Making Consent Meaningful Again: A Review of the Online 'Consent' Model and Alternative Approaches

Jialiang Zhang

Jialiang Zhang is a cyber security and data privacy professional who has worked in consulting and in-house roles for over a decade. After an LLM in Technology Law at Queen's University Belfast, he is reading for an MAcc degree at Downing College, Cambridge. Benefiting from his interdisciplinary background, Jialiang is experienced in realising regulatory requirements in IT architecture design and is interested in quantifying cyber risks.

Introduction

From atoms to bits, digital convergence has made science fictions come true.[1] Web, mobile applications, smart homes, and increasingly more digital products have changed the way people interact with the world time and again. However, no matter how much technologies evolve, the 'agree' or 'consent' button is following like a shadow. From the start of this century to date, the 'notice-and-consent' model, as one of the most fundamental methods to protect the users' privacy, still dominates the virtual world.[2]

There are conflicting attitudes towards this long-established 'consent' model. Criticisms towards the consent model are prevalent, while the legislators seem to ignore them.[3] Academics claim the people today can no longer provide a meaningful form of consent,[4] some even say that the current model offers no choice at all.[5] However, this consent model is still at the heart of many data-protection legislations today worldwide,[6] such as the California Consumer Privacy Act 2018 and China's Personal Information Protection Law 2021.

This essay assesses the status quo of the consent model through the lens of this conflict. It aims to answer two questions: whether the consent model is still a reliable method for privacy protection today? If not, what can be done to bring it back on track? Section II of the essay analyses the two sides of the conflict. Section III then offers suggestions as to how to address problems of the current model summarised in Section II.

I. The Two Sides of the Coin

This section unfolds in two parts. The first part discusses the criticisms of the consent model which are primarily based on the definition of 'valid consent'. The definition, provided by Kim, includes three essential elements: *intentional manifestation of consent*, *knowledge* and *volition/voluntariness.*[7] The second part then considers the causes why, despite the criticisms, legislators still uphold the consent model enthusiastically.

Intentional manifestation of consent

'Intentional manifestation of consent' means the 'reason or purpose for the manifestation of consent is to communicate consent to the act'.[8] However, in the context of online consent, the constantly appearing cookie pop-up windows and agree buttons result in an end-user 'consent fatigue'.[9] This consent fatigue, with the long-winded privacy notices, undermines the original purpose of consent; it only makes people more likely to ignore it.[10] Thus, can clicking the agree button be understood as a well-informed privacy trade-off?

1 Andrew Murray, *Information Technology Law: The Law and Society* (4th edn, Oxford University Press 2019).
2 Alessandro Mantelero, 'The Future of Consumer Data Protection in the E.U. Re-thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics' (2014) 30 Computer Law and Security Review 643.
3 Anne Josephine Flanagan, Jen King and Sheila Warren, 'Redesigning Data Privacy: Reimagining Notice and Consent for Human Technology Interaction' (*World Economic Forum*, 2020) <https://www.weforum.org/reports/redesigning-data-privacy-reimagining-notice-consent-for-humantechnology-interaction> accessed 29 November 2020.
4 ibid.
5 Lord Sales, 'Algorithms, Artificial Intelligence and the Law' (2020) 25 Judicial Review 46.
6 Flanagan, King and Warren (n 3).
7 Nancy S. Kim, *Consentability: Consent and Its Limits* (Cambridge University Press 2019) 10.
8 ibid.
9 Daniel Susser, 'Notice after Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't' (2019) 9 Journal of Information Policy 37.
10 Flanagan, King and Warren (n 3).

Knowledge

Knowledge to consent means the person must understand what they are consenting to.[11] To conform to this principle, it is necessary that the information is clear and the person has the ability to understand.[12] Nevertheless, the majority of privacy policies today are filled with legal jargon deliberated word by word. They are not something that the average end-user could figure out.[13] More ironically, thanks to the rising complexity of the algorithm, the drafter of the statement or developer of the product even sometimes does not understand the real impacts behind the data processing activities they engaged.[14] The developers in commercial companies may be clear about the input and expected output of those algorithms, but they probably do not know how things are worked inside of the algorithm and what kinds of implications the algorithm may bring. Without accessible information, it is impossible that the users can make meaningful consent.

Volition/Voluntariness

Digital services are tempting people to trade off their privacy for *de facto* benefits. Nowadays, it would sound like nonsense if an email service charged a fee or Facebook and Twitter sent an invoice. It becomes so natural to have a pizza delivered to the door or have a ride ready in minutes by just clicking on a smartphone. These benefits make the consent seem to have *voluntariness*.

Nevertheless, is that a real free choice? Voluntariness requires consideration of the cost of rejection. The wide adoption of the 'take-it-or-leave-it' model results in an either/or situation.[15] Rejecting the contemporary digital service means not merely refusing the convenience it brings but isolating oneself from the digital community and one's generation. Moreover, taking a smart city as an example, refusing to give consent means removing oneself from the entire society.[16] The pressure and coercion[17] of exclusivity only leaves people a 'free' Hobson's choice.[18]

The above criticisms suggest an interim conclusion that the online consent model today fails to achieve all essential elements that could make consent meaningful; in other words, in practice, there is no valid consent at all. However, the reasons why legislators around the world still advocate the consent model are worth considering. The intuitive reason is that governments themselves also benefit from the consent model to realise projects such as smart cities and state surveillance. However, Susser's work effectively summarises the deeper reasons: 'it's cheap, encourages innovation, and *appeals to individual choice*'.[19] It means that such a 'free-market' approach[20] could help stimulate the economy at a minimal cost and simultaneously create an illusion of respect to individual choices.[21] This is the allure of the consent model, which sounds fair as an acceptable privacy trade-off appearing in the age of digital technology explosion.[22]

Is the consent model still a reliable way to protect individuals' privacy today? Yes and no. It is worth pointing out that the core rationale of the consent model still stands; both advocates and critics of the current model acknowledge the free-market approach that the consent model brings.[23] Even looking back at the criticisms, almost no one is attacking the rationale of the notice-and-consent model; the critics always go after the actual practice. The critics argue that it is impossible to make meaningful consent under information and power asymmetry.[24]

II. Recommendation for a Way Out

Given that the underlying rationale of the current consent model should be upheld, it is necessary to address the problems arising from the actual practice. I propose a solution which consists of three different levels of actions that would fulfil all three essential elements of consent in practice.

Informational Norms

Ben-Shahar and Schneider argue the simplest way to solve the *knowledge* issue is to give people more information.[25] This approach does not aim to train people as legal or computer experts, but to familiarise people with the context.[26] Sloan and Warner's solution, called the 'informational norms', is an efficient way to achieve this. This proposal advocates establishing norms to govern data processing behaviours, so that people would have a reasonable expectation about what parts of their privacy they would trade off for the services, and in what contexts this trade-off scenario is taking place.[27] They used the analogy that it is very natural to understand 'why your pharmacist may inquire about the drugs you are taking, but not about whether you are happy in your marriage' to illustrate the importance of specific contextual knowledge.[28] Through the informational norms, an individual is equipped with the essential *contextual* knowledge to make such decisions regarding the use of their personal data.

I suggest that the data protection authority coordinate with sector associations and non-profit organisations to establish such norms. They should then continue to run awareness campaigns to ensure that the users are well informed and companies to follow the new norms.

Raising the Bar for Consent

In practice, more and more companies are inclined to implement the consent model even if another lawful basis is available to choose. Susser's study points out an important observation that the notice-and-consent model may be adopted as just 'notice-and-waiver'.[29]

11 Kim (n 7).
12 ibid.
13 Helen Nissenbaum, 'A Contextual Approach to Privacy Online' (2011) 140 Daedalus 32.
14 Susser (n 9).
15 Robert H. Sloan and Richard Warner, 'Beyond Notice and Choice: Privacy, Norms, and Consent' (2013) SSRN Electronic Journal <DOI:10.2139/ssrn.2239099> accessed 28 November 2020.
16 Jennifer Cobbe and John Morison, 'Understanding the Smart City: Framing the Challenges for Law and Good Governance' in E Slautsky (ed), *The Conclusions of the Chaire Mutations de l'Action Publique et du Droit Public* (Sciences Po 2018).
17 Flanagan, King and Warren (n 3).
18 Sloan and Warner (n 15).
19 Susser (n 9), my emphasis.
20 Sloan and Warner (n 15).
21 Flanagan, King and Warren (n 3).
22 Sloan and Warner (n 15).
23 Susser (n 9).
24 ibid.
25 Omri Ben-Shahar and Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton University Press 2014).
26 ibid.
27 ibid.
28 ibid.
29 Susser (n 9).

This enables the companies to shield themselves from liability but reserve the inexhaustible potential of the data.[30]A report released by the President's Council of Advisors on Science and Technology of the Obama government states that 'notice and consent fundamentally places the burden of privacy protection on the individual – exactly the opposite of what is usually meant by a "right"'.[31] Furthermore, it leads to consent fatigue. Thus, the second action in the portfolio is to raise the bar for consent usage.

First of all, there should be a clear boycott against the current abuse of consent. For example, if the purpose is as simple as delivering a pizza order, the lawful basis shall simply be 'contract' rather than asking for 'consent'.[32] Second, with establishing of the informational norms, a clearer sector-based legitimate interest justification could be formed. For instance, why not have personalised advertisements to be legitimate interests for those free services (e.g. Gmail)? If one worries about the level of personal data used in the advertisement, this should be addressed by advertising regulations such as the Committee of Advertising Practice code. Such efforts can restore the *manifestation of consent*: this significantly reduces the times of consent scenario the people face, and makes the people aware that if consent is required, it must be something they should pay special attention to.

Meanwhile, these efforts also offer higher certainty for the companies to engage lawful basis of data processing activities other than the consent model, and the companies' legitimate interests can be protected by the sector norms. Therefore, there is no more excuse for the take-it-or-leave-it model to continue to be adopted in so many data processing scenarios.

Fundamental Safety Guard

The last action is a fundamental safety guard. Zuboff,[33] Yeung[34] and others[35] warn people against other risks of privacy infringement embedded in the current consent model, such as fake news, echo chambers and data breaches. Thus, two related actions may be implemented to help form a fundamental safety guard. First, it should be similar to food safety regulations; there should be 'hard boundaries' for data processing activities that protect people from obvious harms.[36] One possible way would be to ban data processing activities, such as targeted political campaigns, which could cause obvious harms to public safety. Setting up a specific standard may be another choice. For example, China's Cybersecurity Law requires all systems which process personal data above a certain amount to pass a mandatory third-party cybersecurity audit.[37] Second, for those potentially high-risk activities, such as processing special categories of personal data, even with explicit consent, the system should log all activities associated and provide justifications of the output. These records would make retrospective/future investigations possible and deter unnecessary activities. Even though the scope of logging function is limited in the Section 62 of the UK Data Protection Act 2018,[38] this function was an example in which such a requirement to log can be implemented. The ultimate goal for the fundamental safety guard is to further shift the privacy protection burden back to companies and governments.

However, there might be one last flaw in the foregoing three-levels solution, which is that it seems only applicable to private sectors. Indeed, it would be hard for any actions in the solution to restrict the power of the state. In that case, I suggest introducing a data trust[39] to deal with state-level data processing. An independent data trust which represents the collective citizens, authorised by the people, could be an efficient channel to fill the gap in the information and power asymmetry between an individual citizen and the state.[40] The pilot projects conducted by the Open Data Institute are excellent examples.[41]

Conclusion

It is worth emphasising that the core rationale of the consent model is still valid. The issue today is that the people's knowledge can no longer catch up with the explosive growth in technology. Meanwhile, the organisations and governments are circumventing their due responsibilities by abusing the consent model.

The solution proposed in Section III restores the validity of the three essential consent elements. For the private sector, the core strategy is to reduce the unnecessary use of consent by diversifying its legal instruments. The informational norms establish the *knowledge* of the public and facilitate the public's understanding of different sectors' legal interests. *Raising the bar of consent* mitigates fatigue to reinforce the *intentional manifestation of consent.* These two actions are more effective alternatives to the take-it-or-leave-it model, which makes real *voluntariness* possible. Moreover, this combination could also help address the new emerging challenges such as the Internet-of-Things, which does not offer the chance for privacy statements to be presented in advance. Finally, the fundamental safety guard offers an extra protection to reassure the public that they are protected from obvious harms, which plays a crucial role in re-establishing public trust and confidence in the data protection legislation. For the public sector, an independent data trust could draw the power asymmetries back into balance.

The solution to the dilemma is not a full abandonment of the consent model; this would not help. Instead, the real way out is to fully realise the advantages of the consent model through concrete and realistic implementation pathways and thereby make consent meaningful again.

30 ibid.

31 PCAST, *Report to The President – Big Data and Privacy: A Technological Perspective* (PCAST 2014) 38.

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

33 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).

34 Karen Yeung, 'Five Fears About Mass Predictive Personalisation in an Age of Surveillance Capitalism' (2018) SSRN Electronic Journal <https://ssrn.com/abstract=3266800> accessed 28 November 2020.

35 See e.g. Kathleen M. Kuehn and Leon A. Salter, 'Assessing Digital Threats to Democracy, and Workable Solutions' (2020) 14 International Journal of Communication 2589.

36 Susser (n 9).

37 China Cybersecurity Law 2017, art 21.

38 Data Protection Act 2018, s 62(1).

39 Bianca Wylie and Sean McDonald, 'What Is a Data Trust?' (*Centre for International Governance Innovation,* 2018) <https://www.cigionline.org/articles/what-data-trust> accessed 28 November 2020.

40 Anouk Ruhaak, 'Data Trusts: What Are They and How Do They Work?' (*RSA* 2020) <https://www.thersa.org/blog/2020/06/data-trusts-protection?gclid=Cj0KCQiAh4j-BRCsARIsAGeV12CL1qnJPUAxOHc7ROKhlid5xQHrgKbQSAtS6XdINfwadAkjAeScWf4aAuz0EALw_wcB> accessed 23 November 2020.

41 The ODI, *Data trusts: Lessons from Three Pilots*, (ODI 2019).