Law and Technology Centre
The University of Hong Kong

Privacy & Innovation
In Pursuit of Right Incentives
9 June 2015

The Limits of Notice and Choice

Fred H. Cate

Distinguished Professor and
C. Ben Dutton Professor of Law
Director, Center for Information Privacy and Security
Indiana University Maurer School of Law

The Prominence of Notice and Choice

- The Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted in 1980 and reaffirmed in 2013, require that personal information be collected, "where appropriate, with the knowledge or **consent** of the data subject," and prohibit the reuse of personal information except: "(a) with the **consent** of the data subject; or (b) by the authority of law." (emphasis added)
- In 1998, the U.S. Federal Trade Commission (FTC), after reviewing "fair information practice codes", reported to Congress that "[t]he most fundamental principle is **notice**" and "[t]he second widely-accepted core principle of fair information practice is consumer **choice** or **consent** . . . . [over] how any personal information collected from them may be used." (emphasis added)
- The Obama Administration's proposed 2012 Consumer Privacy Bill of Rights includes as its first principle: "Consumers have a right to exercise **control** over what personal data companies collect from them and how they use it." (emphasis added)

- The Obama Administration's 2015 discussion draft of a Consumer Privacy Bill of Rights Act requires "accurate, clear, timely, and conspicuous **notice** about the covered entity's privacy and security practices" and that "[e]ach covered entity shall provide individuals with reasonable means to **control** the processing of personal data about them in proportion to the privacy risk to the individual and consistent with context." (emphasis added)
- The Asia-Pacific Economic Cooperation (APEC) Privacy Framework, adopted in 2004, provides: "Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise **choice** in relation to the collection, use and disclosure of their personal information." (emphasis added)
- In Canada, Philippa Lawson and Mary O'Donoghue have written: "[t]he requirement for **consent** to the collection, use, and disclosure of personal information is a cornerstone of all three [of Canada's] common-law regimes." (emphasis added)

- Article 7 of the European Union's Data Protection Directive provides seven conditions under which personal data may be processed. The first is "the data subject has unambiguously given his **consent**." Article 8 restricts the processing of sensitive data, but then provides that the restriction shall not apply where "the data subject has given his explicit **consent** to the processing of those data." Article 26 identifies six exceptions to the provision prohibiting the export of personal data to non-European countries lacking "adequate" data protection. The first is that "the data subject has given his **consent** unambiguously to the proposed transfer." (emphasis added)
- The pending draft EU General Data Protection Regulation refers to **"consent"** more than 100 times. Consent is the first basis listed for the lawful processing of data (art. 6), a condition for the processing of personal data concerning a child under 13 (art. 8), a basis for processing sensitive data (art. 9), an exception to the restriction on profiling (art. 20), an exception to the prohibition on exporting personal data to countries lacking adequate data protection (art. 44), and an exception to the restriction on the reuse of personal data concerning health (art. 81).

The Critique of Notice and Choice

- Growing consensus that data protection based on notice and choice is both impractical and undesirable.
- Especially true in a world of ubiquitous surveillance, big data, and growing reliance on interconnected sensors (i.e., the "Internet of Things").
- 2014 report by the President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective*, described the "framework of notice and consent" as "**unworkable as a useful foundation for policy**." The report stressed that "only in some **fantasy world** do users actually read these notices and understand their implications before clicking to indicate their consent." (emphasis added)

Seven Challenges Presented by Notice and Choice

1. Complexity
   - It is surprising that many notices are complex given that the laws and business practices they describe are often complex as well.
   - Moreover, notices often read like contracts because regulators have chosen to enforce them like contracts.
   - In March 2012 the UK consumer watchdog Which? reported that when PayPal's privacy notice is added to its other terms of use disclosed to consumers, the total word count is 36,275 words, longer than *Hamlet* (at 30,066 words), and iTunes' comes to 19,972 words, longer than *Macbeth* (at 18,110 words).
   - Experiments with ways of making notices more accessible, including shortened notices, layered notices, standardized notices, and machine-readable notices, have tended to fail in practice, in large part because they ignore the fundamental complexity of the myriad uses of data that notices are trying to describe and the legal liability that can result from inadequate or inaccurate descriptions.

- Especially true in the context of big data, which, in the words of Professor Paul Ohm, ”thrives on surprising correlations and produces inferences and predictions that defy human understanding. . . . **How can you provide notice about the unpredictable and unexplainable**?” (emphasis added)

2. Inaccessibility/Impracticality

- How do you provide opportunities for notice and choice in the case of sensors, such as those in the more than 6.8 billion handheld phones worldwide, or found in automobiles, public transportation, public highways, office buildings, consumer appliances, and even toys around the world?
- How do you provide opportunities for notice and choice concerning the inferences, probabilities, predictions, and other data are created by government and industry at a rapid pace and used to classify or qualify individuals for hundreds of reasons ranging from marketing to tax audits?
- FTC Chairman Jon Leibowitz commented In 2009: “We all agree that consumers don’t read privacy policies.”

3. The Illusion of Choice
   - When choice is offered for a service or product that cannot be provided without personal information.
   - When consent to make other uses of data is required to obtain a product or service.
   - When notice is so broad or vague or complex as to make choice meaningless.
   - When notices are not read.

4. Inadequate Privacy Protection

- Scrolling through privacy policies and clicking “I agree” rarely provides meaningful privacy protection.
- By equating the two, we have actually tended to weaken privacy protections by making them waivable through consent.
- Notice and consent do not protect us from our own bad, ignorant, unintentional, or unavoidable choices.
- As the Institute of Medicine Committee on Health Research and the Privacy of Health Information wrote in 2009: “consent (authorization) itself cannot achieve the separate aim of privacy protection.”
- The more regulators and legislators focus on notice and consent as a basis for privacy protection, the less they focus on more meaningful and effective protections.

5. False Dichotomy

- By focusing on data linked to a specific individual, to whom notice can/must be provided and from whom consent can/must be obtained, we run the risk of ignoring the threats post by less clearly personally identifiable information.
- Big data facilitates making even non-PII identifiable.
- Identifying people by IP address, browser choice and font size, widely reported characteristics (such as 5-digit ZIP Code, gender, and date of birth), or by matching deidentified data with preferences or characteristics.
- In a world of big data, Cynthia Dwork writes, "'De-identified data' isn't."

6. Burden on Individuals

- One 2008 study calculated that to read the privacy policies of just the most popular websites would take an individual 244 hours—or more than 30 full working days—each year.
- While presented as a right, the emphasis on notice and consent in reality often ends up creating a duty on individuals to make choices they are often ill-prepared to make and to accept the consequences of those choices.
- Choice too often shifts responsibility and liability for data stewardship from the data user to the individual, even though we know most choices are made reflexively, without thought, or by default.
- “Notice Fatigue.”

7. Burden on Society

- Choice can actually interfere with activities of great value to individuals or society more broadly.
- This is true of law enforcement, press coverage of public figures and events, medical research, and of the many valuable uses of personal information where the benefit is derived from the fact that the consumer has not had control over the information.
- Consider information about individuals' creditworthiness: its value derives from the fact that the information is obtained routinely, over time, from sources other than the consumer. Allowing the consumer to block use of unfavorable information would make the credit report useless. In the words of former FTC Chairman Timothy Muris, the credit reporting system "works because, without anybody's consent, very sensitive information about a person's credit history is given to the credit reporting agencies. If consent were required, and consumers could decide—on a creditor-by-creditor basis—whether they wanted their information reported, the system would collapse."

- Especially true in the context of big data, where many of the benefits depend on being able to use data for uses that did not even exist when they were collected or created. And many depend on having complete data sets. For example, in the context of health research, refusal rates as low as 3.2% have been clearly shown to introduce selection bias.

The Big Data Context Exacerbates These Challenges

- Greater volume and velocity of data collection and use.
- More data observed by sensors rather than collected from individuals (e.g., “Internet of Things”).
- More data inferred or calculated.
- Greater data aggregation (or federation) and use by third parties.
- Data reused for unexpected purposes or to identify correlations suggested by the data themselves.

Doing Better

1. Focus less on individual consent and more on placing responsibility for data stewardship, and liability for reasonably foreseeable harms, data users
2. Employ a more systemic and well-developed use of risk management
    - In 2013 the OECD Council of Ministers revised the *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* to "implement a risk-based approach." In the accompanying Explanatory Memorandum, the drafters noted the "importance of risk assessment in the development of policies and safeguards to protect privacy."
3. Place greater focus on *uses* of big data as opposed to the mere collection or retention of data or the purposes for which data were originally collected
    - As Professor Susan Landau wrote in 2015 in *Science*: data protection laws have attempted to protect privacy "through notice and consent. But for reasons of complexity (too many tiny collections, too many repurposings) those are no longer effective. . . . [T]he value of big data means we must directly control use rather than using notice and consent as proxies."

4. Develop a broad framework of cognizable harms identified through a transparent, inclusive process including regulators, industry, and individuals
    - Include **tangible injuries** (e.g., financial loss, physical threat or injury, unlawful discrimination, identity theft, loss of confidentiality, and other significant economic or social disadvantage), and **intangible harms** (e.g., damage to reputation or goodwill, or excessive intrusion into private life) and potentially broader societal harms (such as contravention of national and multinational human rights instruments).
5. Pay more attention to transparency and redress
6. Reserve notice and choice for where meaningful and effective

Thank you.

fred@fredhcate.org

Sources

- Article 29 Data Protection Working Party and the Working Party on Police and Justice, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data* (02356/09/EN, WP 168) 17 (Dec. 1, 2009).
- Asia-Pacific Economic Cooperation, *APEC Privacy Framework*, 2004/AMM/014rev1 (2005), at 17.
- David Casarett, *et al*., "Bioethical Issues in Pharmacoepidemiologic Research," in R.L. Strom. ed., *Pharmacoepidemiology* (4th ed., John Wiley & Sons. 2005), at 594; *Beyond the HIPAA Privacy Rule*, *supra* at 210-214.
- Fred H. Cate & Viktor Mayer-Schönberger, *Data Use and Impact Global Workshop*, Center for Applied Cybersecurity Research (2013).
- Fred H. Cate, Peter Cullen & Viktor Mayer-Schönberger, *Data Protection Principles for the 21st Century*, Oxford Internet Institute (2013).
- Fred H. Cate & Viktor Mayer-Schönberger, *Notice and Consent in a World of Big Data*, Microsoft Corporation (2012).
- Fred H. Cate & Viktor Mayer-Schönberger, "Notice and Consent in a World of Big Data," *International Data Privacy Law*, vol. 3, no. 2 at 67 (2013).
- Fred H. Cate, Peter Cullen & Viktor Mayer-Schönberger, *Data Protection Principles for the 21st Century World*, Microsoft Corporation (2014).
- Centre for Information Policy Leadership at Hunton & Williams LLP, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice* (2014).
- Centre for Information Policy Leadership at Hunton & Williams LLP, The Role of Risk Management in Data Protection (2014).

- *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (Eur. O.J. 95/L281), Preamble, arts. 7(a), 8(2)(a), 26(1)(a).
- Cynthia Dwork, "Differential Privacy: A Cryptographic Approach to Private Data Analysis," in Julia Lane, Victoria Stodden, Stefan Bender, Helen Nissenbaum, eds., *Privacy, Big Data, and the Public Good* 297 (Cambridge 2014).
- Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (2014).
- Institute of Medicine, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research* 250 (National Academies Press 2009).
- Susan Landau, "Control use of data to protect privacy," *Science* 347:6221, Jan. 30, 2015, at 504.
- Philippa Lawson & Mary O'Donoghue, "Approaches to Consent in Canadian Data Protection Law," in Ian Kerr, Valerie Steeves & Carole Lucock, eds., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* 23 (Oxford University Press 2009).
- Jon Leibowitz, Introductory Remarks, FTC Privacy Roundtable (Dec. 7, 2009), at 3.
- Viktor Mayer-Schönberger & Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (2013).
- Alecia M. McDonald & Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society* (2008).
- Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond*, Privacy 2001 Conference, Oct. 4, 2001.
- OECD, *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL, as amended by C92013)79 (2013), 12.

- OECD, *Supplementary Explanatory Memorandum to the Revised Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (2013), 30.
- Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701 (2010).
- Paul Ohm, "Changing the Rules: General Principles for Data Use and Analysis," in Julia Lane, Victoria Stodden, Stefan Bender, Helen Nissenbaum, eds., *Privacy, Big Data, and the Public Good* 100 (Cambridge 2014).
- Rich Parris, "Online T&Cs longer than Shakespeare plays – who reads them?" Which? Conversation, Mar. 23, 2012.
- President's Council of Advisors on Science and Technology, *Big Data and Privacy: A Technological Perspective* (2014).
- Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Unofficial Consolidated Draft Text, Oct. 22, 2013.
- Latanya Sweeney, Simple Demographics Often Identify People Uniquely, Carnegie Mellon University, Data Privacy Working Paper 3 (2000).
- U.S. Federal Trade Commission, *Privacy Online: A Report to Congress* 7 (1998).
- U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report (2010).
- U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, FTC Report (2012).

- The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation* 47 (2012).
- The White House, Administration Discussion Draft: Consumer Privacy Bill of Rights Act §§ 101, 102 (2015).