5-2020

Regulatory approaches to consumer protection in the financial sector and beyond: Toward a smart disclosure regime?

Nydia REMOLINA LEON

Aurelio GURREA-MARTINEZ

Yvonne Ai-Chi LOH

David R. HARDOON

SMU Centre for AI & Data Governance Research Paper No. 2020/05

REGULATORY APPROACHES TO CONSUMER PROTECTION IN THE FINANCIAL SECTOR AND BEYOND: TOWARD A SMART DISCLOSURE REGIME?[1]

Nydia Remolina[2], Aurelio Gurrea-Martinez[3], Yvonne Ai-Chi Loh[4] , David R. Hardoon[5]

[1] This research is supported by the National Research Foundation, Singapore under its Emerging Areas Research Projects (EARP) Funding Initiative. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore.

[2] Research Associate, Singapore Management University Centre for AI and Data Governance.
[3] Assistant Professor, Singapore Management University School of Law.
[4] Nudge Leader, Monetary Authority of Singapore.
[5] Senior Advisor for Data and AI, UnionBank of the Philippines and Visiting Faculty, Singapore Management University Sim Kee Boon Institute for Financial Economics.

Abstract

Traditionally, consumer and data protection policies evolved from issues of consent and information disclosure. The purpose of these regulatory approaches is the protection of consumers by reducing some contracting failures, such as asymmetries of information and a lower bargaining power, especially in transactions involving complex issues such as financial products and sensitive personal data. In the past, regulators have responded to privacy and consumer protection by adopting what this paper refers to as an "imperfectly informed regime", in which consumers do not receive full information about the risks associated with their decisions, even if they are still protected through a variety of *ex post* mechanisms such as the judicial system or a consumer protection authority. Recently, jurisdictions, such as the European Union, have adopted a "perfectly informed regime" for data protection based on the idea of full disclosure. While this approach has advantages, it does not effectively assure consumers understand the consequences and risks associated with their decisions. Unless the system still provides reliable mechanisms *ex post* to protect consumers, there will still be a high risk of opportunism of merchants vis-à-vis consumers. As a response to the weaknesses existing in the traditional regulatory approaches to protect consumers, behavioural economists have proposed a new system based on the idea of 'smart disclosure'. According to this system, consumers should get an understanding of their decisions by requiring counterparties to provide a clear information about the content and associated risks. Despite the popularity of this regulatory approach, this paper argues that it is not perfect either. Namely, it will be pointed out that, even though the smart disclosure system can be desirable for countries without reliable institutions to protect consumers *ex post*, the adoption of this regulatory approach faces several challenges. Therefore countries with efficient mechanisms *ex post* to protect consumers may find the traditional regulatory models more desirable. The paper concludes by arguing that despite the favour towards systems of smart disclosure or perfectly informed regimes, the most desirable one will depend on the particular features of a country.

Table of content

1. Introduction

Traditionally, the concept of consent has played an essential role in consumer and data protection. For instance, since the original Data Protection Directive in 1995, the law of the European Union, in one of the first regulatory initiatives in this regard, emphasizes the importance of user consent.[6] By requiring customers' consent, regulators aim to protect consumers from making bad decisions, sometimes due to various contracting failures, the asymmetries of information between seller and buyer and a lower bargaining power. By requiring consent, consumers would be indirectly affirming that they have voluntarily made the decisions.[7] Therefore, there are reasons to believe that, at least from the perspective of the consumer, the transaction is deemed beneficial.

Unfortunately, this traditional approach for the understanding of consent has failed to provide an effective protection to consumers against opportunistic and manipulative behaviours by their counterparties. On the contrary, the idea and regulatory requirements of 'consent' seems to have become a safe harbour for companies rather than an effective tool to protect consumers. Consequently, consumers might not provide consent based on their actual understanding of the facts and risks associated with their decisions. Therefore, while this is not necessarily undesirable, provided that some protections are put in place to protect consumers, it seems to reflect a failure of the underlying rationale of the traditional approach to consumer protection and consent.

Moreover, the digital transformation of many industries and the shift towards a more – data-based economy are changing the relationship between companies and consumers. The use of big data, Artificial Intelligence (AI) and Internet of Things (IoT) represent an immense potential for firms.[8] They allow companies to create better products and services tailored to their customers by increasing the firms' computational capacity to analyse large datasets in real-time and extract precious knowledge.[9]

However, in this data-driven era there are new risks for the protection of consumers. On the one hand, the concept and form of consents differs. On the other hand, companies have a better understanding of consumers' decisions and cognitive biases. Therefore, they design their products and marketing strategies to exploit those biases. At the same time,

---

[6] Eoin Carolan, *The continuing problems with online consent under the EU's emerging data protection principles*, 32 COMPUTER LAW & SECURITY REVIEW 1 (2016) https://www.sciencedirect.com/science/article/pii/S0267364916300322.

[7] Ari E. Waldman, *Cognitive Biases, Dark Patterns, and the "Privacy Paradox"*, ARTICLES & CHAPTERS 1332 (2020).

[8] Organisation for Economic *Co-operation and Development, Data-driven innovation for growth and well-being,* https://www.oecd.org/sti/ieconomy/data-driven-innovation.htm

[9] The value of the "data economy" in the EU was estimated more than EUR 285 billion in 2015, with a 5.03% annual growth. With the right policy and legal framework conditions, its value is expected to increase to EUR 739 billion by 2020. See Francesco Banterle, Data Ownership in the Data Economy: A European Dilemma (August 1, 2018) (on file with Springer).

there has been an increasing number of high-profile data breaches.[10] There is also a growing feeling of despondency amongst consumers who lack control over the interaction with firms, especially with regard to their privacy or their role in the decision-making process of a commercial relationship.[11] These issues raised a variety of challenges for consumer and data protection.

The paper starts with a discussion on the concept and implications of consent (section 2). We then analyse the operation and desirability of different regulatory approaches to provide consent and, more generally, consumer protection (section 3). The paper then discusses why the adoption of each model depends on a variety of country-specific factors (section 4), before providing with some conclusions (section 5).

2. Concept and implications of consent

2.1. Concept of consent

The concept of consent differs across jurisdictions and areas of law. For data protection, consumer protection, contract law, healthcare, and many other areas, the concept of consent might mean different things. For example, traditional contract doctrine views consent as the product of autonomy and choices resulting from human interactions.[12] In this context, consent involves an actual understanding of what one is doing.[13] In contract law, consent is also viewed as a concurrence of wills, voluntarily yielding one's will to the proposition of another.[14] Consent is an act of reason, accompanied with deliberation, the mind as weighing the balance of costs versus benefits.[15] It means voluntary agreement by a person in the possession and exercise of sufficient mentality to make an intelligent choice to do something proposed by another.[16] It supposes a physical power to act, a

[10] Chris Morris, *Hackers had a Banner Year in 2019*, FORTUNE (2020), https://fortune.com/2020/01/28/2019-data-breach-increases-hackers/.

[11] Vanessa Mak, *The Myth of the 'Empowered Consumer' - Lessons from Financial Literacy Studies*, TILBURG INSTITUTE FOR INTERDISCIPLINARY STUDIES OF CIVIL LAW AND CONFLICT RESOLUTION SYSTEMS (TISCO) WORKING PAPER SERIES ON BANKING, FINANCE AND SERVICES NO. 03/2012 (2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2077539; Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information,* PEW RESEARCH CENTER (2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/: Microsoft and International Data Corporation, *Microsoft – IDC Study: Only 31% of consumers In Asia Pacific trust organizations offering digital services to protect their personal data,* MICROSOFT ASIA NEWS CENTER (2019), https://news.microsoft.com/apac/2019/04/16/microsoft-idc-study-only-31-of-consumers-in-asia-pacific-trust-organizations-offering-digital-services-to-protect-their-personal-data/#_ftn1

[12] Joseph Savirimuthu, *Online Contract Formation: Taking Technological Infrastructure Seriously*, University of Ottawa Law & Technology Journal, Vol. 2, No. 1, p. 105, 2005. at 114.

[13] *Seriously*, University of Ottawa Law & Technology Journal, Vol. 2, No. 1, p. 105, 2005. at 130.

[14] Twin Ports Oil Co. v. Pure Oil Co., D.C.Minn., 26 F.Supp. 366, 371.

[15] 1 Story, Eq.Jur. § 222; Lervick v. White Top Cabs, La.App., 10 So.2d 67, 73.

[16] People v. Kangiesser, 44 Cal. App. 345, 186 P. 388, 389.

moral power of acting, and a serious, determined, and free use of these powers.[17] Consent is an act unclouded by fraud, duress, or sometimes even mistake.[18]

In other areas of law, consent is also a requisite for validating transactions. In healthcare, for example, *informed* consent allows patients to participate in their own medical care. This enables patients to decide which treatments they want or do not want to undergo. The collaborative decision-making process is an ethical and legal obligation of healthcare providers in many jurisdictions. The definition in consent might differ from contract law in some respects. Thus, in the healthcare context, the concept of consent is closely related to the information that is provided to the patient. Consent is necessary for all aspects of medical care, whether it is minor interventions with minimal risks or major interventions with significant risks or side effects.

In some countries, such as Singapore, medical providers need to inform patients of the purpose of tests, treatments or procedures offered to them, the benefits, significant limitations, material and more common risks (including those that would be important to patients in their particular circumstances) or possible complications, as well as what alternatives are available to them.[19] Even though there is some convergence with what contract law considers as consent, for healthcare regulators, *materiality* is something decisive when evaluating if the process of giving consent was correctly performed. Thus, materiality plays an important role in the process of giving consent and how medical providers need to document it and comply with it. This materially concept can be undermined when the provision of consent can conflict with saving lives. In this context, the latter goal will prevail over the former.[20]

Consumer protection is another area where the concept of consent is fundamental. Most regulatory approaches to consumer protection focus on consent and the importance of obtaining consent from consumers. Consumer protection law is made to protect consumers against unfair practices and to give consumers additional rights when goods received do not conform to contract.[21] Thus, the traditional approach to consumer protection posits that the consumer is in a state of inferiority in relation to the business providing goods and services.[22] In other words, it assumes some contracting failures, usually identified with greater asymmetries of information and a lower bargaining power against the consumer.[23]

---

[17] Fonblanque, Eq. b. 1, c. 2, s. 1; New Jersey Mfrs' Casualty Ins. Co., 148 A. 790, 791, 106 N.J.L. 238.
[18] Heine v. Wright, 76 Cal.App. 338, 244 P. 955, 956.
[19] Singapore Medical Council Handbook on Medical Ethics (2016 Edition) at 82–92. 2
[20] The Singapore Medical Council (SMC) Ethical Code and Ethical Guidelines (ECEG) 2016 Edition.
[21] Consumer Protection (Fair Trading) Act (Cap 52A, 2009 Rev Ed) at preamble.
[22] SHMUEL I. BECHER & OREN BAR-GILL, *Consumer Protection*, in Uriel Procaccia (ed.), THE ECONOMIC APPROACH TO LAW 223 (Nevo Pub 2012).
[23] Shmuel I. Becher, *Asymmetric Information in Consumer Contracts: The Challenge that is Yet to be Met,* AMERICAN BUSINESS LAW JOURNAL 45 (2008),

In the context of financial regulation, consumer protection is an essential role for regulators.[24] To achieve this goal, financial regulators have developed different tools to protect financial consumers and retail investors.[25] Disclosing risks to consumers, providing information, and obtaining consent are matters regulated by financial regulators. Recently, financial regulators have entered in the discussion on how to empower consumers over the data that the financial institution processes. There is a broad policy consensus that certain data about an individual should not be used by a business without the consent of that individual.[26] Further, that consent should be "informed" by appropriate knowledge.[27] A number of countries have adopted, or are favourably considering, some form of "open banking" requirement. The core idea behind open banking is that consumers have control over their data, such as the right to authorise third parties to access their financial data from a bank through an API (application program interface). Such third parties would most often be a financial technology ('fintech') firm, another bank, or another financial services provider. These third parties may use the data to offer more financial services to the consumer. The access to such personal data[28] presents challenges to financial institutions and third parties, because first, the digital aspect of these relationships might challenge traditional ways of obtaining consent, and second, the concept of consent has not been clearly defined in this context.[29]

The goals of consumer protection laws are very similar to those of data privacy: to protect the autonomy of people.[30] But the concept of consumer protection is more relatable to the layman. For example, where privacy and data protection laws involve complex balancing of interests in a variety of contexts, consumer protection specifically aims to address power differentials based on contracting failures, such as the asymmetries of

---

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1016010; Michael R. Baye & Joshua D. Wright, *How to Economize Consumer Protection*, KELLEY SCHOOL OF BUSINESS RESEARCH PAPER NO. 18-20 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3137122

[24] Analyzing the goals of financial regulation, see JOHN ARMOUR ET AL, PRINCIPLES OF FINANCIAL REGULATION (2016), pp. 61-72.

[25] Good Practices for Financial Consumer Protection, World Bank (June 2012), https://siteresources.worldbank.org/EXTFINANCIALSECTOR/Resources/Good_Practices_for_Financial_CP.pdf

[26] Nydia Remolina, *Open Banking: Regulatory Challenges for a New Form of Financial Intermediation in a Data-Driven World*, SMU CENTRE FOR AI & DATA GOVERNANCE RESEARCH PAPER NO. 2019/05 (2019). See also Markos Zachariadis & Pinar Ozcan, *The API Economy and Digital Transformation in Financial Services: The Case of Open Banking*, SWIFT INSTITUTE WORKING PAPER NO. 2016-001 (2017).

[27] Douglas J. Elliott, *Data Rights in Finance: Key Public Policy Questions and Answers* (2019), https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2019/may/Data%20Rights%20in%20Finance_POV_web_20190403.pdf

[28] In this paper we define "personal data" as any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data for the purposes of this paper.

[29] Sebastiao B. Vale, *PSD2, GDPR and Banking Secrecy: What Role for Consent?* LEXOLOGY (2019), https://www.lexology.com/library/detail.aspx?g=09534fc1-7f28-46c6-a7cb-20574fefe9de

[30] Michiel Rhoen, *Beyond consent: improving data protection through consumer protection law*, 5 INT. POL. REV. (2016) HELEN NISSENBAUM, PRIVACY IN CONTEXT 81–84 (2009).

information and differences in the level of bargaining power. Because of this specific intention, some scholars argue that applying consumer protection laws to privacy issues could help shift power back to consumers by improving participation and accountability.[31] Nonetheless, it is important to recognise some convergence in the regulatory objectives of data protection regulations and consumer protection laws -- both regulatory bodies seek to protect consumers by obliging their counterparties to provide some information in order to obtain consent. Many data protection regimes aim to empower consumers through this type of regulation.[32]

Some jurisdictions consider data privacy as a human right,[33] while others steer the discussion towards more consumer protection-centricity, and holding data controllers accountable.[34] These differences translate into different concepts of consent, which is one of the different tools for data protection.[35] It is important to take into account that in data protection regulations, consent is one of the many instruments for data protection. For instance, while being one of the most well-known legal bases for processing personal data, consent is only one of six bases mentioned in the General Data Protection Regulation (GDPR). The approach to data protection followed in Singapore is very similar in that sense: consent is also only one of the legal bases for processing personal data.

In the European Union, the GDPR has defined consent as being free, informed, specific, and unambiguous. [36] It also necessitates an opt-out option for data subjects, allowing for the partial or complete withdrawal of any previously given consent, and for the removal of all gathered personal data.[37] In Singapore, the Personal Data Protection Act (PDPA) comprises various rules governing the collection, use, disclosure and care of personal data. It recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose

---

[31] Michiel Rhoen, *Beyond consent: improving data protection through consumer protection law*, 5 INT. POL. REV. (2016).
[32] Charlie White, *Introducing Fairness to the Data Marketplace: Privacy Regulation & Consumer Empowerment* (2019), https://jsis.washington.edu/news/introducing-fairness-to-the-data-marketplace/. See also Chih-Liang Yeh, *Pursuing Consumer Empowerment in the Age of Big Data: A Comprehensive Regulatory Framework for Data Brokers*, 42 TELECOMMUNICATIONS POLICY 4, 282–292.
[33] Federico Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.,* TILBURG LAW SCHOOL RESEARCH PAPER NO. 15/2014 (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2482212; Danny O'Brien, *Data Privacy or Data Protection Day? It's a Human Right, Either Way,* ELECTRONIC FRONTIER FOUNDATION (2020), https://www.eff.org/es/deeplinks/2020/01/data-privacy-or-data-protection-day-its-human-right-either-way
[34] Henry S. Gao, *Data Regulation with Chinese Characteristics*, SMU CENTRE FOR AI & DATA GOVERNANCE RESEARCH PAPER NO. 2019/04 (2019). See also Man Yip, *Protecting Consumer's Personal Data in the Digital World: Challenges and Changes*, [2018] PDP DIGEST 104–117 (2018).
[35] Emmanuel Pernot-Leplay, *China's Approach to Data Privacy Law: A Third Way Between the US and the EU?* 8.1 PENN STATE JOURNAL OF LAW & INTERNATIONAL AFFAIRS (2020).
[36] General Data Protection Regulation , art. 4(11).
[37] General Data Protection Regulation , art. 7.

personal data for legitimate and reasonable purposes.[38] Section 13 of the PDPA prohibits organisations from collecting, using or disclosing an individual's personal data unless individuals give, or are deemed to have given, their consent for the collection, use or disclosure of their personal data. Section 14(1) of the PDPA states how an individual gives consent under the PDPA. An individual has not given consent unless the individual has been notified of the purposes for which his personal data will be collected, used, or disclosed and the individual has provided his consent for those purposes. If an organisation fails to inform the individual of the purposes for which his personal data will be collected, used, and disclosed, any consent given by the individual would not amount to consent under section 14(1).

In other words, despite the different regulatory approaches to data protection and consent, an individual has to know what they are consenting to.[39] For example, users who are on the wrong end of a substantial information asymmetry and regulation should take into account the costs and benefits of such intervention in the markets.[40] Users do not and cannot plausibly be expected to know everything for consent to be meaningful, especially if one makes the assumption that those users are following a risk/benefit model of economic rationality.[41] It is important to acknowledge that the strength of the consent must match the sensitivity of the data collected.[42]

The fast-changing digital times and the lack of clarity on the interpretation of current regulations mean that informed consent is hard to come by. In the digital world, obtaining consent in any context might present different challenges. Because of increased technological complexities and multiple data-exploiting business practices, it is hard for consumers to gain control. Therefore, individual control over personal data has become an important subject to adequately protect consumers.[43]

---

[38] Personal Data Protection Act Overview, https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act. Under the PDPA, there are two main forms of consent. Voluntary consent has to be given with a notification of purpose. It may also not be the condition for the provision of a service, nor can there be any deception or trickery involved in the obtaining of the consent. Deemed consent, on the other hand, appears to be a simpler matter. This occurs when the personal data is voluntarily given and it is reasonable to do so.

[39] Gordon Hull, *Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data*, ETHICS AND INFORMATION TECHNOLOGY 17:2 (December 2, 2014 at 89-101.

[40] Gordon Hull, *Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data*, ETHICS AND INFORMATION TECHNOLOGY 17:2 (December 2, 2014 at 89-101

[41] Megan Doerr, Christine Suver & John Wilbanks, *Developing a Transparent, Participant-Navigated Electronic Informed Consent for Mobile-Mediated Research* April 22, 2016 at 9..

[42]Lisa M. Austin, *Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices*, CANADIAN BUSINESS LAW JOURNAL, VOL. 44 (2006) at 21.

[43] Iris van Ooijen & Helena Vrabec, *Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective*, 42 JOURNAL OF CONSUMER POLICY 91–107 (2019).

However, current regulatory approaches to consent rely on certain assumptions about human decision making,[44] and they do not address a cost-benefit analysis when requiring consent. As a result, it seems to us that the concept of consent has a safe harbour for companies rather than an effective tool to protect consumers. While this is not necessarily undesirable, provided that some protections to consumers are put in place, it will generate various issues, and it undermines the power of consent to perform one of the functions that is supposed to perform: the protection of consumers.

Consent does not only represent an expression of choice but should be also an instrument to negotiate the economic value of personal information.[45] As digital services gain popularity, more and more governments are working on regulations that aim to address how to protect consumers. But there is a problem. As mentioned, most laws under consideration rely on consumer consent as a basic cornerstone. Even though this is not the only model, such a framework is deemed insufficient to protect consumer rights in today's highly complex world. For this reason, new models for consent, based more on the idea of 'smart disclosure' and 'actual understanding', have been put in place in the past decades.

2.2. Forms, stages and implications of consent

The forms and stages of consent from consumers to suppliers differ significantly between space and time in the relationship of these two parties. This is a fact often overlooked by regulators. How consent is given, and the allocation of risks - for instance in terms of data breaches and cybersecurity – should vary depending on the stage of the relationship between consumers and businesses.

Similarly, the determination of where and when a data breach occurs is also dependent on the stage of the data's life cycle. This cycle is the sequence of stages that a unit of data goes through from its initial generation or capture to its eventual archival and/or deletion at the end of its useful life.[46] Although specifics vary, data management experts often identify six or more stages in the data life cycle.[47] Something similar occurs with any relationship between customers and suppliers, and regulation regarding consent should

---

[44] Midas Nouwens, et al., *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence* (Jan 8, 2020) https://arxiv.org/pdf/2001.02479.pdf; Rafe Mazer & Kate McKee, *Consumer Protection in Digital Credit*, 108 CGAP FOCUS NOTE (August 2017). See also CARL SCHNEIDER & OMRI BEN-SHAHAR, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 59–78(2014)

[45] Max S. Oppenheimer, *Internet Cookies: When is Permission Consent?* NEBRASKA LAW REVIEW (November 2006).

[46] Anany V. Levitin & Thomas C. Redman, *A model of the data (life) cycles with application to quality*. 35 INFORMATION AND SOFTWARE TECHNOLOGY 4 (1993), p. 217-223. https://www.sciencedirect.com/science/article/abs/pii/095058499390069F

[47] Alex Ball, REVIEW OF DATA MANAGEMENT LIFECYCLE MODELS, University of Bath (2012).

reflect this. Therefore, requiring consent at the beginning of the relationship might not be sufficient if the supplier wants, for example, to transfer consumers' data to a third party.

Additionally, the digital transformation of many industries and the data economy is changing the relationship between firms and consumers. Specifically, the digital transformation of businesses should be considered when drafting regulation about consumer protection and how to obtain consent. New technologies are changing the way consumers have access to goods and services, as well as the way customers provide consent.[48] The new dynamic exacerbates some of the problems associated with the traditional models to provide consent and protect consumers. In a fast-paced digital world, virtually no one truly reads the online contracts, license agreements, terms of service or privacy policies.[49] Consumers accept when they click to confirm they have read and agree to terms and conditions, but several studies show this is far from the truth.[50]

One of the fundamental notions underlying data protection and privacy policy is autonomy for citizens over their data. In theory, it is the individual who decides where their data goes and what companies do with the information. In practice, however, whatever is stated in a provider's privacy policy usually dictates usage and disclosure of personal — sometimes sensitive — information. As a result, consent is insufficient to protect the consumers, their privacy, and their individual autonomy. [51]

3. Regulatory approaches

3.1. Imperfectly informed regime

3.1.1. Definition

This paper will refer to an 'imperfectly informed regime' to those regulatory approaches to consumer protection and consent where consumers are generally poorly informed. While this regime does not look very appealing, it offers many advantages, especially if a variety of *ex post* mechanisms to protect consumers are put in place. This imperfectly

[48] Some examples include the signing of paper consent statements, ticking a box online or on paper, responding to emails, and editing dashboard settings. See How Should We Obtain, Record and Manage Consent? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/.

[49] Gayatri Murthy & David Medine, *Data Protection and Financial Inclusion: Why Consent is Not Enough*, CGAP Blog (December 20, 2018) https://www.cgap.org/blog/data-protection-and-financial-inclusion-why-consent-not-enough.

[50] A recent Deloitte survey of 2,000 consumers found that 91 percent of people consent to legal terms and services conditions without reading them. For younger people, ages 18 to 34, the rate is even higher with 97 percent agreeing to conditions before reading. Even if someone wanted to be diligent and carefully read privacy notices, research shows it would take them 76 work days to read all the notices they should.Citation.

[51] Guy Aridor, Yeon-Koo Che & Tobias Salz, *The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR*, (January 29, 2020) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3522845.

informed system of consent and data protection, for example, has been followed by China.[52]

3.1.2. Rationale

The Chinese legislation is not particularly specific when it comes to attaching a legal definition to "personal data privacy".[53] The surveillance apparatus in China has made clear the government's ambitions to use technology to handle security issues.[54] Additionally, relaxing consent requirements might help innovation in early stages.[55] Proponents have argued that the trade-off between convenience and privacy justifies the acceptance of this approach. For instance, for some industry participants, Chinese internet services have developed rapidly through widespread access to the user data generated by mobile payments, food deliveries, ride-hailing, messaging, and other services.[56] Open access to user data has fuelled China's tech industry for the better part of the last decade.[57] Even though there is insufficient empirical evidence to support this argument, the sacrifice of privacy in favour of productivity seems to be most effective in jurisdictions with authorities that can provide an *ex post* oversight to what data controllers are doing with consumers data. Therefore, regardless of the *ex post* mechanisms for consumer protection existing in a country, this approach is also followed in countries where, as it

[52] 2018-2019 could be viewed as the time when the Chinese public woke up to privacy. When Robin Li, founder of Baidu, made the "trading privacy for convenience" comment in early 2018, his remark incited uproar amongst internet users. As luck would have it, Baidu was sued in the same year by a consumer rights protection group in Jiangsu province for collecting user data without consent (the lawsuit was later withdrawn, after the company removed the function to monitor users' contacts and activities). Chinese users recently challenged another internet giant, Alibaba, on personal data privacy. Ant Financial, Alibaba's financial arm has launched Zhima (Sesame) Credit, an online credit scoring service which offers loans based on users' digital activities, transaction records and social media presence. Users discovered that they had been enrolled in the credit scoring system by default and without consent. Under pressure, Alibaba apologized. Increasingly, Chinese consumers are vocally standing up for their privacy in front of internet giants. Meanwhile, the late-2018 China's People's Congress announced that China's personal data protection law was officially on the agenda of the current term of legislature. Together with the 2017 cybersecurity law and relevant parts of the 2018 e-commerce law, China's personal data protection law will lead to a comprehensive framework for individual data rights and protection. See World Economic Forum. https://www.weforum.org/agenda/2019/11/china-data-privacy-laws-guideline/

[53] Yuxiao Duan, *China's Private Law Approach to Personal Data Protection* (2019) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3484725.

[54] The country is increasingly protecting consumers from tech companies even as government surveillance intensifies. Samm Sacks & Lorand Laskai, *China's Privacy Conundrum*, SLATE (2019), https://slate.com/technology/2019/02/china-consumer-data-protection-privacy-surveillance.html; Ann Bartow, *Privacy Laws and Privacy Levers: Online Surveillance versus Economic Development in the People's Republic of China*, 74 OHIO STATE LAW JOURNAL 6, 854-895 (2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2368530

[55] For a general analysis between the connection of regulation and innovation, see Lev Bromberg, Andrew Godwin & Ian Ramsay, *Fintech Sandboxes: Achieving a Balance Between Regulation and Innovation*, 28 JOURNAL OF BANKING AND FINANCE LAW AND PRACTICE 4, 314–336 (2017).

[56] Harrison Jacobs, *Chinese people don't care about privacy on the internet – Here's why, according to a top professor in China*, BUSINESS INSIDER (June 26, 2018) https://www.businessinsider.sg/why-china-chinese-people-dont-care-about-privacy-2018-6?r=US&IR=T.

[57] Chenyu Liang, *Are Chinese people less sensitive about data privacy?* Sixth Tone (Mar 27, 2018) https://www.sixthtone.com/news/1001996/are-chinese-people-less-sensitive-about-privacy%3F.

happens in China, the value of data for the greater good is usually more important than the value of data as a fundamental right for individuals.[58]

3.1.3. Costs and benefits

While an imperfectly informed system of consent does not provide an effective tool to protect consumers at the time of making decisions, it has several benefits. First, this system can reduce transactions' costs. This can be beneficial for firms, since they would be required to provide full details of their transactions, but also for consumers, since they will not need to read the details of what they sign. Second, for a variety of reasons, including the availability of certain protections *ex post*, such as the possibility of initiating legal actions against opportunistic merchants, or the reliance on the regulatory authorities in charge of protecting consumers, consumers do not generally read what they sign.[59] Therefore, if consumers are properly protected *ex post*, perhaps an imperfectly informed system of consent can be desirable for both consumers and firms.

This system however, can also create some costs. First, the fact that consumers are not informed can create a problem of moral hazard, especially if consumers are properly protected *ex post*.[60] Therefore, it can lead to more reckless behaviour by consumers. Second, if consumers are *not* properly protected *ex post*, this regulatory model of consent can be used by service providers to opportunistically take advantage of consumers. In these circumstances, this model would not be desirable for consumers.

Finally, it should be taken into account that this model may work better in countries where people are more open and less sensitive about the privacy issue. If the cooperation between authorities, private sector and consumers lead the latest to trade privacy for convenience, safety, or efficiency, this regulatory model may seem convenient. For this

---

[58] This is a trend that has been exacerbated in light if the COVID-19 pandemic. Governments as well as public and private organisations have introduced several measures to tackle this crisis and help limit the spread of COVID-19. Some of these measures are data-driven and have been questioned for invading privacy and civil liberties in some jurisdictions. Mark Findlay & Nydia Remolina, *Regulating Personal Data Usage in Covid-19 Control Conditions,* SMU CENTRE FOR AI & DATA GOVERNANCE RESEARCH PAPER NO. 2020/04 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3607706

[59] For a general overview about consumers' failures and mistakes when entering into contracts, see Oren Bar-Gill, SEDUCTION BY CONTRACT: LAW, ECONOMICS, AND PSYCHOLOGY IN CONSUMER MARKETS (Oxford University Press 2012). See also Oren Bar-Gill, Omri Ben-Shahar & Florencia Marotta-Wurgler, *The American Law Institute's Restatement of Consumer Contracts: Reporters' Introduction*, 15 EUROPEAN REVIEW OF CONTRACT LAW 2 (2019); Omri Ben-Shahar, *The Myth of the 'Opportunity to Read' in Contract Law*, 5 EUROPEAN REVIEW OF CONTRACT LAW 1 (2009).
For prior literature that shows that consumers do not read contracts see David A. Hoffman, *From Promise to Form: How Contracting Online Changes Consumers*, 91 NEW YORK UNIVERSITY LAW REVIEW 1595 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2724661; Ian Ayres & Alan Schwartz, *The No-Reading problem in Consumer Contract Law,* 66 STANFORD LAW REVIEW 545 (2014), http://www.stanfordlawreview.org/wp-content/uploads/sites/3/2014/03/66_Stan_L_Rev_545_AyresSchwartz.pdf.

[60] Jeffrey L. Vagle, Cybersecurity and Moral Hazard, 23 STAN. TECH. L. REV. 71 (2020), 76–77.

reason, this approach may work well in places like China, but not on those where privacy is generally considered a fundamental right, as it may happen in Europe.[61]

3.2. Perfectly informed regime

3.2.1. Definition

Under a perfectly informed regime, consumers receive full information regardless of whether they understand this information or not. This is the regime implemented in the European Union under the General Data Protection Authority. Processing personal data is generally prohibited, unless it is expressly allowed by law or the data subject has consented to the processing. While being one of the more well-known legal bases for processing personal data, consent is only one of six bases mentioned in the GDPR.[62]

Consent must be freely given, specific, informed, and unambiguous.[63] In order to obtain freely given consent, it must be accorded on a voluntary basis. The element "free" implies a real choice by the data subject. Any element of inappropriate pressure or influence which could affect the outcome of that choice renders the consent invalid. In doing so, the legal text takes a certain imbalance between the controller and the data subject into consideration.[64] For consent to be informed and specific, the data subject must at least be notified about the controller's identity, what kind of data will be processed, how it will be used and the purpose of the processing operations as a safeguard against "function creep". The data subject must also be informed about his or her right to withdraw consent anytime. The withdrawal must be as easy as giving consent. Where relevant, the controller also must inform about the use of the data for automated decision-making, the possible risks of data transfers due to absence of an adequate decision or other appropriate safeguards. The consent must be bound to one or several specified purposes which must then be sufficiently explained. If the consent should legitimise the processing of special categories of personal data, the information for the data subject must expressly refer to

---

[61] Chinese users recently challenged the internet giant Alibaba on personal data privacy issues. Ant Financial, Alibaba's financial arm, launched Zhima (Sesame) Credit, an online credit scoring service which offers loans based on users' digital activities, transaction records and social media presence. Users discovered that they had been enrolled in the credit scoring system by default and without consent. Under pressure, Alibaba apologised. Increasingly, Chinese consumers are vocally standing up for their privacy in front of internet giants. Meanwhile, the late-2018 National People's Congress announced that China's personal data protection law was officially on the agenda of the current term of legislature. Together with the 2017 cybersecurity law and relevant parts of the 2018 e-commerce law, China's personal data protection law will lead to a comprehensive framework for individual data rights and protection. See Winston W. Ma, *China is waking up to data protection and privacy. Here's why that matters*, World Economic Forum (Nov 12, 2019) https://www.weforum.org/agenda/2019/11/china-data-privacy-laws-guideline/.

[62] The others are contract, legal obligations, vital interests of the data subject, public interest and legitimate interest as stated in Article 6(1) GDPR.

[63] General Data Protection Regulation, art 4(11). See also European Data Protection Board Guidelines 05/20 on Consent under Regulation 2016/679 (2020).

[64] Charlie White, *Introducing Fairness to the Data Marketplace: Privacy Regulation & Consumer Empowerment* (2019), https://jsis.washington.edu/news/introducing-fairness-to-the-data-marketplace/.

this. Finally, consent must be unambiguous, which means it requires either a statement or a clear affirmative act. Consent cannot be implied and must always be given through an opt-in, a declaration, or an active motion, so that there is no misunderstanding that the data subject has consented to the processing.[65] There is no form requirement for consent, even if written consent is recommended due to the accountability of the controller. It can therefore also be given in electronic form. In this regard, consent of children and adolescents in relation to information society services is a special case. For those under the age of 16, there is an additional consent or authorisation requirement from the holder of parental responsibility.[66] The age limit is subject to a flexibility clause. Member States may provide for a lower age by national law, provided that such age is not below the age of 13 years.[67] When a service offering is explicitly not addressed to children, it is freed of this rule. However, this does not apply to offers addressed to both children and adults.

3.2.2. Rationale

The rationale behind this approach is to empower consumers, especially with regard to their data.[68] This approach aims to build trust for consumers while enabling the development of the data economy.[69] Without trust, consumers will not allow companies to control and process their data, which in turn might curtail innovation and economic development.

3.2.3. Costs and benefits

Compared to the imperfectly informed model of consent, this regulatory option provides consumers with full information. Therefore, from an *ex ante* perspective, it seems a more desirable regulatory model, at least at a first glance. However, this regime has several flaws. First, the fact that consumers are provided with full information does not mean that they fully understand what they sign.[70] Secondly, a focus on information, rather than the quality and type of information, can end up doing more harm than good. Indeed, studies have shown that a system of mandatory disclosure fails.[71] Therefore, it would be better to provide less information but in a clearer manner.[72]

---

[65] General Data Protection Regulation, preamble (32).
[66] General Data Protection Regulations, art 8(1).
[67] General Data Protection Regulations, art 8(1).
[68] Charlie White, *Introducing Fairness to the Data Marketplace: Privacy Regulation & Consumer Empowerment* (2019), https://jsis.washington.edu/news/introducing-fairness-to-the-data-marketplace/.
[69] He Li, Lu Yu & Wu He, *The Impact of GDPR on Global Technology Development*, 22 JOURNAL OF GLOBAL INFORMATION TECHNOLOGY MANAGEMENT 1 (2019).
[70] Oren Bar-Gill, Omri Ben-Shahar & Florencia Marotta-Wurgler, *The American Law Institute's Restatement of Consumer Contracts: Reporters' Introduction*, 15 EUROPEAN REVIEW OF CONTRACT LAW 2 (2019).
[71] CARL SCHNEIDER & OMRI BEN-SHAHAR, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE (2014).
[72] INFORMATION OBLIGATIONS AND DISINFORMATION OF CONSUMERS, 77–79 (Gert Straetsmans eds.,2019).

Third, companies can circumvent around the legislation by using technology to deliberately create circumstances for consumers to revert to an imperfect information situation. Such practices are fodder for regulators to respond with more rules in a perfectly informed regime. In fact, it could be argued that the European regulation approach to consent and data privacy can ultimately become a 'compliance check box' that legalises such practices. If the company needs to explain the check box, the consumer will probably not consent to giving away her data to the company. In this case, just the fact of interrupting a web user to ask her to make a choice (i) accept the use of cookies, or (ii) not accept the cookies, the latter which effectively deprives the user of the services. By such choice architecture and pressure imposed on the user, one wonders about the validity of the acquired user "consent".

Finally, some studies have exposed the phenomena of service providers using manipulative designs and configurations to *nudge* or even compel users to give their consent. [73] This suggests that internet users in Europe are not actually benefiting from a legal framework that is supposed to protect their digital data from unwanted exploitation. Instead, consumers are rather being subject to a distracting, and disingenuous "consent theatre".[74]

Therefore, this system still needs to rely on *ex post* mechanisms to protect consumes such as regulators, lawyers, courts, and procedural rules. Otherwise, consumers will remain unprotected under this system of perfectly informed consent. As a result, while the aspirations of this system is very laudable, the desirability of this model depends on the particular features of a country, and the availability of enough protections *ex post*. If these protections are not provided, this system will just protect consumers on the books, but not in practice, converting this system in mere safe harbour for companies seeking to complete with data and consumer protection regulations. And even though this latter aspect can itself generate some benefits, especially in terms of legal certainty for companies, it is far from what it was expected from a theoretically protective regulatory framework for consumers such as the one promoted in the European Union.

Finally, one should consider that this type of regulatory approach may work well in environments where there is a strong sense of individual or consumer rights. Therefore, this perfectly informed regime may make more sense in Europe than, for example, China.

3.3. Smart disclosure regime

[73] For the concept and types of 'nudges', see CASS R. SUNSTEIN & RICHARD H. THALER, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH AND HAPPINESS (2008).
[74] Midas Nouwens, et al., *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence* (Jan 8, 2020) https://arxiv.org/pdf/2001.02479.pdf

3.3.1. Definition

The traditional approaches for consent and consumer protection explained in Sections 3.1 and 3.2 present some flaws. On the one hand, the imperfectly informed regime of consent does not provide consumers with enough tools to provide an informed consent. On the other hand, and as far as the perfectly informed regime is concern, many authors – especially in the behavioural literature- have shown, even with full information, people still make bad decisions.[75] This is due to several factors. First, the information is often disclosed in a manner that may opportunistically favour the interest of the sellers at the expense of consumers.[76]

Second, even if the seller does not act in an opportunistic manner, many products and information are complex to understand. Therefore, consumers can still make bad choices. The reason behind such pessimism[77] can be attributed to observations that disclosures which are verbose, and complex have become an everyday part of life for consumers in developed economies, particularly in the finance industry. Many attempts to improve such financial disclosures, including efforts to translate complex financial terms into simple terms in "plain English".[78]

Third, consumers face various cognitive biases that may undermine the quality of their decisions.[79] Indeed, a consumer needs to consider enough of relevant information in order to make a good purchase decision, such as avoiding buying a high-risk financial product if the former is a risk-averse consumer. Yet, evaluating relevant information can be a cognitively demanding exercise for the consumer, whether they are in a perfectly informed (full information given) or imperfectly informed (some information given) regime. In some cases, consumers themselves cannot absorb the amount of information, particularly for complex financial products. It has been academically found that the consumer's limited attention can curtail the effectiveness of disclosures.[80] As summed up by Nobel Laureate Daniel Kahneman, consumers are "influenced by all sorts of superficial things… they procrastinate and don't read the small print. You've got to create

[75] Rafe Mazer & Kate McKee, *Consumer Protection in Digital Credit*, 108 CGAP FOCUS NOTE (August 2017). See also CARL SCHNEIDER & OMRI BEN-SHAHAR, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 59–78(2014).
[76] Oren Bar-Gill, SEDUCTION BY CONTRACT: LAW, ECONOMICS, AND PSYCHOLOGY IN CONSUMER MARKETS (Oxford University Press 2012).
[77] Rafe Mazer & Kate McKee, *Consumer Protection in Digital Credit*, 108 CGAP FOCUS NOTE (August 2017).
[78] Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARVARD BUSINESS REVIEW (Jan–Feb 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers.
[79] Oren Bar-Gill, SEDUCTION BY CONTRACT: LAW, ECONOMICS, AND PSYCHOLOGY IN CONSUMER MARKETS (Oxford University Press 2012).
[80] George Loewenstein, Cass R. Sunstein & Russell Golman, *Disclosure: Psychology Changes Everything*, 6 ANNU. REV. ECON. 391–419 (2014).

situations that allow them to make better decisions for themselves."[81] Therefore, the objectives of a good disclosure regime should be to help the consumer navigate the information landscape to know (i) what they are getting, (ii) how to compare products and services and (iii) what consent to give.[82] In the spirit of promoting greater transparency for market competitiveness, the better the consumer can understand the features and prices of the financial product, the less the regulator needs to interfere in the market, thereby creating a win-win for all. As a result, it may be argued that a pragmatic approach based on a system of smart disclosure might be needed, and in fact this has been the tendency observed in many countries in the past decades.

This paper refers to the smart disclosure regime as a system of consumer protection and consent where consumers are supposed to provide a reasonably *informed* and unbiased consent. The idea of "smart disclosure" has been encouraging scholarship interest in various fields of law, to improving consumer choices.[83] The definition of smart disclosure refers to "the timely release of complex information and data in standardise, machine readable formats in ways that enable consumers to make more informed decisions."[84] Smart disclosures should be "adaptive, interoperable and innovative to markets providing more alternatives the consumer did not consider before or remind them to take something into account, but they may have forgotten."[85]

The genesis of the philosophy for the smart disclosure regime can be traced to a policy initiative by the US government to regulate information disclosure. Put simply, smart disclosure is defined as the "the act of making data more readily available and accessible, both to consumers directly and to innovators who can use it to build tools that help consumers make better informed decisions, and create more transparent, efficient market for goods and services."[86]

There is a spectrum regarding how a smart disclosure regime is carried out, from broad to specific uses: (i) government release of general data it collects on products and services; (ii) government release to citizens of their personal data (e.g. social security contributions and taxes); (iii) government release of data by private sector companies, pertaining to prices or information on products and services; and (iv) government release

---

[81] Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARVARD BUSINESS REVIEW (Jan–Feb 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers.
[82] Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARVARD BUSINESS REVIEW (Jan–Feb 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers.
[83] Marcelo Corrales et. al., *Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework*, in LEGAL TECH, SMART CONTRACTS AND BLOCKCHAIN 189–220 (2018).
[84] CASS R. SUNSTEIN, SIMPLER: THE FUTURE OF GOVERNMENT at 98 (2013).
[85] MARCELO CORRALES ET. AL., *Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework*, in LEGAL TECH, SMART CONTRACTS AND BLOCKCHAIN 189–220 at 220 (2018).
[86] NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, SMART DISCLOSURE AND CONSUMER DECISION MAKING: REPORT OF THE TASK FORCE ON SMART DISCLOSURE (2013).

to consumers of personal data held by private sector companies providing the products and services.[87]

In terms of addressing asymmetries of information, the motivation for smart disclosure is commendable – to return personal agency to the consumer, whether is it data about the citizen held by the government or data about the consumer held by the private sector company. This is done by transferring the control of personal data from the hands of corporate companies, back to the consumer.[88] In terms of execution, some authors have argued that for smart disclosure to be successful, data needs to be released (i) in a timely manner, (ii) in standardised, machine readable formats, (iii) such that it will enable consumers to make better decisions about finance, healthcare, or energy consumption etc.[89] Put simply, the copious pages of fine print in financial disclosure will need to be replaced by machine-readable files in standardised formats. This is so that algorithms can digest, translate, and analyse the data, then re-upload it on the internet or some third-party platforms for citizens or consumers to access.[90] From the paradigm of information sender-receiver, smart disclosure occurs when companies or governments provide the consumer or citizen with periodic access to his or her own data in open formats that enable him or her to easily put the data to use.

The US Securities and Exchange Commission arguably created the first use-case by mandating financial institutions to post information in the eXtensible Business Reporting Language (XBRL.)[91] This not only reduced the costs of compliance for the financial institution itself, but also improved business efficiency for analysts, auditors, investors, and regulators.[92] XBRL has also enhanced investment decision making for retail investors.[93]

3.3.2. Rationale

[87] Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARVARD BUSINESS REVIEW (Jan–Feb 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers.
[88] CASS R. SUNSTEIN, INFORMING CONSUMERS THROUGH SMART DISCLOSURE (2011).
[89] Alex Howard, *What is smart disclosure?* O'REILLY RADAR, (April 1, 2012) http://radar.oreilly.com/2012/04/what-is-smart-disclosure.html.
[90] Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARVARD BUSINESS REVIEW (Jan–Feb 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers.
[91] XBRL is a standards-based way to communicate and exchange business information between business systems. These communications are defined by metadata set out in taxonomies, which capture the definition of individual reporting concepts as well as the relationships between concepts and other semantic meaning. XBRL, *An Introduction to XBRL*, https://www.xbrl.org/the-standard/what/an-introduction-to-xbrl/; Securities and Exchange Commission Release No. 33-10514.
[92] Thomas R. Weirich & Steven Harrast, *Improving financial reporting with interactive data*, JOURNAL OF OF CORPORATE ACCOUNTING & FINANCE 21(2), 61–69.
[93] Rashmi Malhotra & Francis Garritt, *Extensible Business Reporting Language: The Future of E-Commerce-Driven Accounting*, 9 INTERNATIONAL JOURNAL OF BUSINESS 1 (2004).

This system of consent makes more sense for regulators interested in having well-informed and empowered consumers.[94] In 1854, Abraham Lincoln said that "the legitimate object of government is to do for the people what needs to be done, but which they cannot by individual effort do at all, or do so well, for themselves."[95] The motivation behind a smart disclosure regime for the US, argues Howard, is rooted in Lincoln's thesis about the role of government.[96] When consumers have access to their own personal data and the market provides the technology to make it possible, citizens will be more conscious about the choices they need to make on economic, education and lifestyle decisions.[97] With this heightened consciousness, consumers can achieve aspirational non-economic outcomes such as better physical and mental well-being.[98]

In the context of financial decisions, it has been posited that mandatory disclosures, if designed well, can help the retail investor to understand and evaluate the financial product more effectively, enabling such consumers to easily put such data to use.[99] For example, when private insurers release detailed product data to web aggregators like www.comparefirst.sg, customers looking to purchase life insurance in Singapore can make better finance decisions.

3.3.3. Costs and benefits

A smart disclosure regime can create several benefits.[100] First, it may improve consumer well-being by improving the quality in their decisions in complex markets. Indeed, when consumer must make complex choices, whether they are searching for life insurance, retirement funds or airline flights. The personal productivity trade-offs for consumers to seek out the best deal is two-fold: (i) time and effort needed to research about the product, and (ii) whereupon there is incomplete information, consumers often end up making a sub-optimal decision by either over-paying, missing out on better deals or finding out about hidden fees later on. Such suboptimal decisions do not just hurt consumers' pocketbooks. In microeconomics, poor choices by consumers can result in diminishing overall market efficiency.[101] Conversely, a well-functioning consumer market can result

---

[94] MONETARY AUTHORITY OF SINGAPORE, TENETS OF EFFECTIVE REGULATION (2010).
[95] THE COLLECTED WORKS OF ABRAHAM LINCOLN (2006), https://quod.lib.umich.edu/l/lincoln/lincoln2/1:261?rgn=div1;view=fulltext.
[96] Alex Howard, *What is smart disclosure?* O'REILLY RADAR, (April 1, 2012) http://radar.oreilly.com/2012/04/what-is-smart-disclosure.html.
[97] Ibid
[98] Ibid
[99] Adrian Hillenbrand & Andre Schmelzer, *Beyond Information: Disclosure, Distracted Attention, and Investor Behavior*, PREPRINTS OF THE MAX PLANCK INSTITUTE FOR RESEARCH ON COLLECTIVE GOODS NO. 2015/20 (2015).
[100] NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, SMART DISCLOSURE AND CONSUMER DECISION MAKING: REPORT OF THE TASK FORCE ON SMART DISCLOSURE (2013). See also Djoko S. Sayogo, *Going beyond open data: Challenges and motivations for smart disclosure in ethical consumption*, 9 JOURNAL OF THEORETICAL AND APPLIED ELECTRONIC COMMERCE RESEARCH 2, 1–16 (2014).
[101] BRIAN T. RATCHFORD, CONSUMER SEARCH BEHAVIOUR AND ITS EFFECT ON MARKETS (2009).

in increased consumer ability to make informed choices. At the national level, consumer choices can impact policy issues too. Consider consumers' decisions about higher education, energy consumption, and mortgages for example. A well-informed populace who makes optimal choices in healthcare, finance, and education can positively affect the entire nation's competitiveness, security, and fiscal health.

Second, this system empowers consumers. Not only does it make them the real centre of privacy and data protection laws, at least from an *ex ante* perspective, but it also reduces moral hazard. Besides, by being empowered, consumers can also make smarter decisions for their own interest. For example, through the Green Button initiative in the US, energy companies are sharing customers' energy consumption data with customers themselves, so that the latter can save money on their electricity bills.[102] In the context of health financing, smart disclosures have provided patients better access to their own health records so that they can make informed choices about insurance plans and healthcare providers.[103]

Third, when data is needed to empower consumers via smart disclosure, technology need to be deployed to ensure such data reaches the customer efficiently and effectively, just as big data helped companies gain competitive business intelligence.[104] As mentioned by Thaler and Tucker, the information symmetry provided by a smart disclosure regime do not only benefit consumers economically and socially, suppliers can gain by providing high-quality products at good prices, without the risk of losing out to less scrupulous firms that compete through obfuscation. [105] With ethical consumption as a driving principle, entrepreneurs and innovators can win by devising new ways of serving consumers.[106]

Fourth, the most widely quoted study of how open data can drive the economy – the authors predicted that between US$3 to 5 trillion per year could be reaped across the global economy: education, transportation, consumer products, electricity, oil and gas, health care, and consumer finance.[107] Take the API for Global Positioning System (GPS) innovation, for example. While it has been a bane for printers of physical maps, it has

---

[102] Djoko S. Sayogo & Theresa A. Pardo, *Understanding Smart Data Disclosure Policy Success: The Case of Green Button*, THE PROCEEDINGS OF THE 14TH ANNUAL INTERNATIONAL CONFERENCE ON DIGITAL GOVERNMENT RESEARCH (2013).
[103] Djoko S. Sayogo et. al., *Information flows and smart disclosure of financial data: A framework for identifying challenges of cross boundary information sharing*, 31 GOVERNMENT INFORMATION QUARTERLY 1 (2014).
[104] Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARVARD BUSINESS REVIEW (Jan–Feb 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers.
[105] Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARVARD BUSINESS REVIEW (Jan–Feb 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers.
[106] Djoko S. Sayogo, *Going beyond open data: Challenges and motivations for smart disclosure in ethical consumption*, 9 JOURNAL OF THEORETICAL AND APPLIED ELECTRONIC COMMERCE RESEARCH 2, 1–16 (2014).
[107] James Manyika et. al., *Open data: Unlocking innovation and performance with liquid information*, MCKINSEY GLOBAL INSTITUTE REPORT (October 2013).

been a boon for the economy, attributing about $90 billion in growth to the US economy in 2011, enabling innovators to write new apps and create jobs.[108]

Fifth, with better well-being outcomes, such consumer consciousness can also be extended to the supply of useful personal data to companies and government, thereby creating a positively reinforcing loop. This is based on the microeconomic assumption that better-informed consumers will make decisions that reflect their valence towards that product or service, which sends feedback to the supply chain to produce and operate in more sustainable modes.[109]

Finally, when governments improve how they interact with citizens and businesses, by cutting the paperwork burden substantially, it creates a reciprocal loop of collecting more useful information for policy making.[110]

Despite the benefits associated with this model, there are also some costs and challenges.[111] First, the concept of 'smart disclosure' might not be clear. Therefore, not only can it create uncertainty but, if it is not properly designed, it can lead to bad choices and outcomes. Therefore, the successful implementation of this system would require a qualified body of judges and regulators, which is something that unfortunately cannot be found in all jurisdictions.

Second, a smart disclosure regime works best if data is structured because information that is given in a structured format provides for better data analysis. In the past, searching through unstructured data, even if it is open data, can be extremely tedious for the retail investor who must thumb through pages of physical print-outs or execute numerous *control-F* word searches on their computer just to make sense of the financial reports. On the other hand, when a financial disclosure can be organised and tagged with definitional information, or metadata, the user can quickly and easily locate relevant and useful information. This will require the corporate issuer to implement data tagging, which will result in additional costs when filing their disclosures. The increased overheads are dependent on how the issuer chooses to standardise data – if the tagging is done at the end of the report, the preparation will be onerous and costs will be recurring, but if the standardised tagging is embedded in the company's internal processes from start to finish, the one-time set-up costs will result in long-term savings for the issuer.[112] It has been

---

[108] Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARVARD BUSINESS REVIEW (Jan–Feb 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers.
[109] CASS R. SUNSTEIN & RICHARD H. THALER, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH AND HAPPINESS (2008).
[110] Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARVARD BUSINESS REVIEW (Jan–Feb 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers.
[111] Analysing the perils of a smart disclosure regime, see Oren Bar-Gill, *Smart Disclosure: Promise and Perils*, BEHAVIOURAL PUBLIC POLICY (July 11, 2019).
[112] Rick A. Fleming, *Improving Disclosure with Smart Data* (Oct 24, 2016) https://www.sec.gov/news/speech/improving-disclosure-with-smart-data.html.

suggested that large, technologically sophisticated companies should be persuaded to offer smart disclosures as the direct costs of compliance for them are lower than for smaller firms who do not have the necessary resources.[113]

Third, it is not even clear whether regulators should 'nudge' individuals.[114] While this regulatory approach is becoming more successful internationally, some authors have argued that the role of the regulators should just focus on enacting laws (e.g., requiring information) and enforcing them.[115] Therefore, for many critics of the smart disclosure regime, a system of perfectly informed regime may actually be more desirable since it would be more in line with people's freedom of choice. The reason being, these choices would not be affected by the regulator.

Fourth, even with a system of smart disclosure, it is not clear that consumers will always make the 'right decision'. In fact, the concept of right decision is subjective, and its assessment might need to be made *ex post* and therefore subject to hindsight bias.[116]

Fifth, when it comes to data privacy issues, consumers may not value their data, at least as one might expect at first. In a study conducted by Winegar and Sunstein, it was found that people are willing to pay US$5 to preserve their data, but ask for US$80 to have access to their privacy, to which the authors raise serious doubts about whether consumers are making reasonable trade-offs when giving up their data.[117] On the one hand, consumers are saying that they greatly value their own data privacy, yet on the other hand, readily give consent to forego that privacy by providing access to that data.[118] There is divergence between statements of value and actual behaviour. This is coupled with imperfect information and the wide variation in monetary valuation depending on seemingly irrelevant contextual features.[119] Both challenges make it exceedingly difficult to place any kind of monetary value on data privacy.[120] As with the perfectly informed (full information given) and imperfectly informed (partial information) disclosure

---

[113] Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARVARD BUSINESS REVIEW (Jan–Feb 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers.

[114] For an analysis of the ethical issues surrounding nudges as well as their desirability, see Cass R. Sunstein, THE ETHICS OF INFLUENCE: GOVERNMENT IN THE AGE OF BEHAVIORAL SCIENCE (Cambridge University Press, 2016).

[115] For an analysis of this discussion, see House of Lords Science and Technology Select Committee, *Behaviour Change Report*, HL PAPER 179 (2011). See also Jacob Goldin, *Which Way to Nudge? Uncovering Preferences in the Behavioral Age*, 125 YALE LAW JOURNAL 1, 325 (2015).

[116] Neil J. Roese & Kathleen D. Vohs, *Hindsight Bias*, 7 PERSPECTIVES ON PSYCHOLOGICAL SCIENCE 5, 411–426 (2012).

[117] Angela G. Winegar & Cass R. Sunstein, *How much is data privacy worth? A preliminary investigation*, HARVARD LAW SCHOOL DISCUSSION PAPER NO. 1017 (2019).

[118] Sarah Spiekermann et. al., *E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior*, IN PROCEEDINGS OF THE 3RD ACM CONFERENCE ON ELECTRONIC COMMERCE (2001).

[119] Alessandro Acquisti et. al., *What is Privacy Worth?*, 42 THE JOURNAL OF LEGAL STUDIES 2, 249 (Jun 2013).

[120] Angela G. Winegar & Cass R. Sunstein, *How much is data privacy worth? A preliminary investigation*, HARVARD LAW SCHOOL DISCUSSION PAPER NO. 1017 (2019).

regimes discussed in the first part of this paper, a smart disclosure regime must deal with issues of privacy and data security as well.[121] In a smart disclosure regime, companies that allow a consumer to access the latter's own data are already required to do so in a secure manner, negating any infarctions to her privacy. There are, however, some security concerns that companies need to address. As with the conflicting polls done in industry against academic research to how much consumers really value their privacy, more congruence needs to be established on whether a smart disclosure regime will enable consumers to make reasonable trade-offs when consenting to give their data to private companies.

Blis.com, a location data AI firm, carried out a study to understand how much consumers value their data.[122] The firm found that two in three customers are more knowledgeable about how their personal information is being utilised by companies, compared to a year ago. In addition, the surveyors found that customers are open to sharing their information if (i) it is carried out "transparently", and (ii) there is some reciprocal economic value from the merchant, in return to the former for sharing their data.[123] For example, the survey revealed that 70 percent of respondents are willing to reveal their buying history to Amazon if the latter can give them a 10-30% discount off their next purchase. In this case, consent by the consumers bears an economic value. Some authors have shown that consumers are concerned about their data but not quite enough to stop handing it over completely.[124] For most consumers, they are willing to trade off their email address, household details in return for higher personal commodity called *time* (or convenience). In a Salesforce survey, 63% of millennials and 58% of Gen-X respondents are happy to share their data with companies to get personalised offers and information.[125] It is this personalisation that saves the consumer time, which otherwise the consumer would spend researching, browsing, and interacting with companies to find the best deals.[126]

Sixth, since consumers will be more empowered, and therefore more protected *ex ante,* regulators may have incentives to relax their *ex post* strategies. And if so, the system

---

[121] Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARVARD BUSINESS REVIEW (Jan–Feb 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers.
[122] Consumers are Realising the Value of their Data. Here's How Online Marketers Should Respond (Mar 25, 2019) , https://blis.com/consumers-are-realizing-the-value-of-their-data-heres-how-online-marketers-should-respond/.
[123] Consumers are Realising the Value of their Data. Here's How Online Marketers Should Respond (Mar 25, 2019) , https://blis.com/consumers-are-realizing-the-value-of-their-data-heres-how-online-marketers-should-respond/.
[124] Axel, *How Concerned are Consumers Really When it Comes to Data Privacy?*, MEDIUM (Aug 19, 2018), https://medium.com/@AxelUnlimited/how-concerned-are-consumers-really-when-it-comes-to-data-privacy-21c4587ddc5c.
[125] State of the Connected Customer (2016), https://www.salesforce.com/research/customer-expectations/.
[126] Axel, *How Concerned are Consumers Really When it Comes to Data Privacy?*, MEDIUM (Aug 19, 2018), https://medium.com/@AxelUnlimited/how-concerned-are-consumers-really-when-it-comes-to-data-privacy-21c4587ddc5c.

might end up undermining consumer protection if, by any chance, the system of smart disclosure is not properly designed, or consumers still make poor decisions.

Seventh, it is not clear that consumers want to make informed decisions. While we believe that they do want to have the opportunity to have access to this information, perhaps they may have incentives to avoid reading these details, especially if they know that some *ex post* mechanisms will be available to protect them – encouraging firms *ex ante* to put in place safeguards for consumers.

Finally, it should be taken into account that the adoption of a system of smart disclosure regime implies various challenges in terms of implementation. First, in Europe, for example, the GDPR strengthens the definition of consent, which must be concise, unambiguous, clear, and freely given. For consumers to understand the implications when giving consent, companies are no longer be able to use long terms and conditions full of legal jargon.[127] It has been suggested that the legal requirements for disclosures should be incorporated at the earlier stages of website design. These websites operate specifically on the Cloud. Essentially, the proposal consists of a set of legal questions which can help check the computer codes which process the information in the Cloud computing architectures. The legal questions in turn, can help Cloud providers to comply with the legal requirements of the GDPR.[128] In Asia, Singapore's central bank, the Monetary Authority of Singapore, published a set of general principles and recommended practices for drafting prospectuses and profile statements to improve their readability and facilitate investors' understanding of key information.[129] The guidelines include common drafting issues, recommended practices in the use of language, structure and document length. The Monetary Authority of Singapore (MAS) approach, like the GDPR, nudges the financial industry towards helping consumers understand and make smart decisions when faced with complex choices. The next step would be for companies to develop user-centred agreements based on behavioural and computer sciences for more personalised, data-driven tools, as well as interactive designs to help consumers navigate complex terms and conditions to give their consent.

Second, another challenge for regulators is the development of guidelines that improve smart disclosure without imposing significant sludge on firms. For the financial industry for example, consumer complaints about hidden fees are most vociferous when disclosure of such costs is buried in fine print. By making all fees transparent, central banks of the world can expend fewer resources to police fee disclosure compliance on financial

[127] TIJMEN H. A. WISMAN, *Privacy, Data Protection and E-Commerce*, in EU REGULATION OF E-COMMERCE: A COMMENTARY (Arno R. Lodder & Andrew D. Murray eds., 2017).
[128] MARCELO CORRALES ET. AL., *Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework*, in LEGAL TECH, SMART CONTRACTS AND BLOCKCHAIN 189–220 at 220 (2018).
[129] Monetary Authority of Singapore, Guidelines on Disclosure of Financial Information in Prospectuses (2005), https://www.mas.gov.sg/regulation/guidelines/guidelines-on-disclosure-of-financial-information-in-prospectuses.

institutions. Regulators can then focus on the broader issues of making markets open and competitive and stimulating job growth. Much national productivity can be gained by reducing or eliminating the need for endless cycles of regulation and levelling the playing field.

Third, besides monitoring the financial institutions, it is also important to consider how the regulation of third-party websites can make the smart disclosure regime more effective. An undesirable outcome, for example, would be to simply transfer the source of disclosure obfuscation from financial institutions to such third-party websites. Regulation can help to ensure that such third-party websites are transparent, e.g. consumers being informed when a website aggregator is receiving commissions from service providers for the choices displayed. Specifically, consumers who access web aggregators for mortgages or credit card plans are unlikely to know for sure whether they have been given the best possible deal. In such cases, non-public sector organisations like non-profits such as the Consumer Association of Singapore (CASE), could use tactics like mystery shoppers to assess the accuracy of advice the web algorithms are providing. Such non-profits would still need the authority to audit the advice if there is reason to suspect that it is biased. Preferably, this market should be self-regulating, where competitors and consumers can help keep these third-party websites authentic. Regulators can retain the role of watchdog of last resort, to monitor and audit recommendations.

Fourth, the implementation of this approach may require other challenges. For example, in the case of mortgages, the price is probably the only feature that consumers care about, and any obfuscation of the rest of the product becomes tangential.[130] Something similar happens for complex financial products like leveraged loans mutual funds,[131] layering product attributes on top of one another may make the disclosure in a perfect regime inefficient for the market. Based on the principle of consumer protection, smart disclosure can solve this problem if financial institutions were required to identify the key salience of the investment product in their disclosures. In practice however, such a rule can be circumvented by inexpensive copywriting and editing. By the time the funds are sold to retail institutions such as banks, the new disclosures are rendered technically unique.[132] As the smart disclosure regime evolves, perhaps technology and determined start-up founders can help solve this problem. After all, electronic disclosure is by nature flexible and adaptable. Such properties must be exploited to accommodate new products and

[130] Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARVARD BUSINESS REVIEW (Jan–Feb 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers.
[131] Sally Bakewell, *Retail Investors Creep Back to Loan Market that Didn't Miss Them*, BLOOMBERG (Sep 12, 2019) https://www.bloomberg.com/news/articles/2019-09-11/retail-investors-creep-back-to-loan-market-that-didn-t-miss-them.
[132] Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARVARD BUSINESS REVIEW (Jan–Feb 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers.

services.[133] As a result of the aforementioned factors, the desirability of the system of smart disclosure is far from clear.

4. Toward a country-specific approach

All the existing regulatory models to provide consent and provide protection to consumers present both advantages and disadvantages. In our opinion, despite the current tendency to adopt a system of 'smart disclosure regime', in which the consumer is supposed to be empowered at the moment of providing consent, there are not any 'optimal' regulatory approach. Indeed, one size does not fit all, and the same applies to consumer and data protection laws.

In our view, the optimal regulatory approach to consumer and data protection will depend on a variety of country-specific factors. For example, in countries with reliable *ex post* remedies to protect consumers (e.g., good regulators, efficient judicial systems, existence of class actions, developed market of litigation lawyers, etc), the perfectly or even imperfectly informed regimes may actually work. In fact, these regulatory models may even be preferred by consumers, since they can be more relaxed when making their decisions, and they could save the costs associated with gathering and analysing information. At the same time, companies may also prefer this system, since it is easier to implement and it can create more legal certainty. However, in countries without reliable institutions and other *ex post* remedies to protect consumers, the use of *ex ante* strategies should be favoured. Therefore, in these countries, it would make more sense to adopt a system characterized for putting more emphasis on the idea of *informed* consent, such as it implies the smart disclosure regime.

Finally, it should be taken into account that, along with the desirability of each regulatory model in a particular country, another factor affecting the implementation of each system can be the political economy of the country, or the perception and value of data privacy. These factors can also explain some of the divergences observed across jurisdictions.

5. Conclusion

Traditionally, consumer and data protection policies evolved from issues of consent and information disclosure. The purpose of these regulatory approaches was the protection of consumers by reducing some contracting failures, such as asymmetries of information and a lower bargaining power, particularly existing in transactions involving complex issues such as financial products and sensitive personal data. In the past, regulators have responded to privacy and consumer protection by adopting what this article refers to as

[133] Richard H. Thaler & Will Tucker, *Smarter Information, Smarter Consumers*, HARVARD BUSINESS REVIEW (Jan–Feb 2013), https://hbr.org/2013/01/smarter-information-smarter-consumers.

an "imperfectly informed regime", in which consumers do not receive full information about the risks associated with their decisions, even if they are still protected (if so) through a variety of *ex post* mechanisms such as the judicial system or a consumer protection authority. More recently, other jurisdictions, such as the European Union, have adopted a "perfectly informed regime" for data protection based on the idea of full disclosure. While this approach has some advantages, it does not effectively make consumers understand the consequences and risks associated with their decisions. Therefore, unless the system still provides reliable mechanisms *ex post* to protect consumers, there will still be a high risk of opportunism of merchants vis-à-vis consumers. As a response to the weaknesses existing in the traditional regulatory approaches to protect consumers, behavioural economists have proposed a new system based on the idea of 'smart disclosure'. According to this system, consumers should get an actual understanding of their decisions, and this can be done by forcing their counterparties to provide a clear and understandable information about the content and risks associated with those decisions made by consumers. While this regulatory approach has become very popular, this paper has argued that it is not perfect either. Namely, it has been pointed out, that, even though this system can be desirable for countries without reliable institutions to protect consumers *ex post*, the adoption of this regulatory approach faces several challenges. Therefore, in countries with efficient mechanisms *ex post* to protect consumers, this system might not be needed, and the traditional regulatory models can be more desirable. Based on this idea, this paper concludes by arguing that, despite the international tendency to favour systems of smart disclosure or perfectly informed regimes, each regulatory approach has its advantages and disadvantages, and the most desirable one will depend on the particular features of a country.