Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law

Christoph Busch†

This Essay explores how the rise of big data and algorithm-based regulation could fundamentally change the design and structure of disclosure mandates in consumer law and privacy law. Impersonal information duties and standardized notices could be replaced by granular legal norms that provide personalized disclosures based on the personal preferences and informational needs of an individual. This Essay makes several contributions to the emerging debate about personalized law. First, it shows how information technology can be implemented for tailoring disclosures in consumer law and privacy law in order to take into account actor heterogeneity. Second, it argues that personalized disclosures should be conceived as a learning system based on feedback mechanisms in order to continuously improve the relevance of the information provided. Third, this Essay explores the ramifications of personalization for compliance monitoring and enforcement. Finally, this Essay claims that, with the advent of the Internet of Things, the wave of the future, at least in data privacy law, could be a mix of personalized defaults implemented through virtual personal assistants and only occasional active choices.

INTRODUCTION

Mandated disclosures are probably one of the most widely used regulatory tools in consumer law and data privacy law on both sides of the Atlantic.[1] Long lists of standardized information duties are the hallmark of EU consumer law directives, which are based on the information paradigm and the model of the average consumer.[2] Similarly, mandated disclosures are a standard staple

† Professor of Law at the University of Osnabrück, Germany. I am grateful to the participants of The University of Chicago Law Review Symposium on Personalized Law organized by Omri Ben-Shahar, Anthony Casey, Ariel Porat, and Lior Strahilevitz in April 2018 for their very helpful comments and suggestions. I would also like to thank Alberto De Franceschi and the participants of the conference on Granular Legal Norms at Villa Vigoni in March 2017 for their insightful inputs.

1 See Omri Ben-Shahar and Carl E. Schneider, *More than You Wanted to Know: The Failure of Mandated Disclosure* 3 (Princeton 2014) ("'Mandated disclosure' may be the most common and least successful regulatory technique in American law.").

2 For an overview of disclosure mandates in EU consumer law, see Christoph Busch, *The Future of Pre-contractual Information Duties: From Behavioural Insights to Big Data*, in Christian Twigg-Flesner, ed, *Research Handbook on EU Consumer and Contract Law* (Elgar

of American consumer protection law.[3] One of the reasons why disclosure mandates are so popular with lawmakers is their "ecumenical" nature.[4] For those who believe in the free-market principle, information duties have the advantage of regulating lightly and minimizing market interference. From this perspective, mandated disclosures improve the functioning of markets by helping to overcome information asymmetries without distorting markets by specifying prices, quality, or contracts terms. In contrast, for those who focus on consumer autonomy, mandated disclosures are a well-suited tool for increasing consumer self-determination and promoting consumer empowerment.

Similarly, despite many fundamental differences with regard to data protection, the "information paradigm" is a common element of data privacy law both in the United States and Europe. Contemporary data protection laws rest on what Professor Daniel Solove has called a model of "privacy self-management."[5] Under this model, consumers shall exercise control over their personal data and make informed decisions about the use of their data. Thus, "notice and choice" has become the key element of self-regulation of fair information practices in the United States.[6] Under this approach, "notice" is generally described in terms of transparency of the information practices, while "choice" is typically defined in terms of consent.[7] European data protection law, while more restrictive than US privacy law, also largely rests on a model of "notice and choice."[8] Thus, under Article 6 of the recently enacted EU General

---

2016) 221, 224–25. See also generally Peter Rott, *Information Obligations and Withdrawal Rights*, in Christian Twigg-Flesner, ed, *The Cambridge Companion to European Union Private Law* 187 (Cambridge 2010); Thomas Wilhelmsson and Christian Twigg-Flesner, *Pre-contractual Information Duties in the* Acquis Communautaire, 2 Eur Rev Contract L 441 (2006); Christian Twigg-Flesner and Thomas Wilhelmsson, *Article 2:201: Duty to Inform about Goods or Services*, in Research Group on the Existing EC Private Law, ed, *Principles of the Existing EC Contract Law (Acquis Principles): Contract II* 115–19 (Sellier 2009).

3 For an overview of disclosure mandates in US consumer law and other areas of law, see Omri Ben-Shahar and Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U Pa L Rev 647, 651–65 (2011).

4 See Ben-Shahar and Schneider, *More than You Wanted to Know* at 5–6 (cited in 1).

5 See generally Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 Harv L Rev 1880 (2013).

6 See Joel R. Reidenberg, et al, *Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding*, 30 Berkeley Tech L J 39, 42–46 (2015). See also generally Ari Ezra Waldman, *Privacy as Trust: Information Privacy for an Information Age* 80–83 (Cambridge 2018).

7 See Reidenberg, 30 Berkeley Tech L J at 43–44 (cited in note 6).

8 See id at 44–46.

Data Protection Regulation (GDPR),[9] informed consent is one of several lawful bases to process personal data.[10] In addition, the GDPR includes rules on giving privacy information to consumers in Articles 12 to 14, which contain lengthy lists of mandated disclosures about data processing.[11] However, both in consumer law and data privacy law, the information paradigm has attracted fierce criticism.[12] A growing body of behavioral research has questioned the effectiveness of mandated disclosures as a regulatory tool. The aim of this Essay is not to review once more why most consumers neither read nor understand verbose and complex privacy notices or the lengthy disclosures mandated under consumer protection law. Many articles[13] and books[14] have done this already. Some of them have even called for abandoning "disclosurism" generally, claiming that mandated disclosures as a regulatory instrument do not work and cannot be fixed.[15]

This Essay takes a more optimistic view and argues that, in the near future, many of the weaknesses of the current approach to disclosure could be cured with the help of data science and algorithm-based regulation. In this vein, Professors Ariel Porat and Lior

---

9 Regulation 2016/679 of the European Parliament and of 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 (General Data Protection Regulation), 2016 OJ L119 1 (May 4, 2016).

10 Regulation 2016/679, 2016 OJ L119 at 36.

11 Regulation 2016/679, 2016 OJ L119 at 39–40, 41–42. Notice and consent is also an important element of the international framework for transborder data flows. Thus, the Safe Harbor agreement concluded in 2000 between the European Union and the United States and the EU-US Privacy Shield, its 2016 successor, specifically include "notice" and "choice" as two essential principles. See *EU-U.S. Privacy Shield Framework Principles* (US Department of Commerce, 2016), archived at http://perma.cc/QT7M-GVXV.

12 See, for example, Ben-Shahar and Schneider, 159 U Pa L Rev at 651 (cited in note 3).

13 See, for example, Samuel Issacharoff, Martin Engel, and Johanna Stark, *Buttons, Boxes, Ticks, and Trust: On the Narrow Limits of Consumer Choice*, in Klaus Mathis, ed, 2 *European Perspectives on Behavioural Law and Economics, Economic Analysis of Law in European Legal Scholarship* 107, 118–21 (Springer 2015); Anne-Lise Sibony, *Can EU Consumer Law Benefit from Behavioural Insights? An Analysis of the Unfair Practices Directive*, 6 Eur Rev Private L 901, 902–03 (2014); Annette Nordhausen Scholes, *Behavioural Economics and the Autonomous Consumer*, 14 Camb Yearbook Eur Legal Stud 297, 306–18 (2012); *Disclosure, Agents, and Consumer Protection*, 167 J Institutional & Theoretical Econ 56, 61–64 (2011). See also generally Eva Maria Tscherner, *Can Behavioral Research Advance Mandatory Law, Information Duties, Standard Terms and Withdrawal Rights?*, 1 Austrian L J 144 (2014); Hans-W. Micklitz, Lucia A. Reisch, and Kornelia Hagen, *An Introduction to the Special Issue on "Behavioural Economics, Consumer Policy, and Consumer Law"*, 34 J Consumer Pol 271 (2011).

14 See, in particular, Ben-Shahar and Schneider, *More than You Wanted to Know* at 33–55 (cited in note 1).

15 See id at 183.

Strahilevitz have argued in their seminal article that personalization could be used to design disclosures tailored to specific individuals in order to increase the relevance of the information and to reduce the risk of information overload.[16] Indeed, as information technology evolves and the cost of data collection, storage, and processing declines, the analysis of large volumes of unstructured data (big data)[17] could play a transformative role for disclosure as a regulatory tool. With the help of big data, it could be possible to provide consumers with information that is tailored to their situations, personalities, demographic characteristics, and cognitive capabilities. The provision of such behaviorally informed (personalized) information instead of standardized (impersonal) information could increase the relevance of a disclosure for the individual recipient of the information.

Starting from this premise, this Essay explores how such personalized disclosures could be operationalized and implemented in the fields of consumer and data privacy law. This Essay proceeds as follows: Part I lays the groundwork by introducing the concept of personalized disclosures and briefly outlining its theoretical foundations. Part II provides some illustrations of how personalization, based on various metrics, could be implemented to tailor disclosures in consumer law. Part III illustrates how personalization could work in data privacy law. Part IV deals with a number of practical issues of regulatory design for personalized law. In particular, it makes the point that personalized disclosures should be conceived of as a learning system based on feedback mechanisms in order to continuously improve the relevance

---

[16] See generally Ariel Porat and Lior Jacob Strahilevitz, *Personalizing Default Rules and Disclosure with Big Data*, 112 Mich L Rev 1417 (2014). There is an emerging debate about personalization in various areas of the law. See generally, for example, Omri Ben-Shahar and Ariel Porat, *Personalizing Negligence Law*, 91 NYU L Rev 627 (2016). See also, for example, Cass Sunstein, *Choosing Not to Choose: Understanding the Value of Choice* 157–73 (Oxford 2015); Christoph Busch, *The Future of Pre-contractual Information Duties* at 221 (cited in note 2); Anthony J. Casey and Anthony Niblett, *The Death of Rules and Standards*, 92 Ind L J 1401 (2017); Philipp Hacker, *Personalizing EU Private Law: From Disclosures to Nudges and Mandates*, 25 Eur Rev Private L 651 (2017). See also Geneviève Helleringer and Anne-Lise Sibony, *European Consumer Protection through the Behavioral Lens*, 23 Colum J Eur L 607, 629–30 (2017).

[17] There is not yet a rigorous and commonly accepted definition of big data. See Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* 6 (Houghton Mifflin Harcourt 2013) ("There is no rigorous definition of big data."). For the purposes of this Essay, the term refers to new processing technologies that make it possible to manage large quantities (volume) of heterogeneous data (variety) at a high speed (velocity).

of the information provided. Lastly, it addresses ramifications of personalization for compliance monitoring and enforcement.

I. FROM IMPERSONAL TO PERSONALIZED LAW?

Legal norms usually formulate impersonal and abstract rules that are supposed to cover a large number of individual cases: To legislate means to generalize.[18] A tool for generalizing commonly used by the legislators are "typifications," which are normative models that divide the infinite variations of the social world into certain categories that create meaningful order.[19] Through the use of typifications, situations that are, on closer inspection, heterogeneous are typified as homogeneous. Thus, the disclosure rules of consumer law generally do not take into consideration the informational needs of the individual consumer. Instead, they are based on the fictional model of the average consumer, who is, in the words of the European Court of Justice, "reasonably well-informed and reasonably observant and circumspect."[20]

However, the rather crude one-size-fits-all design of disclosures based on typifications suffers from a certain degree of imprecision. The underlying typifications represent only a blurred picture of reality and ignore what Oliver Wendell Holmes called the "personal equation."[21] In mathematical terms, typifications offer only an approximate value. The use of such legal approximations leads to regulatory errors and inequities caused by the over- and underinclusiveness of the normative models. From an economic perspective, one could argue that typifications are mainly used as means for reducing complexity costs.[22] Developing a complex system of rules, exceptions, and counterexceptions is difficult not only for the legislator. Standardized rules are also easier for targets of those rules (for example, businesses and consumers) to communicate, to understand, and to comply with ex ante. Finally, less complex rules are easier for courts to administer ex post.

---

18 Paul Kirchhof, *Allgemeiner Gleichheitssatz*, in Josef Isensee and Paul Kirchhof, eds, 8 *Handbuch des Staatsrechts der Bundesrepublik Deutschland* 697, 773 (Heidelberg 3d ed 2010). See also Hans Kelsen, *Allgemeine Staatslehre* 231–32 (Springer 1925).

19 See Michael D. Barber, *Social Typifications and the Elusive Other: The Place of Sociology of Knowledge in Alfred Schutz's Phenomenology* 36–37 (Bucknell 1988) (describing the use of typifications in sociology).

20 *Gut Springenheide and Tusky v Oberkreisdirektor Steinfurt*, Case C-210/96, 1998 ECR I-04657, ¶ 31.

21 Oliver Wendell Holmes Jr, *The Common Law* 108 (Macmillan 1881).

22 See Louis Kaplow, *A Model of the Optimal Complexity of Legal Rules*, 11 J L Econ & Org 150, 150–52 (1995).

From this point of view, complexity costs related to the design of legal norms are directly linked to the limited capacity of human information processing. Thus, one could argue that the optimal complexity of legal rules—and the granularity of the entire legal system—is limited by the bounded capacity of human information processing. From this perspective, one could also argue that the widespread use of typifications is essentially the answer to an information problem—a concession to the imperfections of a legal system administered by humans. In the near future, however, big data, superhuman information processing capabilities, and artificial intelligence could redefine the optimal complexity of legal rules and refine their content to a hitherto unachievable level of granularity.[23] In such a scenario, granularized or personalized legal rules could take into account actor heterogeneity to a degree impersonal laws are unable to do. As a result, regulatory errors stemming from over- and underinclusive norms based on coarse-grained typifications can be reduced.

Against this background, standardized disclosures, as prescribed by current consumer and data privacy law, are a product of the predigital and industrial mass society. Disclosures standardized in shape and content seem like a distant echo of Henry Ford's dictum that any customer can have a car painted any color that he wants "as long as it's black."[24] This approach does not fit in the digital economy. Indeed, in the field of manufacturing, there has already been a profound transformation since the 1990s toward mass customization, allowing consumers to customize their products with a range of components and colors. Currently, information technology and increased precision in customer data are driving the next wave of mass customization, making it even easier to build unique products and services for individual customers.[25]

II. CONSUMER LAW

The idea of mass customization could easily be implemented in the field of consumer law. The replacement of standardized information with personalized disclosures could reduce the amount of information to be provided and, at the same time, increase the

---

[23] See generally Casey and Niblett, 92 Ind L J 1401 (cited in note 15).

[24] B. Joseph Pine II, *Mass Customization: The New Frontier in Business Competition* 7 (Harvard Business 1993).

[25] See, for example, Russell Walker, *From Big Data to Big Profits: Success with Data and Analytics* 91–92 (Oxford 2015).

relevance of a disclosure for the individual recipient of the information. The following examples may illustrate how data on consumers' purchasing habits and other patterns of past behavior can be used for reducing both the quantity problem of information overload and the quality problem of information mismatch, which are associated with the one-size-fits-all approach to disclosure.

A. Product Information

Article 6(1)(s) of the EU Consumer Rights Directive requires an online seller to inform the consumer before the conclusion of a contract about "any relevant interoperability of digital content with hardware and software that the trader is aware of or can reasonably be expected to have been aware of."[26] According to the European Commission's Guidance Document for the implementation and application of the EU Consumer Rights Directive, such information should include details "about the necessary operating system and additional software, including the version number, and hardware, such as processor speed and graphics card features."[27] Under the current model of standardized disclosure, traders usually provide the information in a rather technical and impersonal manner (for example, "This software requires Mac OS X version 10.5.x or later."). For less tech-savvy users who do not know which operating system they are using, this information will not be very useful. If, however, the device used by the consumer for accessing the online shop is identified by the shop's software, the information could be provided in a more personalized way (for example, "This product is compatible with the computer that you are currently using."). Additional information about the interoperability with other systems that might be relevant only for certain consumers could be relocated to a second layer of disclosure that is displayed only upon request (for example, "For more information on interoperability, click here.").

Personalization could also be used to make certain information items more or less salient based on the consumer's past behavior.[28]

---

[26] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on Consumer Rights (EU Consumer Rights Directive), 2011 OJ L304 64, 76 (Oct 25 2011).

[27] *DG Justice Guidance Document concerning Directive 2011/83/EU* *68 (European Commission Directorate-General for Justice and Consumers, June 13, 2014), archived at http://perma.cc/9KH9-ML4A.

[28] See, for example, Hacker, 25 Eur Rev Private L at 669 (cited in note 15) (suggesting that, if the purchase history of a consumer shows that she tends to miss deadlines for withdrawal rights and often sends goods back after the deadline has passed, personalized

If, for example, a credit card company offers one of its customers travel insurance, the company is obliged under Article 3(1)(2)(a) of the EU Directive on Distance Marketing of Consumer Financial Services to provide "a description of the main characteristics of the financial service."[29] Under a personalized disclosure model, the company could be obliged to take into account the available data on the consumer's credit card usage for tailoring the information about the insurance. If, for example, the credit card usage data shows that the client regularly travels to Iraq or Libya, the information about an exclusion of these countries from the insurance coverage should be made in a prominent way.

Similarly, data about a consumer's purchasing history could be used for personalized health warnings. A famous and often cited example that illustrates this use case is the retailer Target, which used data mining to identify pregnant women among its customers.[30] Target's data miners observed that pregnant women were likely to buy certain nutritional supplements in their first trimester, unscented lotion in their second trimester, and hand sanitizer close to their due dates.[31] Knowing that the birth of a child is a watershed moment in the customer relationship, when shopping behaviors are open to change and new brand loyalties are likely to emerge, Target used the information to send personalized advertising and coupons to the pregnant women.[32] From a regulatory perspective, one could consider whether a retailer who has obtained such insights through data analytics should be obliged to use this information to provide consumers with targeted health warnings.[33] For example, a customer with a high "pregnancy prediction score" could be confronted with a specific warning message if she buys alcoholic beverages or raw cheese in an online shop.

Maybe the last example seems a little bit creepy and overly paternalistic. This could indeed be the case. Let me be clear: I am not saying that the law *should* require online retailers to identify

---

law could require the seller to highlight withdrawal deadlines when this client orders goods online).

[29] Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the Distance Marketing of Consumer Financial Services, 2004 OJ L271 16, 19 (Sept 23, 2002).

[30] See Charles Duhigg, *How Companies Learn Your Secrets* (NY Times Magazine, Feb 16, 2012), archived at http://perma.cc/8VGY-D93F.

[31] See id.

[32] See id.

[33] See Busch, *The Future of Pre-contractual Information Duties* at 234 (cited in note 2).

pregnant customers and confront them with unwanted warnings. What I am saying is that the law *could* do this on the basis of data analytics. This is a regulatory option that was not available a few years ago. Therefore, it has to be decided in which cases it is appropriate to use the new type of data-driven disclosure mandates and where to draw a line. This is of course a policy question that may be subject to conflicting points of view.

B. Financial Health Warnings

While the above examples involve only information about observable consumer preferences (for example, the interoperability of software and the suitability of insurance) or physical characteristics (for example, pregnancy), personalization could go much further based on personality characteristics. In this vein, Professors Porat and Strahilevitz have suggested personalizing default rules and disclosures according to personality types, drawing on the "Big Five" model.[34] Under this model, which is the dominant paradigm among psychologists who study personality traits, individuals can be categorized on the basis of five essential personality characteristics (extraversion, agreeableness, conscientiousness, neuroticism or emotional stability, and openness to experience).[35] The following example illustrates how personality characteristics could be used to identify particularly vulnerable consumers who might need special financial health warnings.

In 2016, the German legislature passed a new regulation that compels banks to offer special advice to financially vulnerable consumers who continuously and significantly use the overdraft facility of their bank accounts.[36] The underlying idea is that overdraft credit is easily available and can be used without further action but, at the same time, is comparatively expensive. Consumers who use their overdraft on a regular basis, whether for convenience or out of ignorance of alternatives, pay a high price. The new advice duty is aimed at protecting vulnerable consumers from being financially overburdened as a result of improper use of overdrafts. Thus, under the new § 504(1) of the German Civil

---

[34] Porat and Strahilevitz, 112 Mich L Rev at 1434–40 (cited in note 15).

[35] Robert R. McCrae and Oliver P. John, *An Introduction to the Five-Factor Model and Its Applications*, 60 J Rsrch Personality 175, 175 (1992); Samuel D. Gosling, Peter J. Rentfrow, and William B. Swann Jr, *A Very Brief Measure of the Big-Five Personality Domains*, 37 J Rsrch Personality 504, 510 (2003).

[36] See Ulrich Krüger, *Neue Beratungspflichten bei Verbraucherdarlehen—ein Paradigmenwechsel*, 16 Zeitschrift für Bank- und Kapitalmarktrecht 397, 398–99 (2016).

Code[37] (BGB), banks have to offer financial advice to consumers who are using more than 75 percent of the agreed overdraft amount for at least six months. For customers who accept the offer, the bank has to advise them about less expensive credit options as alternatives to the overdraft, about the possible consequences of further using the overdraft, and about counseling facilities for consumers who are experiencing financial difficulties.[38] Section 504(1) of the German Civil Code can be conceptualized as a crude example of a personalized financial health warning. Instead of prescribing a general warning regarding overdraft facilities, the regulation focuses on a customer segment that is identified as particularly vulnerable based on the data available to the bank. In this regulatory model, a continuous and significant use of overdraft is considered a signal of financial vulnerability.

However, based on psychological research, the concept of a "vulnerable consumer" that is used as a trigger for the advisory duty could be refined by taking into account particular vulnerabilities resulting from specific personality traits. Empirical research shows that people living on a low income tend to spend a higher percentage of it on products or services perceived to have a high status.[39] One reason for this seems to be the desire to compensate for perceived self-deficits ("compensatory consumption").[40] Such behavior can be one reason for continuing financial hardship.[41] Interestingly, recent research suggests that the preference for "status spending" is linked to certain personality traits.[42] Extraverted people with low income spend more on status

---

37 Buirgerliches Gesetzbuch § 504(1).

38 See Frank Drost and Elizabeth Atzler, *Banks under Pressure for Overdraft Rates* (Handelsblatt Global, July 20, 2015), archived at http://perma.cc/LNL5-DHQH:

> At the behest of the [German] federal government, banks are supposed to advise customers who have overdrawn their account by half their average incoming payments for three months, or who have used 75 percent of their credit allowance for six months or more. Banks must offer heavily indebted customers alternatives to an overdraft.

39 See generally Laurie Simon Bagwell and B. Douglas Bernheim, *Veblen Effects in a Theory of Conspicuous Consumption*, 86 Am Econ Rev 349 (1996). See also generally, Thorstein Veblen, *The Theory of the Leisure Class* (Macmillan 1899).

40 Derek D. Rucker and Adam D. Galinsky, *Compensatory Consumption*, in Russell W. Belk and Ayalla A. Ruvio, ed, *The Routledge Companion to Identity and Consumption*, 207 (Routledge 2013) (defining compensatory consumption as "the desire for, acquisition, or use of products to respond to a psychological need or deficit").

41 See Omer Moav and Zvika Neeman, *Saving Rates and Poverty: The Role of Conspicuous Consumption and Human Capital*, 122 Econ J 933, 938–40 (2012).

42 Blaine Landis and Joe J. Gladstone, *Personality, Income, and Compensatory Consumption: Low-Income Extraverts Spend More on Status*, 28 Psychological Sci 1518, 1518–19 (2017).

than their introverted peers. The interaction between income and extraversion remains a significant predictor of status spending when controlled for a range of demographic, financial, and other personality variables.[43] In other words, extraverted people seem to be more likely to engage in behavior that bears the danger of perpetuating their financial hardship.

Based on these findings, one could use different triggers for financial advisory duties depending on the personality of the customer. For example, for extraverted customers with low incomes, the threshold for the advisory duty to apply could be lower than for introverted customers (for example, 60 percent instead of 75 percent or three months instead of six months). The data required for identifying the personality traits could be harvested from the bank account or from other sources easily accessible to the bank (for example, Facebook or Instagram). It goes without saying that such a regulatory approach raises complicated issues of data privacy. Part IV.B deals with these issues.

III. DATA PRIVACY LAW

A. Personalized Privacy Notices

The information paradigm is not only a cornerstone of consumer law but also a central pillar of data privacy law. However, as in consumer law, these disclosures fail on several accounts. Empirical evidence suggests that, despite detailed privacy notices, many users do not know to what extent personal information is gathered and processed by companies. Often, the mere existence of a privacy notice is interpreted as a cue signaling a high level of privacy protection, regardless of its content.[44] One could argue that it is rational to refrain from reading privacy policies if the costs of reading exceed the expected benefits of ignorance (rational ignorance).[45] However, empirical research suggests

---

See also *Poor Extroverts Spend Proportionately More on Buying Status: Personality, Poverty, and Purchases* (The Economist, Aug 26, 2017), archived at http://perma.cc/T5HE-YGD6.

43 See Landis and Gladstone, 28 Psychological Sci at 1519 (cited in note 36).

44 See Joseph Turow, et al, *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: J L & Pol Info Socy 723, 731–32 (2007). See also Florencia Marotta-Wurgler, *Self-Regulation and Competition in Privacy Policies*, 45 J Legal Stud S13, S17–20 (2016) (describing users interpreting the existence of a privacy seal as a guarantee of confidential communication).

45 See Ben-Shahar and Schneider, 159 U Pa L Rev at 709–11 (cited in note 3); Tess Wilkinson-Ryan, *A Psychological Account of Consent to Fine Print*, 99 Iowa L Rev 1745, 1753 (2014); Yoan Hermstrüwer, *Contracting around Privacy: The (Behavioral) Law and*

that users' efficacy in privacy management is hampered by their bounded rationality[46] and limited motivation to control privacy.[47]

In light of these findings, several proposals have been made for making privacy disclosures more useful. The evident solution is to simplify the disclosures by shortening the privacy notices, making them more user-friendly, or improving the formatting.[48] However, empirical studies show that simplified disclosures (for example, "privacy nutrition labels") or warning labels have little effect on consumers' comprehension of privacy disclosure, willingness to disclose information, or expectations about their privacy rights.[49]

If simplification does not make privacy notices more useful, personalization might be an alternative. Personalizing disclosures about data sharing not only reduces the quantity of information but also could help bring to the fore those aspects that are particularly relevant for the individual user. Moreover, current privacy notices—whether long or short—do not take into account the heterogeneity of privacy preferences. Empirical research indicates that privacy preferences are diverse and differ across individuals. A recent study of privacy management strategies among Facebook users shows that users vary substantially in how

Economics of Consent and Big Data, 8 J Intell Prop, Info Tech & Electronic Commerce L 9, 18 (2017).

46 See, for example, Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 Sci 509, 512–13 (2015); Alessandro Acquisti, Curtis R. Taylor, and Liad Wagman, *The Economics of Privacy*, 52 J Econ Lit 442, 476–78 (2016).

47 Ralph Gross and Alessandro Acquisti, *Information Revelation and Privacy in Online Social Networks*, in David Matheson, *Contours of Privacy* 206–11 (Cambridge 2009); Ramón Compañó and Wainer Lusoli, *The Policy Maker's Anguish: Regulating Personal Data Behavior between Paradoxes and Dilemmas*, in Tyler Moore, David J. Pym, and Christos Ionnidis, ed, *Economics of Information Security and Privacy* 169, 175 (Springer 2010).

48 For example, a condensed information format ("one-pager") has recently been proposed by the German Federal Ministry of Justice and Consumer Protection. *Privacy at a Glance: "One-Pager" Presented as a Template for Transparent Privacy Notices* (German Federal Ministry of Justice and Consumer Protection, Nov 19, 2015), archived at http://perma.cc/CQB6-DDZX.

49 See, for example, Omri Ben-Shahar and Adam Chilton, *Simplification of Privacy Disclosures: An Experimental Test*, 45 J Legal Stud S41, S65–66 (2016); Sara Elisa Kettner, Christian Thorun, and Max Vetter, *Wege zur Besseren Informiertheit: Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und Weiterer Lösungsansätze im Datenschutz* *89–97 (ConPolicy, Feb 28, 2018), archived at http://perma.cc/VDF9-L3JE (suggesting that a "one-pager" with simplified information about data use does not significantly improve comprehension).

they use privacy mechanisms.[50] Preferences regarding privacy may vary among different users, both with regard to different types of personal data (for example, location or browsing history) and different usage purposes (for example, personalizing a service, targeted marketing, or research). Moreover, empirical research suggests that privacy risk is perceived differently by people with different demographic characteristics.[51] As a result, different segments of the population may show different degrees of vulnerability to privacy harms.

Currently, regulation on privacy disclosures does not take into account different privacy preferences or vulnerabilities. However, the recently published Guidelines[52] of the Article 29 Data Protection Working Party[53] (WP 29) on transparency under the GDPR contain some starting points for tailoring privacy notices. Thus, for privacy disclosures in a digital context, WP 29 recommends the use of layered privacy notices rather than displaying all information in a single notice.[54] Another way of reducing the complexity of privacy notices suggested by WP 29 is the use of "push" and "pull" notices.[55] Push notices refer to the provision of "just-in-time" disclosures that are displayed at the very moment the user makes a decision about sharing her data, while pull notices contain additional information that are displayed only upon request. WP 29 even suggests that "data controllers may also choose to use additional transparency tools . . . which provide tailored information to the individual data subject which is specific to the position of the individual data subject concerned and the goods/services which that data subject is availing of."[56] This seems to point toward personalized disclosures about data usage.

---

50 Pamela J. Wisniewski, Bart P. Knijnenburg, and Heather Richter Lipford, *Making Privacy Personal: Profiling Social Network Users to Inform Privacy Education and Nudging*, 98 Intl J Human-Computer Stud 95, 103–06 (2017).

51 See, for example, Jaspreet Bhatia and Travis D. Breaux, *Empirical Measurement of Perceived Privacy Risk ACM Transactions on Human-Computer Interaction* *30 (forthcoming 2019), archived at http://perma.cc/76DF-EG42 (suggesting differences based on age and ethnicity).

52 *Guidelines on Transparency under Regulation 2016/679* (Article 29 Data Protection Working Party, Apr 11, 2018), archived at http://perma.cc/Z46P-XJPM.

53 The Article 29 Working Party is an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor, and the European Commission. Under the GDPR, the European Data Protection Board (EDPB) will replace the Article 29 Working Party.

54 *Guidelines on Transparency under Regulation 2016/679* at ¶ 30 (cited in note 52).

55 Id at ¶ 32.

56 Id at ¶ 31.

Tailoring privacy disclosures to the needs of individual targets requires that the information provider identifies its audience and their informational needs and preferences. Information about privacy preferences could be based on past behavior. According to a recent study, it might be possible to predict privacy preferences with rather high accuracy by asking users a small number of questions about data collection.[57] Based on their past privacy behavior, users could be grouped into clusters in order to provide user-tailored privacy notices. One could even consider more advanced techniques to predict the privacy preferences of users based on profiles of users with similar characteristics.[58]

B. Personalized Privacy Assistants

While personalized privacy notices could be a first step toward making disclosures about data sharing more meaningful, it is doubtful whether this approach will be sufficient to achieve a personalized privacy environment that is based on user preferences. The "notice and consent" model not only risks information overload but also requires users to make many active choices about their privacy. The cumulative cognitive demand of these decisions may erode users' ability to make wise choices about data sharing. Psychologists refer to this erosion of self-control after making repeated decisions as "decision fatigue."[59] This problem may even get worse with the advent of the Internet of Things (IoT). In the near future, smart buildings, connected cars, and entire smart cities will collect information about individuals. Under such a scenario, the regulatory model of active choice based on privacy notices—whether long or short, standardized or personalized—reaches its limits.

---

[57] Pardis Emami-Naeini, et al, *Privacy Expectations and Preferences in an IoT World*, Proceedings of the Thirteenth Symposium on Usable Privacy and Security 399, 410 (2017) (showing that, by asking users to rate from strongly agree to strongly disagree how they feel about certain data-collection scenarios, one can predict with 88 percent accuracy how users will answer for other scenarios after only three data points per individual).

[58] Consider Norman Sadeh, et al, *Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application*, 13 Personal & Ubiquitous Computing 401, 404–08 (2009) (suggesting the use of a k-nearest neighbor approach, in which new situations are compared with the user's previous behaviors, to predict location-sharing preferences).

[59] See Kathleen D. Vohs, et al, *Making Choices Impairs Subsequent Self-Control: A Limited-Resource Account of Decision Making, Self-Regulation, and Active Initiative*, 94 J Personality & Soc Psychology 883, 895–96 (2008). See also Jonathan Levav, et al, *Order in Product Customization Decisions: Evidence from Field Experiments*, 118 J Pol Econ 274, 296 (2010).

A possible solution could be to automate consent based on personalized privacy preferences. The idea of consent assistants that implement an automated matching of user preferences with requests for personal data is not entirely new. An early example was the Platform for Privacy Preferences (P3P), a web standard developed in 2002 by the World Wide Web Consortium (W3C).[60] The P3P tool enables web browsers to read website privacy policies and compare them with user-specific privacy preferences and allows users to avoid websites that do not meet their privacy preferences. The P3P tool probably came too early and largely failed due to lack of industry participation. However, with the merger of online and offline worlds into a new hyperconnected environment that Professor Luciano Floridi refers to as "onlife,"[61] it may now be necessary to implement an automated matching of user preferences with requests for personal data. Under such a scenario, personalized privacy ecosystems could consist of two components:[62] (1) *privacy-aware smart objects* (for example, smart buildings or other IoT devices) that communicate machine-readable privacy policies to users in their vicinity and (2) *personalized privacy assistants* (for example, smartphone apps or wearable devices) that capture the privacy preferences of their users and communicate these to the IoT devices. Through the interaction of the two components, an automated matching of user preferences with requests for personal data could be implemented. In particular, a personalized privacy assistant would automatically communicate opt-out decisions based on a user's privacy preferences without the need for an explicit consent in each and every scenario. However, in order to ensure that the automated settings are still in conformity with the privacy preferences of the user, the system could occasionally require an explicit consent.

The above scenario shows two things: First, technological progress makes it possible to manage the increasing complexity of smart ecosystems and tailor disclosures to the informational needs and preferences of individual users. Second, even if the complexity of information is reduced through personalization, a

---

60 See Reidenberg, et al, 30 Berkeley Tech L J at 49–50 (cited in note 7).

61 Luciano Floridi, *The Onlife Manifesto: Being Human in a Hyperconnected Era* 1 (Springer 2015).

62 See Primal Pappachan, et al, *Towards Privacy-Aware Smart Buildings: Capturing, Communicating, and Enforcing Privacy Policies and Preferences* 195–96 (Institute of Electrical and Electronics Engineers Workshop Paper, 2017), archived at http://perma.cc/HMX8-BX4N. See also Hermstrüwer, 8 J Intell Prop, Info Tech & Electronic Commerce L at 21 (cited in note 39).

regulatory approach that is based on explicit consent is limited by the cognitive capacity of the human decisionmaker. A system that relies entirely on active choice is probably not workable in an IoT scenario. Therefore, the wave of the future might be a mix between personalized privacy defaults implemented through privacy assistants and only occasional active choices about data sharing.

IV. IMPLEMENTING PERSONALIZED DISCLOSURES: ELEMENTS OF A REGULATORY DESIGN

A. Personalized Law as a Learning System

Whether personalized information is really more useful than standardized disclosures very much depends on the quality of the data that is used for profiling and the algorithm used for generating personalized disclosures. This problem is well-known from recommender systems used by online shopping websites. Although Amazon, for example, uses an advanced collaborative filtering algorithm for product recommendations,[63] the suggestions made by Amazon on the basis of past choices do not always meet their customers' true preferences. The lack of sophistication of Amazon's recommender system becomes obvious if, for example, a reader with a keen interest in sociology and cultural history purchases the book *Love as Passion: The Codification of Intimacy*[64] by social theorist Niklas Luhmann and then keeps receiving recommendations for rather explicit erotic literature.

In order to avoid such errors, personalized disclosures should be conceived as a dynamic and "learning" system in the sense that the content of the information can change over time. In such a dynamic system, the relevance of the information can continuously be improved. Therefore, personalized disclosures should be combined with a monitoring system that provides feedback on actual consumer comprehension and consumer decision, which can be used to improve the regulatory design.[65] In this vein, several learning mechanisms could be envisaged. A simple approach

---

[63] See generally Brent Smith and Greg Linden, *Two Decades of Recommender Systems at Amazon.com*, 21 IEEE Internet Computing 12 (2017).

[64] Niklas Luhmann, *Love as Passion: The Codification of Intimacy* (Harvard 1987).

[65] See generally Lauren E. Willis, *Performance-Based Consumer Law*, 82 U Chi L Rev 1309, 1345–72 (2015) (describing a regulatory instrument that provides feedback on actual consumer comprehension and product choices while meeting performance standards for consumer comprehension).

would be to include in the system a routine asking some users for feedback on the helpfulness of the information provided. Similar techniques are already used by online retailers for information that is provided voluntarily.[66] For example, some online retailers improve the usefulness of customer reviews displayed next to a product by asking, "Was this review helpful to you?" Even if only a small percentage of consumers actually give an answer to the question, this may help further improve the targeting of disclosure.[67] This approach could be combined with randomized trials. Indeed, many online companies, such as Google and Facebook, already run a large number of randomized studies (A/B testing) on a daily basis in order to improve their products. The same approach could be used to improve personalized disclosures.[68] On an individual level, the information provided should be adapted to changing circumstances in the life of the consumer and intrapersonal changes in consumer preferences. If, for example, the consumption pattern indicates that the consumer is pregnant or has developed an intolerance to gluten, personalized health warnings could be displayed more visibly than before.

The critics of mandated disclosure have argued that "[d]isclosurites believe they know better than the people intended to receive disclosures how they should make decisions and what they need to make them well."[69] This criticism echoes Professor Friedrich August von Hayek, who warned social scientists that "[t]o act on the belief that we possess the knowledge and the power which enable us to shape the processes of society entirely to our liking, knowledge that in fact we do *not* possess, is likely to make us do much harm."[70] This criticism could also be raised against bespoke

---

66 See Erin Geiger Smith, *How Online Retailers Predict Your Perfect Outfit* (Wall St J, Aug 5, 2015), archived at http://perma.cc/U99P-BHYT.

67 See Porat and Strahilevitz, 112 Mich L Rev at 1450–52 (cited in note 15). Professors Porat and Strahilevitz suggest a regime of default rules under which

> a subset of the population ("guinea pigs") is given a lot of information about various contractual terms and plenty of time to evaluate their desirability, with the choices of particular guinea pigs becoming the default choices for those members of the general public who have similar personalities, demographic characteristics, and patterns of observed behavior.

Id.

68 See Willis, 82 U Chi L Rev at 1336–37 (cited in note 60). See also Michael Abramowicz, Ian Ayres, and Yair Listokin, *Randomizing Law*, 159 U Pa L Rev 929, 933–38 (2011).

69 Omri Ben-Shahar and Carl E. Schneider, *Coping with the Failure of Mandated Disclosure*, 11 Jerusalem Rev Legal Stud 83, 91 (2015).

70 Friedrich August von Hayek, *The Pretence of Knowledge*, 79 Am Econ Rev 3, 7 (1989) (reprinting Hayek's Nobel Memorial Lecture from Dec 11, 1974). See also John Stuart

disclosures because designing the algorithm for personalizing information requires certain assumptions about which information is relevant to a specific individual. Therefore, in order to avoid what Hayek called the "pretence of knowledge," it is essential to include into the regulatory design the feedback mechanism described above, which ensures that the information provided is really helpful for the individual consumer.

B. Personalized Disclosures and Privacy

Personalized disclosures are built on user profiling. Therefore, it is obvious that this regulatory model raises privacy concerns. In particular, one may wonder whether the use of personalized law in the field of data privacy, as described above, amounts to fighting fire with fire. In other words, one could ask whether the classic conflict between legal certainty and individual fairness, which personalized law purportedly is meant to solve, is just replaced by a new conflict between individual fairness and *privacy*.

Within the European Union, a system of personalized law would have to comply with Article 8(1) of the Charter of Fundamental Rights of the European Union[71] and Article 16(1) of the Treaty on the Functioning of the European Union[72] (TFEU), which both guarantee the protection of personal data privacy. At the level of secondary legislation, these fundamental principles are mainly implemented by the GDPR. Therefore, a system of personalized law introduced in the European Union would have to be in line with the requirements laid down by the GDPR. First, the GDPR would require the enactment of a (national or European) legal basis for collecting data for the purpose of personalizing disclosures.[73] Second, it is important to note that, under the GDPR, customer

---

Mill, *On Liberty*, in Dale E. Miller, ed, *The Basic Writings of John Stuart Mill: On Liberty, The Subjection of Women, and Utilitarianism* 3, 79 (Modern Library 2002) (underlining that the individual "is the person most interested in his own well-being" and that "the most ordinary man or woman has means of knowledge immeasurably surpassing those that can be possessed by any one else").

71 Charter of Fundamental Rights of the European Union Art 8(1), 55 OJ C326 391, 397 (2012) ("Everyone has the right to the protection of personal data concerning him or her.").

72 Consolidated Version of the Treaty on the Functioning of the European Union Art 16(1), 55 OJ C326 455, 463 (2012) (mirroring the language in the EU Charter of Fundamental Rights).

73 See Regulation 2016/279, 2016 OJ L119 at 36 (requiring a legal basis for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller).

profiling, which would be the basis for personalized disclosures, is not prohibited as such. However, Article 22(1) of the GDPR gives every natural person the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects concerning him or her or similarly significantly affects him or her.[74] This provision is subject to several exceptions spelled out in Article 22(2) of the GDPR. In particular, Article 22(2)(b) allows measures based on profiling if they are authorized by EU law or the national law of an EU member state.[75] This is essentially an opening clause which allows member states to authorize automated decisions (including profiling) by law, provided that the law "also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests."[76]

For additional complication, Article 22(4) of the GDPR lays down a basic rule that profiling "shall not be based" on special categories of data referred to in Article 9(1) of the GDPR, unless there is explicit consent.[77] These "special categories" of personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data used for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.[78] Considering the broad wording of Article 22(4) of the GDPR ("shall not be based"), the provision could apply to a scenario in which the inputs used by a personalization algorithm are nonsensitive, but the output inferences may be, as was the case in the abovementioned example of the "pregnancy prediction score."[79] As a consequence, the implementation of personalized disclosures would in many cases require an explicit consent from the consumer.

Regardless of the question whether such explicit consent is necessary under Article 22(4) of the GDPR, it seems preferable to

---

74 On the scope of Article 22 of the GDPR, see Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 Intl Data Private L 76, 79–83 (2017).

75 Regulation 2016/279, 2016 OJ L119 at 46.

76 Regulation 2016/279, 2016 OJ L119 at 46.

77 Regulation 2016/279, 2016 OJ L119 at 46.

78 Regulation 2016/279, 2016 OJ L119 at 38.

79 See text accompanying notes 29–30. See also Lilian Edwards and Michael Veale, *Slave to the Algorithm? Why a "Right to Explanation" Is Probably Not the Remedy You Are Looking For*, 16 Duke L & Tech Rev 18, 36 (2017).

design personalized disclosures based on an *opt-in model* following the general principle *volenti non fit iniuria*.[80] Under such a regime, the consumer would have the right to choose between impersonal and personalized information. As a consequence, the degree of personalization of the information provided to the consumer would depend on the individual's preference for privacy. This approach would reflect actor heterogeneity and take into consideration that different consumers may have different attitudes toward privacy. A consumer who prefers the benefits of personalized information must accept customer profiling. A consumer, in turn, who is not willing to accept the processing of personal data for the purpose of customer profiling must pay a price for the higher level of privacy protection. The price she pays is less personalized information.

As an extension of this model, one could consider whether a right to choose between personalized and impersonal disclosures should also be granted to businesses that are obliged to provide information. Under this approach, a business would be obliged to personalize disclosures only if it already collects the relevant data for other purposes (for example, personalized advertising). If, however, a business opts for a privacy-friendly business model and abstains from customer profiling, the traditional model of impersonal disclosures would apply. As a consequence, personalized disclosures would be contingent on a *double opt-in* by both the consumer and the business. Finally, this approach could also be conceived of as a continuum of personalized information. A trader who collects data about the consumer for profiling purposes must use this knowledge to provide the consumer with information that is relevant to her. More knowledge about the consumer therefore means more responsibility for providing her with relevant information. Or in more technical terms, a more granular consumer profile means more granular disclosure.

C. Compliance Monitoring and Algorithm Auditing

Changing the traditional model of mandatory disclosure of standard information into a system of personalized disclosure also has consequences for the level of compliance and enforcement. Monitoring compliance with standardized information duties is rather simple. Enforcement authorities, such as the Federal

---

[80] This translates to: "To a willing person, injury is not done." See also Busch, *The Future of Pre-contractual Information Duties* at 237–38 (cited in note 2).

Trade Commission in the United States or the Competition and Market Authority in the United Kingdom, have to verify only whether the information provided by a trader complies with the list of disclosure items defined by the law. The same applies to competitors and consumer associations in countries with systems of decentralized and private enforcement of consumer law, such as Germany.[81] Compliance is even simpler if the law requires the use of certain standard forms for informing consumers, such as the Standard European Consumer Credit Information[82] or the European Standard Information Sheet for Mortgage Credit.[83]

In contrast, monitoring compliance with personalized information duties is more complex. In the above-mentioned example[84] of a credit card company that offers travel insurance to one of its customers, the content of the personalized disclosure depends on the data available to the company about the customer's traveling habits. Similarly, in the case[85] of financial health warnings based on consumer personality traits, the applicability of the advisory duty depends on classifying consumers into the right customer segment. Consequently, compliance monitoring in these cases would involve testing whether the business effectively used the data that was available and has drawn the right conclusions from the data set. More generally, the information provided to an individual consumer could depend on the data available about the consumer's demographics, personality traits, purchasing habits, and other patterns of past behavior.

From a market control perspective, this increases the complexity of the "disclosure landscape" and leads to a differentiation, maybe even an "atomization," of disclosures. Therefore, it is much more difficult and maybe even impossible for private actors, such as consumer organizations, to monitor whether a business complies with the applicable disclosure regulation. Effective enforcement of personalized law probably requires some form of public

---

81 See Justin Eugene Malbon and Allen Asher, *Institutional Structures Relating to the Administration and Enforcement of Consumer Laws*, in Stephen Corones, et al, *Comparative Analysis of Overseas Consumer Policy Frameworks* 150, 151 (Australia 2016). See also generally Hans-W. Micklitz and Geneviève Saumier, eds, *Enforcement and Effectiveness of Consumer Law* (Springer 2018).

82 Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on Credit Agreements for Consumers, Annex II, 2008 OJ L133 1, 10 (Apr 23, 2008).

83 Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on Credit Agreements for Consumers Relating to Residential Immovable Property, Annex II, 2014 OJ L60 34 (Feb 4, 2014).

84 See text accompanying notes 27–28.

85 See text accompanying notes 31–32.

enforcement. From a practical perspective, compliance monitoring would require that the enforcement authority perform regular algorithm audits to ensure that the personalization algorithms perform as provided by the law—that is, use the right criteria for generating personalized disclosures. Such audits would also cover the data pools used for profiling in order to assess the validity of the data and to ensure that the data is unbiased.[86]

CONCLUSION

Tailoring disclosures to the informational needs of individuals or groups of individuals increases the relevance of the information provided and reduces the risk of information overload. Personalization could possibly rejuvenate disclosures as a regulatory tool. Maybe the reports about the death of disclosures are greatly exaggerated. However, while the idea of personalized disclosures is as simple as it is appealing, its practical implementation proves to be difficult. Generating personalized disclosures on the basis of user data is a form of algorithmic regulation. Therefore, compliance monitoring and enforcement will require new regulatory approaches involving algorithm audits and data quality management in order to ensure the proper functioning of the new data-driven regulatory system.

On a more general level, the example of personalized disclosures shows how advances in information technology could increase the granularity of legal rules in other areas of the legal system. From this perspective, many impersonal and standardized rules can be seen as an answer to an information problem—a concession to the bounded capacity of human information-processing. If this is correct, artificial intelligence and superhuman information processing capabilities could redefine the optimal complexity of legal rules and refine, for example, the content of disclosures to a hitherto unachievable level of granularity.

However, while personalized disclosures may reduce the quantity of information and increase their quality, the current model of "notice and consent" that dominates consumer and privacy law still requires human decision-making, which is a limited resource. With the advent of the IoT, the "notice and consent" model could reach its limits as users will be overwhelmed by the

---

[86] See generally Brent Mittelstadt, et al, *The Ethics of Algorithms: Mapping the Debate*, 3 Big Data & Society (2016).

number of requests for decisions about data sharing and privacy. In such a scenario, personalizing disclosures in order to reduce the amount of irrelevant *information* is probably not sufficient. It may be necessary to go a further step and reduce the number of *decisions* to be taken while still preserving the autonomy of the individual. Therefore, the wave of the future, at least in data privacy law but maybe also beyond, is probably a mix of personalized defaults implemented through virtual personal assistants and only occasional active choices.