privacy Regulation and Market Structure, Journal of Economics & Management Strategy 24 (2015), 47 (48).

89 *Preibusch/Krol/Beresford*, The Privacy Economics of Voluntary Over-disclosure in Web Forms, in Böhme (Ed.), The Economics of Information Security and Privacy (2013), 183 (203).

90 *O'Donoghue/Rabin*, The Economics of Immediate Gratification, Journal of Behavioral Decision Making 13 (2000), 233; *O'Donoghue/Rabin*, Choice and Procrastination, Quarterly Journal of Economics 116 (2001), 121.

91 *Frederick/Loewenstein/O'Donoghue*, Time Discounting and Time Preference: A Critical Review, Journal of Economic

captured by models of hyperbolic discounting, it is not entirely clear whether it really results from a distortion of preferences and what the underlying psychological processes are. The debate about utility functions notwithstanding, the model helps explain several phenomena of self-harming over-consumption; for instance when people overuse their credit card at the beginning of the month or when they eat more fast food than healthy meals.[92] In a similar vein, empirical evidence suggests that users tend to underestimate the long-term risks associated with the disclosure of personal information.[93]

48 Three general tendencies are likely to be observed. First, the longer the time period between consent and the use of personal information, the less likely it is that the user will have considered the risk when consenting. Second, the stronger and the more immediate the rewards from consent, the stronger the underestimation effect. Third, the more intangible the consequences of the use of personal information, the stronger the underestimation effect.[94] These factors might even push people to alter privacy-protective default options and eventually curb the impact of *privacy by default*.[95] More importantly, models of hyperbolic discounting help us to understand how companies might try to exploit myopia to extract more personal information through minimal rewards for consent.

49 The problem becomes clear when comparing a service offering a privacy-unfriendly 'consent option' and a privacy-friendly 'paid option' in a simple model.[96] Suppose that the price for the paid option remains constant over time and that the user only uses one service, maybe due to lock-in effects. Assume that the price of the service over two periods is $p_{paid} = p_{t1} + p_{t2}$, where t1 denotes the point of time when the user begins using the service and t2 denotes some posterior point of time when the service is actually used. Now suppose that the service can extract higher rents from users through *behavioral targeting* but that this practice requires consent to the processing of personal information. The potential to extract a higher rent later on allows the company to lower the price in the first period. It might set $p_{consent} = p_{t1} - c + p_{t2} + \delta p_a$, where p_a denotes the price increase in the second period, c the monetary discount for consent and δ the bias resulting from hyperbolic discounting. If users underestimate p_a because of their cognitive bias, they might think that the consent option is cheaper than the paid option. This is the case if $p_{t1} - c + p_{t2} + \delta p_a \leq p_{t1} + p_{t2}$.

50 The company will then offer users a discount $c \geq \delta p_a$ for giving their consent. The stronger the error, the higher the discount that companies can offer their users. This simple analysis shows that the perception of the service as being 'free' will often be an illusion. More importantly, it shows that assessing consent only makes sense when considering the extent to which personal information may be used to extract user rents in later periods. This will depend on the purposes of data processing. Allowing the processing of personal information for the purpose of the 'analysis of Big Data' is not only conceptually circular. Unspecified purposes are likely to facilitate the exploitation of biases in general and myopia in particular.

51 In light of these findings, behavioral economists tend to conclude that over long time horizons, i.e. if people have to anticipate the long-term costs and risks of their choices in the present, they often fail to make choices that reflect their true preferences and impose externalities on their future selves (*internalities*).[97] Turning positive analysis into a normative conclusion, some authors claim that this constitutes a kind of *behavioral market failure* justifying government interventions.[98] The problem is that until now there is no firm reason why we could or should assume a superior second-order preference of the future self over the present self and hence restrict choices in the present.[99]

Literature 40 (2002), 351 (361). Hyperbolic discounting does not necessarily coincide with a reversal of preferences as described in my example.

92 *Jolls*, Behavioral Law and Economics, in Diamond/Vartiainen (Eds.), Behavioral Law and Economics and Its Applications (2007), 115 (124-125).

93 *Acquisti/Grossklags*, Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting, in Camp/Lewis (Eds.), The Economics of Information Security (2004), 165; *Strandburg*, Social Norms, Self Control, and Privacy in the Online World, in Strandburg/Raicu (Eds.), Privacy and Technologies of Identity: A Cross-disciplinary Conversation, 2006, 31 (39).

94 For the general mechanism see *Rick/Loewenstein*, Intangibility in intertemporal choice, Philosophical Transactions of the Royal Society 363 (2008), 3813.

95 For an assessment in context see *Willis*, When Nudges Fail: Slippery Defaults, University of Chicago Law Review 80 (2013), 1155 (1216-1217).

96 The following thoughts have a flavor of the more complex models discussed by *Gabaix/Laibson*, Shrouded Attributes, Consumer Myopia, and Information Suppression in Competitive Markets, Quarterly Journal of Economics 121 (2006), 505 (512); *Bar-Gill*, Bundling and Consumer Misperception, University of Chicago Law Review 73 (2006), 33 (39–46); *Bar-Gill*, The Behavioral Economics of Consumer Contracts, Minnesota Law Review 92 (2008), 749 (774).

97 *Herrnstein et al.*, Utility Maximization and Melioration: Internalities in Individual Choice, Journal of Behavioral Decision Making 6 (1993), 149 ff.; *Loewenstein/Haisley*, The Economist as Therapist: Methodological Ramifications of "Light" Paternalism, in Caplin/Schotter (Eds.), The Foundations of Positive and Normative Economics: A Handbook, 2008, 210 (212).

98 *Sunstein*, The Storrs Lectures: Behavioral Economics and Paternalism, Yale Law Journal 122 (2013), 1826 (1842 sq.).

99 *Rizzo/Whitman*, Little Brother Is Watching You: New

52 Does this mean that privacy law should ignore users' tendency to opt for immediate rewards and give their consent? I do not believe so. Privacy law could take account of myopia without resorting to outright paternalism.

53 On the one hand, privacy lawyers could implement some of the interpretive rules known from contract law. Long time horizons might justify the application of the *ambiguity rule* enshrined in § 305c II of the German Civil Code. According to this interpretive rule, a provision in a standard form contract is considered invalid when there are doubts about its exact content and meaning (*interpretatio contra proferentem*). A similar rule could be applied when interpreting consent or contract terms on consent.

54 The primary effect of such an interpretive rule would be to increase the burden of proof that companies already carry under Art. 7 § 1 EU-GDPR. Furthermore, it would compel companies to seek consent renewal after longer time periods.

55 On the other hand, privacy law could try to mitigate the problem of myopia through cooling-off periods. Consent options could be designed such that users have to reconsider their opt-in after the initial opt-in. § 7 II of the German Law on Unfair Commercial Practices, for instance, requires a *double opt-in* (DOI) when consenting to commercial ads. In this case, consent is only valid if the user opts in twice, the second opt-in usually being given through a clickbox in an email that confirms that the user has previously opted in (combination of two opt-in defaults). Another solution could be to require a *confirmed opt-in* (COI). In this case, consent would only be valid if the user does not opt out after being reminded that she has previously opted in (combination of an opt-in and an opt-out default). Finally, an intermediate solution could be to use a pre-ticked box for the second choice to be made. Since DOI and COI would generally increase protection of users, the use of pre-ticked boxes would probably not be prohibited by Recital 32 EU-GDPR.

IV. Impact of Control

56 The general approach of EU privacy law is to provide users with rights to control the various steps of the processing of personal information – like consent to processing (Art. 7 § 1 EU-GDPR), withdrawal of consent (Art. 7 § 3 EU-GDPR), access to data (Art. 15 EU-GDPR), rectification of data (Art. 16 EU-GDPR), deletion of data (Art. 17 EU-GDPR), restriction of processing (Art. 18 EU-GDPR), portability of data (Art. 20 EU-GDPR) or objection to processing (Art. 21 EU-GDPR). On a deontological view, control might be considered as a precept of autonomy and the fundamental right to data protection under Art. 8 of the EU Charter of Fundamental Rights. However on a consequentialist view, control might trigger behaviors that are incompatible with the objectives of user empowerment through rights.

57 Generally, psychological evidence shows that control over some risks associated with an activity might induce users to neglect or underestimate other risks resulting from the same activity, thus creating an illusion of control.[100] Similar problems may arise when increasing control over single steps of the processing of personal information. Empirical evidence suggests that increasing the degree of control over the release of personal information may induce users to underestimate the risks associated with the use of personal information.[101] In a similar vein, a recent field study shows that facilitating the use of the privacy control interface on Facebook and increasing control over the type of personal information and third-party tracking significantly increases the propensity to share personal information.[102] The upshot of these findings is that rights to control are ambiguous tools.

58 If the objective of such rights is to facilitate the objective level of control, this objective will probably be achieved – especially for sophisticated users. If, however, the objective is to improve the matching of true privacy preferences and objective privacy risks, control rights might have effects that run counter to these objectives. In social networks, there is a risk that users might confound control vis-à-vis other users and control vis-à-vis the company. Giving users control over the visibility of personal information for other users might trigger the illusion that they are not being tracked by the company either. In sum, making control options more granular will not only increase the costs of privacy choices; it also has the potential to mislead users and impair the quality of privacy choices. How could EU privacy law guarantee a sound level of granularity of control without disempowering users?

Paternalism on the Slippery Slopes, Arizona Law Review 51 (2009), 685 (701); in the context of privacy law *Jolls*, Rationality and Consent in Privacy Law, Working Paper, 2010, 1 (51).

100 *Peltzman*, The Effects of Automobile Safety Regulation, Journal of Political Economy 83 (1975), 677; for a metastudy *Klein/Helweg-Larsen*, Perceived Control and the Optimistic Bias: A Meta-Analytic Review, Psychology and Health 17 (2002), 437.

101 *Brandimarte/Acquisti/Loewenstein*, Misplaced Confidences: Privacy and the Control Paradox, Social Psychological and Personality Science 4 (2013), 340.

102 *Tucker*, Social Networks, Personalized Advertising, and Privacy Controls, Journal of Marketing Research 51 (2014), 546.

59 One possibility could be the use of technical user assistants or privacy bots based on artificial intelligence and smart (personalized) defaults.[103] Big Data analytics and artificial intelligence could be used to generate information about users' privacy preferences and design technical user assistants and default rules tailored to these preferences – just like targeted ads are tailored to consumption preferences. These assistants or defaults would require a one-time (mandated) active choice for specific types of services and data and then learn from users' past choices. The advantage is that the initial setup of the assistant or default would require full user awareness and then allow for granular control without having to make an active choice each and every time. This would reduce the costs of privacy choices.

60 The obvious disadvantage is that such assistants or defaults would be quite intrusive and require the processing of personal information.[104] Furthermore, users might become entrenched in their past privacy choices which might become a problem when the assistant or default determines the kind of information that users are exposed to, for instance in a social network. This might eventually lead to filter bubbles or echo chambers.[105] Finally, alleviating users from the burden of choice might undermine learning and hamper the emergence of new tastes and preferences. To a certain extent, these problems could be solved through limited data retention periods and the renewal of privacy settings on a regular basis. Choice renewals would compel users to start with a clean slate, thereby limiting the effects of status quo bias and raise users' awareness. To conclude, personalized technical assistants and defaults are not a panacea, but it is difficult to see how control could really work out in practice without any kind of technical assistance.

D. Behavioral Privacy Law and the Problem of 'Mixed Rationalities'

61 Some authors have suggested that the legislator could or should nudge users towards disclosing less personal information.[106] Others have seen nudges as a threat to privacy.[107] Moreover, some lawyers have qualified the prohibition principle enshrined in Art. 6 § 1 EU-GDPR as straightforward 'interventionist paternalism' and *privacy by default* enshrined in Art. 25 § 2 EU-GDPR as 'libertarian paternalism' and hence a paternalistic nudge.[108] These claims notwithstanding, the understanding of nudges is rather vague.[109] According to the proponents of libertarian paternalism, a nudge describes any kind of intervention affecting "the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid."[110] Other authors have taken a broader approach to libertarian paternalism as a set of interventions designed to overcome unavoidable cognitive biases to approximate autonomous choices under idealized conditions.[111] One of the problems of the nudging debate is that the *objectives* and *effects* of regulatory tools are often swept under the rug. In addition, there is usually no precise discussion about how the objectives and effects of nudges are or should be related. Consequently, all kinds of regulatory tools and interventions are considered as nudges, even when neither their goals nor their effects are really clear. This translates into a legal problem when determining the grounds on which the intervention may be justified.

62 Consider default options in privacy law. Without any further specification of the objective and effects of a default rule, it does not make sense to qualify a default option as a nudge. As I have shown above, an opt-in default may be justified on different legal grounds.

63 If the purpose of an opt-in default is to set a strategic incentive for companies to disclose better information for users, it aims at reducing information asymmetries and hence a market failure. Similarly,

103 *Sunstein*, Deciding by Default, University of Pennsylvania Law Review 162 (2013), 1; *Porat/Strahilevitz*, Personalizing Default Rules and Disclosure with Big Data, 112 Michigan Law Review 112 (2014), 1417; *Sunstein*, Choosing Not to Choose (2015), 157-173.

104 *Porat/Strahilevitz*, Personalizing Default Rules and Disclosure with Big Data, 112 Michigan Law Review 112 (2014), 1417 (1467-1469); *Sunstein*, Choosing Not to Choose (2015), 169-173.

105 See *Pariser*, The Filter Bubble: How the New Personalized Web is Changing What We Read and How We Think (2012).

106 *Acquisti*, Nudging Privacy: The Behavioral Economics of Personal Information, IEEE Security & Privacy, November/December 2009, 82; *Balebako et al.*, Nudging Users Towards Privacy on Mobile Devices, CHI 2011, 1; *Wang et al.*, Privacy Nudges for Social Media: An Exploratory Facebook Study, PSOSM 2013, 1; *Wang et al.*, A Field Trial of Privacy Nudges for Facebook, CHI 2014, 1; *Ziegeldorf et al.*, Comparison-based Privacy: Nudging Privacy in Social Media (2015), 1.

107 *Kapsner/Sandfuchs*, Nudging as a threat to privacy, Review of Philosophy and Psychology 6 (2015), 455.

108 *Krönke*, Datenpaternalismus. Staatliche Interventionen im Online-Datenverkehr zwischen Privaten, dargestellt am Beispiel der Datenschutz-Grundverordnung, Der Staat 55 (2016), 319 (325-330).

109 *Dworkin*, Paternalism, in Zalta et al. (Eds.), Stanford Encyclopaedia of Philosophy Online, 2016 (<https://plato.stanford.edu/entries/paternalism/>).

110 *Sunstein/Thaler*, Nudge: Improving Decisions About Health, Wealth, and Happiness (2008), 6.

111 *Rebonato*, Taking Liberties: A Critical Examination of Libertarian Paternalism (2012), 6.

an opt-in default could be used to mitigate collective action problems and the negative externalities associated with an unconstrained disclosure of personal information. The prime purpose of such a default would not be to protect users against themselves but to enhance the efficiency of contracts between companies and users. In both cases, it would not make much sense to qualify the default option as a paternalistic nudge, since the default rule could more aptly be justified within the standard economic framework and the traditional approach to market failures.

64 However, if the purpose of an opt-in default is to correct the effects of over-optimism and exploit users' status quo bias, it aims at correcting supposedly distorted privacy preferences or at helping users to avoid individual mistakes, i.e. violations of the axioms posited by rational choice theory. Its prime purpose would be to protect users against mistaken privacy choices. It would then be a nudge in the sense of libertarian paternalism.

65 More generally, this shows that not every type of privacy regulation informed by behavioral economics can reasonably be qualified as a paternalistic nudge. Sometimes, an intervention that seems to be justified on the grounds of libertarian paternalism at first sight might well be justified as a correction of a market failure within the standard economic framework. Simply put, it might make sense to increase the depth of the legal 'duck test' when determining whether an intervention actually is a paternalistic nudge and how the intervention may be justified legally.[112] An intervention may look like a paternalistic nudge (look like a duck), but it might not pursue the objectives or have the effects of a paternalistic nudge (walk, swim and quack like a duck). Therefore, it is crucial to draw a sharper distinction between *libertarian paternalistic regulation* and *non-paternalistic soft regulation*.[113]

66 The law offers various doctrinal frameworks to implement this distinction, most notably the principle of proportionality. According to this principle, a government intervention is justified if it pursues a legitimate objective, if it is suitable and necessary to achieve this objective, and if the costs of the intervention – the weight of the infringement of an individual right – are not disproportionate to its benefits (balancing test).[114]

67 The assessment of the *legitimate objective* is purely normative. The legislator has discretionary powers in determining these objectives but there is a large consensus that the protection of the public interest is easier to justify than outright paternalism.[115] The correlate of discretion is the constitutional duty to specify and justify the objectives. Some of the normative misunderstandings could be solved if the rules of privacy law specified whether an intervention aims at protecting users against themselves (paternalism) or at correcting a market failure (public interest).[116] A nudge used to correct a market failure resulting from unfettered consent should be easier to justify than a nudge to protect against mere harm to the self.

68 The *suitability test* requires an empirical assessment of facts. The suitability threshold is rather low and met if the intervention potentially furthers the legitimate objective. On this level of the test, the assessment might draw a distinction between interventions that mainly correct biases (*debiasing*) and those that mainly reinforce existing cognitive biases for the regulatory objective (*rebiasing*).[117] In general, interventions based on the behavioral insights presented in the previous sections will potentially generate the intended effect. Behavioral insights, for instance about the unintended consequences of too much information or control, could be used to somewhat increase the depth of the suitability test and hence the burden of justification imposed on regulators.

69 The *necessity test* can be considered as a legal implementation of pareto-optimality.[118] The

112 The 'duck test' is often phrased as follows: "This bird has no label that says 'duck'. But the bird certainly looks like a duck. Also, he goes to the pond and you notice that he swims like a duck. Then he opens his beak and quacks like a duck. Well, by this time you have probably reached the conclusion that the bird is a duck, whether he's wearing a label or not." The origin of the phrase is not clear but often attributed to US ambassador Richard Cunningham Patterson Jr., see *Immerman*, The CIA in Guatemala: The Foreign Policy of Intervention (1982), 102.

113 *Sunstein*, The Ethics of Nudging, Yale Journal on Regulation 32 (2015), 413 (426), distinguishes between *paternalistic nudges* and *market failure nudges*.

114 *Harbo*, The Function of the Proportionality Principle in EU Law, European Law Journal 16 (2010), 158 (165).

115 *Schweizer*, Chapter 7: Nudging and the Principle of Proportionality, in Mathis/Tor (Eds.), Nudging – Possibilities, Limitations and Applications in European Law and Economics (2016), 93 (102-106).

116 *Dworkin*, Paternalism, in Zalta et al. (Eds.), Stanford Encyclopaedia of Philosophy Online, 2016 (<https://plato.stanford.edu/entries/paternalism/>).

117 *Larrick*, Chapter 16: Debiasing, in Koehler/Harvey (Eds.), Blackwell Handbook of Judgment and Decision Making (2004), 316; *Soman/Liu*, Debiasing or rebiasing? Moderating the illusion of delayed incentives, Journal of Economic Psychology 32 (2011), 307 (309), define *rebiasing* as the use of a second bias to offset the effects of the original bias while achieving the same result as *debiasing*. On a legal view, however, there could be cases where the regulatory purpose of *rebiasing* would be distinct from that of *debiasing*.

118 *Alexy*, A Theory of Constitutional Rights (2002), 66-69; *Petersen*, How to Compare the Length of Lines to the Weight of Stones: Balancing and the Resolution of Value Conflicts in Constitutional Law, German Law Journal 14 (2013), 1387

threshold is met if the least restrictive (coercive) but equally effective means of achieving the objective is implemented. Nudges or soft regulation will usually be the least coercive means with the potential to be as effective as outright coercion. Notably, the effect of default options is not weaker when people are told that the chosen default is usually effective.[119] Therefore, soft interventions need not be subliminal; they can and should be transparent and be subject to judicial scrutiny.[120] Perhaps the most important consideration is that designing effective nudges will often be complex and costly.[121] Designing privacy-protective default options, for instance, requires very granular regulation capturing the details of choice frames. The crucial question is whether the freedom benefits of such a legal nudging framework will really outweigh its costs. This should be assessed in the *balancing prong* of the proportionality principle, where the scales could be tilted against soft regulation in favor of traditional regulation in a surprisingly large number of cases.

E. Conclusion

70 In this article, I have argued that the legal problems raised by consent and the monetization of personal data cannot be solved without considering how users actually behave. By the same token, I have tried to flesh out some of the 'sweet spots' where privacy law could step in to steer privacy choices. My argument rests on the claim that it is not sufficient to design the rules of privacy law on the grounds of either a standard economics or a behavioral economics analysis. To fully capture the regulatory problems addressed by privacy law, we need both.

71 Looking through the lens of game theory, I have argued that consent will often reflect a rational choice. In networked environments, the protection of privacy has the features of a collective action problem. In this dilemma, consent can be considered as a rational choice yielding a suboptimal level of collective privacy and imposing negative externalities on other users. Looking through the lens of behavioral economics, I have argued that bounded rationality and bounded willpower will often make it difficult for users to make choices according to their stated privacy preferences. While the impact of information is rather low when consent is incentivized, framing, time and control have a strong impact on privacy choices. Companies have an incentive to exploit these effects and take advantage of bounded rationality. However, the combined analysis shows that we should be very cautious when assessing the objectives and effects of what has come to be called a privacy nudge.

72 On the one hand, debiasing users, i.e. facilitating rational choices, could well accelerate the erosion of privacy in environments relying on the use of Big Data. This result casts doubt on the implicit assumption that informing users would push them to disclose less personal information. On the other hand, using privacy-protective nudges to constrain users' propensity to disclose personal information may not only be justified to correct cognitive biases and behavioral market failures. Such restrictions might well be justified to cope with public goods problems and counter negative externalities. In this case, the nudge would not qualify as an intervention on the grounds of *libertarian paternalism* but on the grounds of *non-paternalistic soft regulation*.

73 Accordingly, the scope of libertarian paternalism and nudging in the paternalistic sense might be much smaller in privacy law than the existing literature suggests. Collective action problems in Big Data environments or the privacy externalities associated with unraveling might even justify stricter restrictions, such as sectoral prohibitions. An integrated approach combining competition law, consumer protection law, and data protection law might be the most adequate to address the regulatory problems associated with the continuous monetization of privacy.[122] In the end, behavioral and traditional interventions in privacy law should be used as complements, not substitutes.

(1394).

119 *Loewenstein et al.*, Warning: You are about to be nudged, Behavioral Science & Policy 1(2015), 35.

120 *Sunstein*, The Ethics of Nudging, Yale Journal on Regulation 32 (2015), 413 (428).

121 *Willis*, When Nudges Fail. Slippery Defaults, University of Chicago Law Review 80 (2013), 1155 (1161); *Bubb/Pildes*, How Behavioral Economics Trims Its Sails and Why, Harvard Law Review 127 (2014), 1595.

122 *Kerber*, Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection, GRUR Int. 2016, 639.