PROTECTING FINANCIAL CONSUMER DATA IN DEVELOPING COUNTRIES: AN ALTERNATIVE TO THE FLAWED CONSENT MODEL

KATHARINE KEMP AND ROSS P. BUCKLEY

(2017) 18(3) *Georgetown Journal of International Affairs* 35
[2018] *UNSWLRS* 57

UNSW Law
UNSW Sydney NSW 2052 Australia

Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model

Katharine Kemp[1]
Ross P. Buckley[2]

Introduction

"Big data" analytics and other data-driven innovations have recently been promoted as important tools for advancing digital financial inclusion in developing countries,[3] permitting financial services providers to offer credit to consumers without a formal credit history and design products which meet local consumers' needs.[4] However, these new data practices also create significant risks, including data theft, fraud, and potentially financial *exclusion*. Nonetheless, many providers and standard-setting bodies consider that data practices can be justified if consumers provide their informed consent to the relevant collection, use, sharing, and storage of their data.

We argue that this traditional "informed consent" model for consumer data protection has real weaknesses in effectively protecting the privacy of consumers in developing countries.

---

[1] Research Fellow, and Member, Centre for Law, Markets and Regulation, Faculty of Law, UNSW Sydney.

[2] King & Wood Mallesons Chair of International Financial Law, Scientia Professor, and Member, Centre for Law, Markets and Regulation, Faculty of Law, UNSW Sydney. We are grateful for the research funding for this article provided by the Australian Research Council ('ARC') and the United Nations Capital Development Fund ('UNCDF') through ARC Linkage Project 150100269; and also for the perspicacious comments of the anonymous referees. Thanks also to Wilson Zhang, for his research assistance, all responsibility is ours.

[3] See, eg, Arjuna Costa, Anamitra Deb and Michael Kubzansky, "Big Data, Small Credit: The Digital Revolution and Its Impact on Emerging Market Consumers" (2016) 10 *Innovations* 49. "Digital financial inclusion" has been defined as "digital access to and use of formal financial services by excluded and underserved populations": Timothy Lyman and Kate Lauer, "What is Digital Financial Inclusion and Why Does It Matter?" (CGAP Blog, 10 March 2015).

[4] Kathleen Yaworsky, Dwijo Goswami and Prateek Shrivastava, "Unlocking the Promise of (Big) Data to Promote Financial Inclusion" (Accion Global Advisory Solutions, Accion Insights, March 2017) 3; Global Partnership for Financial Inclusion, "Global Standard-Setting Bodies and Financial Inclusion: The Evolving Landscape" (G20 Global Partnership for Financial Inclusion, March 2016) 63.

This model may make services more accessible but also significantly increases the likelihood of private information being exposed. We propose an alternative approach to financial consumer data protection, which takes account of the modern dynamics of digital data collection, use, sharing and storage, and the limitations of consumers individually negotiating acceptable levels of data protection. This alternative approach would be for regulators, industry and scholars to: recognize that the problem of consumer data protection is not solved by consumers supposedly providing consent to data practices; reframe the discourse to avoid euphemisms and assumptions which unjustifiably favor provider interests; recognize that data protection and innovation need not be a zero-sum game; and more broadly, challenge the validity of the dominant "privacy self-management" paradigm in the context of developing countries.

Financial Inclusion Benefits from Digital Financial Services and Data-Driven Innovations

Digital financial services have been widely accepted as important for improving financial inclusion in developing countries. Increased mobile coverage, mobile phone ownership, and innovative delivery of financial services via new technological channels are permitting increased access for those who have not been served by traditional financial services.

Applying "big data" analytics and other data-driven innovations can bring further benefits. "Big data" refers broadly to the relatively new phenomenon of firms capturing, and using, very large quantities of data. "Big" data is generally considered to have four attributes: volume (it is collected on a very large scale), velocity (it is collected very rapidly or in real time), variety (it is collected from a number of sources), and value (it is accurate and useful).[5] This data is then analyzed, increasingly by the application of algorithms, to discern correlations which can then underpin business decisions.[6]

[5] See Daniel J Solove, "Introduction: Privacy Self-Management and the Consent Dilemma" (2013) 126 *Harvard Law Review* 1880, 1889–90; Lokke Moerel and Corien Prins, "Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things" (25 May 2016) 14–5.

[6] See Yaworsky, Goswami and Shrivastava, above n 4.

The use of big data analytics enables financial services providers to extend formal credit to some consumers for the first time.[7] Traditional lending models have often failed to serve poor consumers because they have no formal credit history, and other methods of assessing their creditworthiness (e.g., physical visits and interviews) are not cost effective given the small amounts of money involved.[8]

Some providers and credit scorers now use digital records of mobile phone usage, mobile phone recharge history, utility bill payments, and even social media activity to determine the borrower's likely willingness and ability to make repayments.[9] Similar digital records have been used by providers to supply services to customers who lack formal identification documents,[10] and to tailor new products to particular types of consumers based on their behavior and demographic information.[11]

Potential Harms from Financial Consumer Data Practices

However, the collection and analysis of vast swathes of consumer data give rise to concerns for the protection of financial consumers' data and privacy rights in developing countries.[12] The mere collection and storage of personal data exposes consumers to increased risks.[13] New data collection and storage technologies allow more data to be collected and stored

[7] Ibid 9-11. See also Rafe Mazer, Jessica Carta and Michelle Kaffenberger, "Informed Consent: How Do We Make It Work for Mobile Credit-Scoring" (CGAP Blog, 2 September 2014).

[8] See Costa, Deb and Kubzansky, above n 3, 49–53.

[9] See Yaworsky, Goswami and Shrivastava, above n 4, 9–11, 29–33; Productivity Commission, Australian Government, "Data Availability and Use" (Productivity Commission Inquiry Report No 82, 31 March 2017) 543, 546; Tom Groenfeldt, "Lenddo Creates Credit Scores Using Social Media" (Forbes Online, 29 January 2015) <https://www.forbes.com/sites/tomgroenfeldt/2015/01/29/lenddo-creates-credit-scores-using-social-media/#184cb64c2fde>.

[10] See, eg, "GPFI Global-Standard Setting Bodies and Financial Inclusion", above n 4, 63.

[11] Ibid. See also Productivity Commission, above n 9, 541 et seq.

[12] See, eg, "GPFI Global-Standard Setting Bodies and Financial Inclusion", above n 4, 63–4; David Medine, "Making the Case for Privacy for the Poor" (CGAP Blog, 15 November 2016); Kate McKee, "503.2 Million Reasons to Tackle Data Protection Now" (CGAP Blog, 10 November 2016).

[13] See Justin Brookman and J S Hans, "Why Surveillance Matters: Surveillance as a De Facto Privacy Harm" in *Big Data and Privacy: Making Ends Meet* (The Center for Internet Society, Stanford Law School, and Future of Privacy Forum, 2013) 11–3.

more rapidly, more cheaply, and more permanently than ever before.[14] However, the more data is collected and stored, and the longer it is held, the greater is the risk of harm to the financial consumer, including through:

- fraudulent use of biometric data (such as fingerprints or iris scans) and of a person's financial and other personal information;[15]
- unanticipated aggregation of a person's data from multiple sources to draw conclusions which may adversely affect that person's future credit or employment prospects;[16] and
- disclosure of personal and sensitive information (such as geolocation, ethnicity, associates or certain purchases) to governments without transparent process and/or to governments which act without regard to the rule of law.[17]

New data practices may also expose consumers to increased risk of inappropriate marketing of products or services, as financial services providers use data analytics to sell more products and services to more consumers more profitably.[18] This will not always benefit consumers. Particularly in markets where irresponsible lending practices are not well regulated, increased access may not equate to liberation or empowerment but to new burdens and oppression.

Finally, new data practices may in fact lead to financial exclusion of vulnerable consumers. Unethical uses of customer data have led to reputation-destroying harassment and humiliation, for instance, where digital lenders in Kenya published details of loan defaulters on Facebook.[19] But even the practices of relatively responsible providers can cause harm.

---

[14] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (WW Norton & Co, 2015) 21–2.

[15] See Medine, above n 12, 1.

[16] Moerel and Prins, above n 5, 22.

[17] See Brookman and Hans, above n 13, 12; Paul de Hert and Gertjan Boulet, "Cloud Computing and Trans-Border Law Enforcement Access to Private Sector Data: Data Challenges to Sovereignty, Privacy and Data Protection" in *Big Data and Privacy: Making Ends Meet* (The Center for Internet Society, Stanford Law School, and Future of Privacy Forum, 2013) 23, 25.

[18] See Yaworsky, Goswami and Shrivastava, above n 4, 6, 14.

[19] Medine, above n 12, 1. See also Ariel Ezrachi and Maurice E Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press, 2016) 81–115.

Data from a person's prior purchasing history, location, habits, income, friends, associates, and social media activity may all be used to classify and "segment" consumers and to "customize" the prices or interest rates a particular consumer is charged.[20] A person could, for example, be charged higher rates based on the creditworthiness of their friends on social media, or the neighborhood in which they live.[21]

Relatively new and untested algorithms applied to data may lead to inaccurate and detrimental conclusions about a person's creditworthiness.[22] Some algorithms may even directly or indirectly discriminate against a customer on the basis of their ethnicity, gender, or religion.[23] These potential harms are not speculative. Many are known to have occurred.[24] All potentially undermine consumer trust in digital financial services and reduce their uptake.[25]

In highlighting these harms, we do not deny the advantages of data-driven innovations, but emphasize the need for balance and caution. Data-driven innovations in the provision of financial services may benefit and include, or discriminate and exclude.

While regulation typically should seek to promote the appropriate balance between consumer access to financial products and privacy, this is often not achieved in many jurisdictions. The

---

[20] See Yaworsky, Goswami and Shrivastava, above n 4, 4, 33; Ramsi A Woodcock, "The Bargaining Robot" (2017) 40 *CPI Antitrust Chronicle*.

[21] See Moerel and Prins, above n 5, 24–5.

[22] Medine, above n 12, 1. Gordon Hull, "Successful Failure: What Foucault Can Teach Us About Privacy Self-Management in a World of Facebook and Big Data" (2015) 17 *Ethics and Information Technology Journal* 89, 91–2, citing the example of a study which concluded that "obesity was associated with credit delinquency".

[23] Ezrachi and Stucke, above n 19, 124–7. See also Deidre K Mulligan and Cynthia Dwork, "It's Not Privacy, and It's Not Fair" in Christina Gagnier, "Regulating the Man Behind the Curtain" in *Big Data and Privacy: Making Ends Meet* (The Center for Internet Society, Stanford Law School, and Future of Privacy Forum, 2013) 94–6.

[24] Consider two examples. Kevin Johnson of Atlanta, Georgia returned from a honeymoon abroad to discover American Express had cut his credit limit severely for using his credit card at places where algorithms indicated other people had a poor repayment history (and despite his sound credit rating): Tracy Alloway, "Big Data: Credit Where Credit's Due," *Financial Times* (5 February 2015) <https://www.ft.com/content/7933792e-a2e6-11e4-9c06-00144feab7de>. CompuCredit, a credit company, reduced credit to cardholders who used their credit card to pay for items such as marriage counseling, psychotherapy and billiards: Dennis D Hirsch, "That's Unfair! Or is it? Big Data, Discrimination and the FTC's Unfairness Authority," (2015) 103 *Kentucky Law Journal* 345, 345.

[25] See Medine, above n 12, 1.

most significant current development in global data protection regulation is the forthcoming EU General Data Protection Regulation (GDPR) due in May 2018.[26] Meanwhile, many developing countries have no general data protection legislation, creating significant uncertainty for providers and consumers. The United Nations Conference on Trade and Development (UNCTAD) reports that, in Africa and Asia, fewer than 40 percent of countries have legislation in place "to secure the protection of data and privacy."[27] Even in countries with data protection laws, there is often little or no enforcement due to limited regulatory resources.[28]

Financial Consumer Data Protection Standards and Agreements in Developing Countries

The general consensus among commentators proposing standards for financial services providers is that providers should only collect, use, and share consumer data with the consumer's informed consent, and should be transparent about how the data will be treated and used.[29]This approach is also reflected in regulations and guidelines for financial services in developing countries.[30]

Many financial services providers in developing countries currently follow an "informed consent" approach to data protection in their published privacy policies and standard form agreements with customers. These are often expressed in broad terms, which permit very

[26] See European Commission, "Exchanging and Protecting Personal Data in a Globalised World" (Brussels, COM (2017) 7, 10 January 2017) 3-4.

[27] UNCTAD, "Data Protection and Privacy Legislation Worldwide," (1 June 2017), <http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx>.

[28] Alex B Makulilo, "The Context of Data Privacy in Africa," in Alex B Makulilo (ed), *African Data Privacy Laws* (Springer International Publishing, 2016).

[29] See, eg, Mobile Financial Services Working Group (MFSWG), Alliance for Financial Inclusion, "Mobile Financial Services: Consumer Protection in Mobile Financial Services" (Guideline Note No 13, March 2014) 15; World Bank, "Good Practices for Financial Consumer Protection" (June 2012) 24; "G20 High-Level Principles on Financial Consumer Protection" (October 2011).

[30] *Kenyan National Payment System Regulation* (2014), reg 42(2). See also Bank of Namibia Guidelines for Issuers of Electronic Money and Other Payment Instruments in Namibia (March 2012) Art 9; Sierra Leone Guidelines for Mobile Money Services, Art 26.1(c); Bank of Uganda, Mobile Money Guidelines (2013) Art 12(c).

wide collection, use and sharing of data (e.g.,, "[w]e may disclose Customer Information to any of our associates and affiliates, without any limitation")[31] in respect of a very wide range of consumer information (e.g., the "type, date, time, location and duration of calls or messages, the numbers you call and how much you spend, and information on your browsing activity when visiting one of our group companies' websites, the location of your mobile phone from time to time, lifestyle information, details of your . . . transactions and any other information collected in relation to your use of our products and services").[32]

These agreements and policies may also state that the provider can amend the terms without contacting the customer,[33] and expressly limit the providers' responsibility to protect customer data or privacy.[34]

Traditional "Informed Consent" Model for Consumer Data Protection

These recommendations and practices based on "informed consent" are consistent with traditional approaches to privacy and data protection in jurisdictions such as the US and EU, which have influenced numerous laws and standards around the world. For instance, the Fair Information Practice Principles (FIPPs), first developed in the United States in the 1970s, are founded on "notice" and "choice."[35] As with consumer protection laws more generally, data protection regulation aims to cure an information asymmetry between providers and consumers by requiring providers to disclose their intended practices to the consumer and ensuring subsequent action is based on the consumer's consent.

---

[31] Kotak Mahindra Bank, India, "Privacy Policy" <http://www.kotak.com/privacy-policy.html> (accessed 14 June 2017).

[32] Vodafone India, "M-Pesa India: Privacy Policy" <https://www.mpesa.in/portal/pdf/privacy_policy.pdf>. See also Ant Financial Services Group: Privacy Policy, "How we collect your personal information", <https://render.alipay.com/p/f/privacy-policy-en/share-information.html>.

[33] See, eg, Ant Financial Services Group: Privacy Policy, "Revisions to this policy", <https://render.alipay.com/p/f/privacy-policy-en/share-information.html>; Privacy Policy of Pan Oceanic Bank <http://pob.com.sb/?page_id=636> (accessed 15 June 2017).

[34] See "bKash Terms and Conditions", cl 6.3 <https://www.bkash.com/terms-and-conditions> (accessed 15 June 2017). See also Ant Financial Services Group: Privacy Policy, "Statement on third party liability" <https://render.alipay.com/p/f/privacy-policy-en/share-information.html>.

[35] See Solove, above n 5, 1882–3; Policy and Research Group, Office of the Privacy Commissioner of Canada, *Consent and Privacy: A Discussion Paper Exploring Potential Enhancements to Consent Under the Personal Information Protection and Electronic Documents Act* (2016) 5.

This has been described as "privacy-control,"[36] or "privacy self-management."[37] The underlying rationale is that the rational consumer enjoys freedom and autonomy in deciding when and how to disclose his or her own information,[38] and the consumer is "paid" for that information according to the bargains they make. On the basis of these bargains, corporations produce more of the privacy options that consumers value. This is the theory.

Weaknesses in the "Informed Consent" Model

In recent decades, there has been increasing criticism of the "informed consent" model as the basis for privacy and data protection laws in developed countries.[39] While the underlying theory has some appeal, the approach cannot be supported in practice for three reasons. First, in all likelihood, the consumer will not actually understand how his or her data will be used or shared: there will be no effective notice.[40] Second, the consumer will not have a real choice as to how or when they will part with their data or at what price. Third, the determination of privacy and liberty in society should not be left to unwitting, incremental individual actions in minor transactions.[41]

Research has shown consumers do not read privacy policies.[42] While this might be shrugged off with a "*caveat emptor*," even anecdotal experience tells us it is no simple matter to read

[36] Office of the Privacy Commissioner of Canada, above n 36, 9. See Makulilo, above n 28, 16–7, for a similar approach in the African context.

[37] Solove, above n 5, 1880.

[38] According to the "autonomy principle", "[p]eople are entitled as a matter of moral right and of practical policy to make decisions that shape their lives. Disclosures equip them to do so": Omri Ben-Shahar and Carl E Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton University Press, 2016) 5; Office of the Privacy Commissioner of Canada, above n 36, 2; Moerel and Prins, above n 5, 7. Cf Solove, above n 5, 1886–7.

[39] See, eg, Moerel and Prins, above n 5, 62–4; Hull, above n 22, 89.

[40] See Hull, above n 22, 91; Christina Gagnier, "Regulating the Man Behind the Curtain" in *Big Data and Privacy: Making Ends Meet* (The Center for Internet Society, Stanford Law School, and Future of Privacy Forum, 2013) 36.

[41] See Hull, above n 22.

[42] Solove, above n 5, 1884–5.

and absorb the myriad privacy policies presented to a consumer. A commonly cited study found that it would take the average person an utterly unrealistic 244 hours per year to read all the privacy policies presented for their approval or acquiescence.[43]

Even if a person did have the time and attention span necessary to read these terms, it is a very difficult matter to interpret and synthesize the information provided, given the broad and frequently opaque language adopted in these policies.[44] Most consumers simply do not and cannot understand the new ways in which their data will be used and shared, or the consequences of these practices: the information asymmetry is not cured by notice.[45]

Data collected for one use under a broadly-stated privacy policy can be used for another purpose, which may be entirely beyond the experience or reasonable expectations of the consumer, and may not even be anticipated by the user at the time of consent. For example, data collected during financial literacy training by a provider might later be used to predict loan default rates.[46] Information collected by a provider may also be provided to a data aggregator who combines it with information from a variety of other service providers, utilities, public registers, mobile service providers, and social media to create an in-depth profile of a person's preferences and likely behavior in subsequent situations.[47]

One cannot therefore make a serious argument that consumers have genuine notice of how their data will be treated. But do they have a choice? In many cases, rival providers present similar terms which are no more reasonable or understandable. Further, these terms are generally offered in standard form on a "take it or leave it" basis.[48] The consumer cannot

---

[43] A M McDonald and L F Cranor, "The Cost of Reading Privacy Policies" (2008) 4 *Journal of Law and Policy for the Information Society* 540. See also Solove, above n 5, 1888–9.

[44] Solove, above n 5, 1886, arguing that "Even if most people were to read privacy policies routinely, people often lack enough expertise to adequately assess the consequences of agreeing to certain present uses or disclosures of their data."; Moerel and Prins, above n 5, 62–3.

[45] Patrick Eggimann and Aurelia Tamo, "Taming the Beast: Big Data and the Role of Law" in *Big Data and Privacy: Making Ends Meet* (The Center for Internet Society, Stanford Law School, and Future of Privacy Forum, 2013) 28; Productivity Commission, above n 9, 67–8.

[46] See Yaworsky, Goswami and Shrivastava, above n 4, 20.

[47] See Solove, above n 5, 1889–90, on "Big Data" mining and data aggregation.

[48] Eggimann and Tamo, above n 46, 28.

bargain according to his or her own preferences or agree to some uses of their data and refuse others.[49] It is also not feasible for consumers to compare privacy policies.[50]

Finally, in making incremental "bargains" regarding their own data, individual consumers are unlikely to appreciate the implications of their individual transactions for the development of privacy norms more broadly.[51] As explained later in this article, privacy is not only an individual right but a "social good," however, consumers suffer from a collective action problem which is likely to prevent them from coordinating their responses for the benefit of society.[52]

All of these criticisms of the consent model also apply in developing countries, often with more force. First, relatively low literacy rates mean that many will not be able to read the terms for themselves and will rely on a summary or opinion from an agent or friend, which may be cursory and/or inaccurate. Second, while we have already noted that in developed countries most consumers will have little concept of the new uses to which their data may be put, consumers in poor countries will almost certainly not appreciate the many new uses for their data, the kinds of third parties with which the data may be shared, or the consequences of this for their futures. Third, the responses of poor financial consumers involved in minor transactions are unlikely to produce best practice results for society as a whole. Our lawmakers and regulators need to respond to the fundamental changes in the power dynamics between providers, consumers, and the holders of big data.

In these circumstances, the consumer's consent to the uses listed in the provider's terms and conditions or privacy policy is utterly illusory. Further, in concentrated markets, consumers may have no choice—or feel they have no choice—but to accept these terms if they wish to have their desired financial service.[53] This absence of choice is likely to be heightened for

[49] See Solove, above n 5, 1885; Hull, above n 22, 93–4.

[50] Hull, above n 22, 94.

[51] See Hull, above n 22, 95.

[52] Ibid.

[53] See Moerel and Prins, above n 5, 27, arguing that the idea that consent is freely given "implies the existence of a valid alternative".

poor consumers being offered access to much-needed formal credit for the first time.

An Alternative Approach to Consumer Data Protection in Developing Countries

Recognizing the Problem is Not Solved by Consumer Consent

The first conclusion from our analysis is that consumer consent cannot be the central solution to the data protection problem for financial services in developing countries. Consent—especially implied or assumed,[54] or buried in the terms of a third-party data collector[55]—should not be the primary justification for the collection, use, sharing or storage of consumer data.

Commentators and standard-setting bodies often propose that the solution to the consumer data protection problem has two limbs: (i) for providers to give more notice, and educate consumers, about their data uses, and (ii) for the rules to insist that the requisite consent be express, rather than assumed.[56] However, simpler disclosures will often fail to reveal the complex uses and consequences of data practices,[57] while providing more information to consumers will not improve their ability to understand what is offered (more so if delivered via their small phone screen), and is more likely to lead to information overload.[58] Furthermore, no amount of extra information will change whether the consumer has any real choice but to accept what is put before them now, or as amended by the provider in future.[59]

---

[54] Consent is "implied" or "assumed" where a provider indicates that consumers will be taken to have agreed to the provider's privacy terms by their silence or inactivity, as opposed to express consent which is provided by some "clear affirmative action", such as ticking a box or selecting a technical setting. See Council of European Union, General Data Protection Regulation (5419/16, 6 April 2016), Recital 32.

[55] Eg, where a financial services provider collects data from the customer's telecommunications provider.

[56] See, eg, Office of the Privacy Commissioner of Canada, above n 36, 10–3; Medine, above n 12, 2, also arguing for "transparency and restraint"; Mazer, Carta and Kaffenberger, above n 7.

[57] Ben-Shahar and Schneider, above n 39, 25.

[58] Ibid 8-13. See also Ian Ayres and Alan Schwartz, "The No-Reading Problem in Consumer Contract Law" (2014) 66 *Stanford Law Review* 545, 550.

[59] See Moerel and Prins, above n 5, 8–9.

To be sure, there are in some markets relatively new proposals for mechanisms which provide more realistic, informed, and "granular" privacy choices to consumers, particularly as the EU GDPR creates pressure for companies both inside and outside the EU to ensure that consent is real, explicit, and informed. However, these solutions rely on the presence of more vigorous competition in the area of privacy protection and more advanced and affordable technology than that which is available in developing countries at this stage. The reality in developing countries is that no real choice is given or made.

Reframing the Discourse: Calling a Spade a Spade

It is important to reframe the discourse among policymakers, and in society generally, about big data analytics and other data-driven innovations. The language used can have a profound impact on policy outcomes. There is a tendency to refer to personal data euphemistically in a way which unjustifiably favors the interests of providers. For example, it is common to refer to a "digital footprint" or "digital exhaust" which consumers "leave behind."[60] But the data is not a waste product discarded in the public domain. It is personal information about our physical location throughout the day; when and how much we paid for phone credit; who we chose to connect with on private social media and what we said to them; who we called or texted and when; what we purchased, from whom and for what price. Corporations actively track our activities in these domains and store the data produced by the surveillance of our seemingly private activities. To the extent that this data is used for other purposes or shared with other entities it is because it has not been protected.

Care should also be taken in determining whether consumers actually care about their privacy.[61] When consumers are asked whether they would sacrifice some of their privacy in return for a larger or quicker loan, they may well answer yes. But what does this signify? Such assent may spring from: (i) the "present bias" of consumers, who may prefer the

[60] See, eg, Costa, Deb and Kubzansky, above n 3, 49; Laurence Chandy et al, "Disrupting Development With Digital Technologies: Brookings Blum Roundtable 2015 Post-Conference Report" (2015) 30; Jessie Hempel, "Banks Are Now Handing Out Loans to People They'd Normally Shun" (Wired, 1 January 2015) <https://www.wired.com/2015/01/banks-handing-loans-people-normally-shun/>.

[61] See, eg, Mazer, Carta and Kaffenberger, above n 7, reporting that "many consumers noted that the need for a loan would supersede concerns for privacy".

immediate pay-off of having more cash than the longer term pay-off of preserving their privacy; [62] (ii) the vulnerable consumer over-paying to meet their financial needs unaware of other options; or (iii) the consumer assuming their privacy cannot be preserved if they are to have this loan or that they have no bargaining power to get a loan on better terms; or (iv) the consumer's simple ignorance of the potential harms and consequences which may flow from incrementally surrendering their privacy.

Recognizing Data Protection Need Not Be a Zero-Sum Game

Current enthusiasm about the potential of "big data" analytics and "data mining" creates the temptation to store and analyze and re-analyze very broad data sets in the quest to discover things of value.[63] At the same time, the more data is collected and the longer it is retained, the greater are the risks to the data subjects—as well as to the provider storing the data, who may be exposed to legal liability and/or reputational harm in the event of data breaches.

However, data protection and data-driven innovation need not be mutually exclusive. Cavoukian, for example, has advocated "Privacy by Design" principles as a useful model "to reconcile the need for robust data protection and an organization's desire to unlock the potential of data-driven innovation."[64] The aim of Privacy by Design is for the protection of consumer data and privacy to be designed into any new product, service or system from the beginning, so that privacy and security are "baked in" to the technical design, without sacrificing functionality.[65] Security is maintained throughout the lifecycle of the data process and data is securely destroyed at the end of that process. The interests of individuals are central in the design of the service, including by the provision of strong privacy defaults.

---

[62] See Frederik Zuiderveen Borgesius, "Consent to Behavioural Targeting in European Law: What Are the Policy Implications of Insights from Behavioural Economics?" (Amsterdam Law School Legal Studies Research Paper No 2013-43, 2013) 40.

[63] "Data mining" refers to the "use of dynamic data processing techniques to find hidden patterns and trends in large amounts of … data" as an essential step in the process of "knowledge discovery in databases": Colonna, above n 11, 19–20; Ibid.; Yaworsky, Goswami and Shrivastava, above n 4.

[64] See Ann Cavoukian, David Stewart and Beth Dewitt, "Using Privacy by Design to Achieve Big Data Innovation Without Compromising Privacy" (Deloitte, 10 June 2014) 15.

[65] Moerel and Prins, above n 5, 10 fn 40.

While providers in developing countries may not be able to justify the same expenditure on "privacy enhancing technologies" (PETs) as their counterparts in developed markets at this stage,[66] they can still provide similar signals to consumers by highlighting their diligent and restrained approach to data protection (assuming this is their practice) and building data protection into system designs. The growth in PETs, especially in response to the forthcoming implementation of the EU GDPR, is likely to improve opportunities for providers to use data in ways that create benefits for consumers and society, while minimizing risks from such uses. This development deserves the support of international standard setting bodies, policymakers and regulators.

Questioning the "Privacy Self-Management" Paradigm

The current debate about data protection in developing countries is taking place almost exclusively within the conventional informational privacy paradigm of "privacy self-management,"[67] or "informational self-determination."[68] Developing country policymakers would do well to challenge whether this dominant paradigm is appropriate in their local contexts, particularly having regard to the vulnerabilities of their populations, and the importance of the values served by data protection

As noted earlier, according to the "privacy self-management" paradigm, informational privacy is viewed as an individual's "control" over their personal information.[69] While this is the prevailing paradigm, it has been challenged by numerous commentators who argue that privacy should actually be seen as a "social good" which creates benefits for the community as a whole—and may be sacrificed to the detriment of the community as a whole.[70] Constant

[66] Liz Coll, "Personal Data Empowerment: Time for a Fairer Data Deal?" (Citizens Advice Bureau, 2015) 43, 50, citing examples "personal data empowerment tools and services" offered by Microsoft, Apple, Barclay's Bank, Acxiom, Intel, Telefonica and BT. See also UNCTAD, above n 29, 101.

[67] See Solove, above n 5.

[68] See Antoinette Rouvroy and Yves Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy" in S Gutwirth et al (eds) *Reinventing Data Protection?* (Springer, 2009).

[69] See Hull, above n 22; Office of the Privacy Commissioner of Canada, above n 36, 2.

[70] See, eg, Debbie VS Kasper, "Privacy as a Social Good" (2007) 28 *Social Thought and Research* 165.

surveillance is known to reduce the ability of humans to engage in independent, creative and innovative thought,[71] and pervasive segmentation, social sorting, and differential treatment of communities through the application of data analytics may threaten democratic values.[72] In the context of financial services, big data analytics could also work against important social benefits—such as risk pooling via insurance—as consumers are declined coverage or charged much higher premiums on the basis of information gleaned about their personal circumstances and risk factors.[73]

Research shows that consumers do care about the privacy of their information and that this is important to the trust consumers place in providers.[74] To date, a focus on privacy self-management, and the provision of vague and broadly-worded "agreements" concerning data protection, has encouraged providers to focus on the *procedural* protection of supposedly obtaining consumers' consent to data practices. Policymakers should not restrict the debate to these matters but should give consideration to the need for legislation which provides *substantive* protection from harms caused by inappropriate collection, use, sharing and storage of information,[75] having regard to the multiple social values served by consumer data protection.

In this regard, the prevalence of the "privacy self-management" framework is also relevant in understanding perceptions about the importance of privacy in developing countries. It has been suggested that privacy in general may be less important in African societies, in which the interests of the individual are subordinate to the interests of the broader society and the concept of "self" does not accord with Western norms.[76] Those who view data protection as a

---

[71] See Schneier, above n 14, 112-6, 147 ff; Brookman and Hans, above n 13, 12–3.

[72] See Deidre K Mulligan and Cynthia Dwork, "It's Not Privacy, and It's Not Fair" in Christina Gagnier, "Regulating the Man Behind the Curtain" in *Big Data and Privacy: Making Ends Meet* (The Center for Internet Society, Stanford Law School, and Future of Privacy Forum, 2013) 94–6.

[73] See discussion in the text at nn 20–3.

[74] See, eg, Katharine McKee, Michelle Kaffenberger and Jamie M Zimmerman, "Doing Digital Finance Right: The Case for Stronger Mitigation of Customer Risks" (CGAP Focus Note No 103, June 2015) 14–6.

[75] See Moerel and Prins, above n 5, 8–9, referring to the "mechanical proceduralism, whereby data controllers notify individuals and ask for their consent in a mechanical manner, without offering effective data protection in practice". See also Solove, above n 5, 1902–3.

[76] See Makulilo, above n 28, 15–7.

"Western" concern may be making the unspoken assumption that informational privacy is necessarily defined in terms of an individual's ability to control their personal information.

However, the debate about data protection in developing countries should not be constrained to the dominant informational privacy paradigm. It is necessary to understand local concepts of privacy,[77] as well as other values which are served by data protection in the local context, including dignity, identity, exclusion from publicity, and freedom from oppression,[78] which may be given a high priority in developing countries.

Conclusion

The promise of new data analytics and other data-driven innovations for the advancement of financial inclusion is real. These innovations can promote convenient and affordable credit and other services to consumers who would otherwise be excluded from formal financial services. At the same time, real and significant harms may flow from the increased collection, use, sharing and storage of ballooning quantities of consumer data. We have proposed an alternative approach to the policy debate on financial consumer data protection which:

- Acknowledges that, given the clear flaws in the "informed consent" approach, consumer consent should not be the primary justification for data practices;
- Reframes the discourse to avoid misleading euphemisms and poorly grounded assumptions about why financial consumers consent, or appear to consent, to the disclosure of their personal data;
- Recognizes data protection and benefits from data-driven innovations need not be mutually exclusive, but that data protection can be built into the design of systems; and
- Questions the applicability of the dominant "privacy self-management" paradigm in the context of financial consumer data protection in developing countries, taking into account multiple social values served by data protection.

[77] Ibid 16–7.

[78] See European Data Protection Supervisor, "Opinion 4/2015: Towards a New Digital Ethics – Data, Dignity and Technology" (2015), on the relevance of data protection for human dignity.

In our view, the benefits of taking such a course will far eclipse the cost or effort involved. In particular, in developing countries where many financial products are being crafted anew to meet local needs, the incorporation of privacy-by-design measures into the architecture of the products themselves and the systems that operate and provide oversight of them, can be relatively inexpensive and simple.