Navigating the Incoherence of Big Data Reform Proposals

Nicolas Terry

Introduction
The health care industry will be a large customer of big data while predictive analytics already underlie important health care and public health initiatives. Yet big data are not benign. For example, data brokers, the businesses that buy, process, and sell “big data” are performing an end-run around health data protection by creating data “proxies” outside of HIPAA-protected space.¹ From 2012-14 various branches of the federal government published five major reports on privacy. All five were in favor of increased regulation of data brokers. However, their recommendations for legislative or regulatory intervention were quite diverse. This essay describes the various proposals and offers a critical synthesis.

Five Reports: (Too) Many Suggestions
The rhetoric of the first report, the White House’s Consumer Data Privacy in a Networked World,² was itself interesting because it invoked a haloed phrase in proposing a “Consumer Privacy Bill of Rights.” This bill of rights was premised on a series of “Fair Information Practice Principles” (FIPPs). If adopted, four of them (Individual Control, Transparency, Respect for Context and Focused Collection) would significantly reign in some dubious big data practices. Further, the report acknowledged the specific challenge posed by data brokers in contrast to other data custodians noting that as “third parties become further removed from direct interactions with consumers, it may be more difficult for them to provide consumers with meaningful control over data collection.”³ To counter this, the report urged data brokers to over-emphasize other FIPPs such as transparency.

The second report was published a month later by the FTC: Protecting Consumer Privacy in an Era of Rapid Change.⁴ This report augmented the FIPPs with the recommendation that data custodians adopt “Privacy by Design” (“Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy”).⁵ The FTC also recommended “targeted legislation to provide greater transparency for, and control over, the practices of information brokers” to “provide consumers with access to information about them held by a data broker.”⁶

The two reports from 2012 shared an unfortunate feature. Neither would apply their proposals to already regulated sectors such as health care or financial services, presumably believing that existing regulation (in the case of health care, HIPAA) provided adequate protections. However, data brokers generally are not subject to HIPAA regulation and the reports underestimated the growing ability of brokers to create health data “proxies” in un-regulated space as substitutes for the data residing inside health care protected by HIPAA.⁷

The White House and FTC reports preceded both the 2012 presidential election and the Snowden revelations about government surveillance in the U.S. that began in June 2013.⁸ Thereafter, perhaps it is not surprising that federal government interest in any fundamental overhaul of individual privacy apparently has decreased. Notwithstanding, in 2014 considerable energy was poured into a more narrowly focused area: the regulation of data brokers.

Nicolas Terry, LL.M., is the Hall Render Professor of Law and Executive Director of the Hall Center for Law and Health at Indiana University Robert H. McKinney School of Law. He works at the intersection of healthcare, law and information technology and is @nicolasterry on Twitter.
The third report, the White House’s *Big Data: Seizing Opportunities and Preserving Values,* was published after White House counselor John Podesta announced a 90-day review of the topic. Given the surveillance technologies underlying big data, it was not a surprise that the report opined that the federal government “should support the development of big data technologies with the full suite of policy instruments in its toolkit” and “invest in research and development to support big data technologies, especially as they apply to education, health care, and energy.”

However, the report also recognized that “big data technologies can cause societal harms beyond damages to privacy, such as discrimination against individuals and groups,” including the “intent to prey on vulnerable classes.” As a result the White House prodded the Department of Commerce to make progress on the Consumer Privacy Bill of Rights and recommended that federal “civil rights and consumer protection agencies should expand their technical expertise to be able to identify practices and outcomes facilitated by big data analytics that have a discriminatory impact on protected classes, and develop a plan for investigating and resolving violations of law.”

Published soon after the FTC’s *Data Brokers* report was primarily a fact-finding exercise, examining the markets and practices of nine major data brokers. When the FTC did address policy or regulation, it returned to its 2012 theme of recommending greater transparency from the brokers. Importantly, however, the agency had by now realized how data brokers could make an end-run around health data protection by creating data “proxies” outside of HIPAA-protected space. As a result the FTC recommended immediate action but hardly a barrier to abusive conduct by big data brokers. Other than that its primary recommendation was gaining “technical expertise to stop collection and sharing such information with data brokers.”

This proposal seems to suggest a shift in FTC policy with the agency ceasing to believe that existing domain protections for health information are sufficient. Increasingly, HIPAA protections will be marginalized as health data is generated or processed outside of the conventional health care domain. This legislative proposal thus seems consistent with the agency’s recent assertion of its general powers to regulate privacy and security and its willingness to assert its general jurisdiction notwithstanding possible application of sector-specific regulation.

Finally, the President’s Council of Advisors on Science and Technology (PCAST) issued its *Technological Perspective* report. To a large extent this was a companion report to the White House’s *Seizing Opportunities, focusing on the technologies behind big data. However, in the second half of its report, PCAST also made some very interesting policy observations. First, and of considerable salience because big data companies at best support opt-out consents, PCAST was highly critical of current notice and consent privacy models, viewing them as “increasingly unworkable and ineffective.” Second, PCAST proposed a modern technological replacement for current choice architectures: automated privacy preference profiles.

With regard to more conventional data protection tools, PCAST was skeptical of regulation of data collection, the right of erasure or “a priori limitations on applications, and analysis.” Rather, PCAST favored regulation of harm-causing uses rather than its collection and analysis. The report defined such uses as “the specific events where something happens that can cause an adverse consequence or harm to an individual or class of individuals” because such “use” events (in commerce, by government, or by individuals) embody the necessary specificity to be the subject of regulation.”

A Reform Synthesis?
There is little fundamental disagreement among these reports as to the challenge of big data and the need for additional self-regulation and legal reform. However, finding agreement on specific proposals so as to drive a legislative agenda is more difficult.

The 2012 White House report contained relatively robust proposals suggesting that data subjects should have considerably more control over what data is collected and respect for the context of that collection. Two years later the West Wing repeated its support for FIPPs. But that support seemed less than convincing. After all, if this was the preferable approach, why had the administration’s own Department of Commerce failed to make any apparent progress? By 2014 the White House seemed more in favor of a national notification of breach law — a worthwhile addition but hardly a barrier to abusive conduct by big data brokers. Other than that its primary recommendation was gaining “technical expertise to stop discrimination.”

For the FTC there was no back-sliding; it took the same position in 2014 as it had in 2012. Alas, its calls for data custodian transparency and data subject access are processed themed rather than substantive and offer only downstream data protection. However, the agency’s approach should not be a surprise; until given the broader cross-sector powers it deserves, the FTC will continue to argue that businesses should promise transparency, access, and
Transparency and point-of-use regulation should be part of the regulatory toolbox. But, if the worst excesses of big data are to be resisted (and in the process promote its positive uses in health care), then Congress needs to take up the 2012 White House FIPPs proposals and ensure that data subjects have more control over what data is collected and that the context for any collection is respected.

privacy because enforcing such promises is its clear-est mandate.18

Notwithstanding its technological perspective, the PCAST report surprisingly added real value to the policy/regulation debate over big data. Indeed, the report’s dismemberment of notice and consent may be a landmark in our data protection debate. However, PCAST’s core position, that collection and erasure regulation should be abandoned, is regrettable. The PCAST substitute is “use point” regulation that mirrors the White House’s exhortation that privacy regulators should gain expertise in point-of-use discrimination. Obviously this type of discrimination should be prohibited. Equally, we have at least one successful example of such regulation: the Genetic Information Nondiscrimination Act of 2008 (GINA). However, genetic discrimination is broadly understood and definable. How would we regulate other, more generalized point-of-use concerns such as “inferences related to ethnicity, income, religion, political leanings, age, and health conditions”?20 Or the even more amorphous “data determinism”?21

Transparency and point-of-use regulation should be part of the regulatory toolbox. But, if the worst excesses of big data are to be resisted (and in the process promote its positive uses in health care), then Congress needs to take up the 2012 White House FIPPs proposals and ensure that data subjects have more control over what data is collected and that the context for any collection is respected.

Conclusion
In contrast to the indecision shown by the federal government some of our trading partners seem more willing and capable of taking on the big data brokers. Recently the European Court of Justice asserted a right of erasure21 and in the UK a broad review by the Information Commissioner concluded, “Our view is that the basic data protection principles already estab-

lished in UK and EU law are still fit for purpose in the big data world. The view that current data protection principles are not adequate underestimates their inherent flexibility.”22

Unfortunately, the current views of our federal government on big data regulation and how to deal with the threat to health privacy are either incoherent or, at best, coalescing around inadequate downstream data protection models such as transparency and use point regulation. Although a step in the right direction, the White House’s recently released draft Consumer Privacy Bill of Rights Act is not without its problems.23 If nothing else, we should rally around the clearest legislative proposal on the table — the FTC’s recommendation that affirmative express consent should precede the collection and sharing of health information with data brokers.

Acknowledgement
I thank Scott Ř. Spicer, Indiana University Robert H. McKinney School of Law J.D./M.B.A. Candidate 2016, who assisted with timely and perceptive edits. Of course, the errors that remain are mine.

References
3. Id., at 13.
5. Id., at viii.
6. Id., at iv.-v, 73.
11. See White House, supra note 9, at 48, 51, 60.
13. Id., at viii-ix.
14. FTC § 5(a)(1) “Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.” FTC v. Wyndham Worldwide Corp., (D. NJ 2014) (FTC had authority to regulate companies’ failure to maintain reasonable and appropriate data security).


17. Id., at 40-50.


