TECH FREEDOM

Comments of

TechFreedom[1]

In the Matter of

Government "Big Data"

Request for Information
A Notice by the Office of Science and Technology Policy

March 31, 2014

[1] TechFreedom is a a non-profit, non-partisan technology policy think tank with 501(c)(3) tax-exempt status. Questions may directed to Berin Szoka, President of TechFreedom, at bszoka@techfreedom.org.

Understanding the benefits and costs of Big Data and even beginning to weigh them against each other is likely not something that can be achieved in the limited 90-day window given to the Office of Science and Technology Policy. Mr. Podesta seemed to acknowledge this in his blog post about this inquiry:

> we expect to deliver to the President a report that anticipates future technological trends and frames the key questions that the collection, availability, and use of 'big data' raise – both for our government, and the nation as a whole. It will help identify technological changes to watch, whether those technological changes are addressed by the U.S.'s current policy framework and highlight where further government action, funding, research and consideration may be required.[2]

Above all, we urge OSTP, the Administration, and those following this inquiry to keep clearly in mind that this report is the beginning of an ongoing process, not the end, that it will frame many more questions than it can possibly answer. Even with this more limited ambition, the Report can offer invaluable guidance to policymakers struggling to understand Big Data and what, if anything, to "do" about it.

Economics Must Guide Any Study of Big Data

On the benefits of Big Data, we urge OSTP to keep in mind two cautions. First, Big Data is merely another trend in an ongoing process of disruptive innovation that has characterized the Digital Revolution. Even before the advent of the Internet, the semiconductor industry saw change accelerate at a pace that was scarcely before conceivable. We now know that this was Moore's Law at work: the doubling of computing power roughly every eighteen months. One industry after another has been disrupted by digital technologies, which allow new companies to emerge out of nowhere with new ways of doing things that can quickly render obsolete not just existing companies but existing ways of doing business – and radically change consumer expectations.[3]

In hindsight, the benefits to consumers of this topsy-turvy process loom large in many aspects of American life. Yet the process has been painful, not just for incumbent industries and business models, but for those uncomfortable with "What Hath [Technology] Wrought"[4] in our daily lives, from transforming media to unsettling our most deeply held assumptions about privacy, security, child-rearing and a host of other emotionally wrought topics. The only safe

---

[2] http://www.whitehouse.gov/blog/2014/01/23/big-data-and-future-privacy

[3] *See generally* Larry Downes & Paul Nunes, *Big Bang Disruption: Strategy in the Age of Devastating Innovation* (2014).

[4] "What hath God wrought," a phrase from the Book of Numbers, was the first message transmitted by telegraph in 1844.

generalization that can be made is that, however difficult these changes may seem to us in hindsight, we tend to forget how painful they were at the time, both because it was difficult for even experts to predict the benefits of new technologies and because risk aversion so is deeply rooted in human nature that few at the time would really have believed even the most accurate predictions that it was worth it. Had "the future" been put up for a vote, it probably would have been banned. The point is that any inquiry into future benefits should begin from the assumption that many of the greatest benefits remain unknowable *ex ante* and that any attempt to weigh unknown future benefits against more easily imaginable potential harms will fundamentally bias policymakers against innovation.

Second, cost-benefit analyses generally, and especially in advance of evolving technologies, tend to operate in aggregates because those are more easily measured: How large an economic boost might Big Data make to our society? What are the current costs of, say, identity theft? These predictions can be useful for providing directional indications of future trade-offs, but they should not be mistaken for anything more than that. Life operates, at all levels, not in terms of aggregate, but on the margin: aggregate benefits tell us little about the trade-offs involved in specific practices, and where regulation can be most helpful – or harmful.

These two cautions should lead this inquiry to begin from a stance of humility and a general presumption that we are limited in our ability both to predict and to shape the future in ways that will actually benefit consumers. The task of economics is not to make specific predictions so that policymakers can pull "policy levers" with a clear sense of what the resulting effect of their manipulations will be, but, as Friedrich Hayek famously put it, "to demonstrate to men how little they really know about what they imagine they can design."

Economics *can* play a vital role in this inquiry, however, if assessment of trade-offs on the margins is integrated throughout, even in topics that may seem to have little to do with economics. Nowhere is economics more sorely needed than in the debate over the efficacy of de-identification, which is in fact a debate over the cost-effectiveness of re-identification. It is not enough to assert that a data set *can* be re-identified. After all, "Three monkeys hitting keys at random on typewriters for an infinite amount of time will almost surely produce Hamlet."[5] The key question is: is a particular data set *likely* to be re-identified based on the potential value of the uses of the data and the costs of re-identification. In other words, how many monkeys and

[5] David Ives, *Words, Words, Words* (1987).

how long *would* it take? And on the other end, how much de-identification is adequate is also as much an economic question as it is a computer science or statistical question.[6]

An economics-informed assessment of these trade-offs should lead us to more carefully weigh the costs and benefits of large data sets and to focus regulation, and the limited enforcement resources of regulators, on areas where regulation can do more good than harm. This is true on most, if not all, of the concerns raised by Big Data, from privacy to data security. Economics can help understand the trade-offs involved in addressing "non-economic" concerns like societal and constitutional values. Even if economists do not have the final word on policy decisions, they have an invaluable role to play as advisors.

Big Data *Is* Speech: This Inquiry Must Address the First Amendment

Since the purpose of this inquiry is, in the end, to shape policymaking, it must also confront another dimension of trade-offs: regulation of the private sector's use of "Big Data" largely means regulation of speech protected by the First Amendment. The Supreme Court made clear in *Sorrell v. IMS Health, Inc.*, 131 S. Ct. 2653 (2011) that data *is* speech:

> This Court has held that the **creation and dissemination of information are speech** within the meaning of the First Amendment. See, e.g. , Bartnicki , supra , at 527 ("[I]f the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct" (some internal quotation marks omitted)); Rubin v. Coors Brewing Co. , 514 U. S. 476, 481 (1995) ("information on beer labels" is speech); Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc. , 472 U. S. 749, 759 (1985) (plurality opinion) (credit report is "speech"). Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes.
>
> The State asks for an exception to the rule that **information is speech**...[7]

It is by no means clear how the Court's jurisprudence on First Amendment protection will evolve. The Court has *always* struggled to apply free speech principles as technology has changed, and Big Data will, in that respect, be much like the telegraph, telephone, film, television, the Internet

---

[6] See generally, Jane Yakowitz, *Tragedy of the Data Commons*, 25 Harv. Jrnl. Law & Tech 1 (2011), http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech1.pdf

[7] 131 S. Ct. at 2667.

and video games. Given that OSTP's competence is technical rather than legal, this inquiry, and the future studies it engenders, should focus on the forms of "speech" enabled by Big Data and how it might "advance human knowledge" within its overall inquiry into the benefits of Big Data. This will help policymakers to approach Big Data with greater caution than they have traditionally approached new media.

This does not necessarily mean *less* regulation but does mean *better* and more constitutionally defensible regulation. Even those who think the government should have a lower burden in regulating Big Data than it would in regulating speech more generally should find the general approach of First Amendment analysis a useful heuristic for thinking about how best to deal with Big Data: What, exactly, is the government's interest? How substantial is it? Are the means chosen appropriately or narrowly tailored to address that interest? Are they over-broad? Are there other, less restrictive means available to address the problem? Is the approach either over- or under-inclusive?[8]

These are difficult questions that will either be dealt with carefully by policymakers or, if not, by courts who send legislators back to the drafting board. This inquiry cannot, of course, address all of them, but it must begin the process of integrating an assessment of First Amendment values and doctrines, along with economics, into the study of Big Data and its policy implications.

Government Threats to Privacy

The low-hanging fruit for this inquiry – the areas where policymakers can do the greatest good at the lowest cost in terms of lost innovation, economic benefits or meddling in the still-evolving speech platforms of the Digital Age – is clear: focus on government. Government is not the only source of harm to consumers, but it is the source of the greatest and clearest harms.

Long before Edward Snowden's revelations, TechFreedom and dozens of other non-governmental civil liberties organizations, trade associations and companies joined together in the Digital Due Process Coalition to advance four simple principles for reforming the Electronic Communications Privacy Act of 1986.[9] A clear, broad consensus now exists around the need to ensure that law enforcement agencies cannot access content without a warrant. Indeed, the Sixth Circuit has even ruled that ECPA's failure to require a warrant for content in general

---

[8] See generally Berin Szoka, The Progress & Freedom Foundation, *Privacy Trade-Offs: How Further Regulation Could Diminish Consumer Choice, Raise Prices, Quash Digital Innovation & Curtail Free Speech*, Comments to the FTC Privacy Roundtables (Dec. 7, 2009), available at http://www.scribd.com/doc/22384078/PFF-Comments-on-FTC-Privacy-Workshop-12-7-09

[9] http://digitaldueprocess.org/index.cfm?objectid=A77781D0-2551-11DF-8E02000C296BA163

violates the Fourth Amendment's protection against unreasonable searches and seizures.[10] Essentially the entire court in *U.S. v. Jones* clearly indicated their discomfort with the failure of our laws to protect Fourth Amendment values as technology has changed.[11] Justice Sotomayor warned that "Awareness that the Government may be watching chills associational and expressive freedoms" and called for the Court "to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." Justice Alito and three other Justices explicitly called on Congress to address "concern about new intrusions on privacy" through legislation because Chief Justice Taft's warning that "regulation of wiretapping was a matter better left for Congress has been borne out."

Yet, four years later, while the courts have made great progress, including a scathing magistrate decision scolding the Department of Justice for not meaningfully complying with *Warshak*,[12] Congress has talked about the issue but has done nothing – but at least action finally appears imminent: ECPA Reform legislation now has 193 sponsors in the House.[13] This momentum towards long overdue reform has built slowly but steadily – with no help whatsoever from this Administration.

It takes a special kind of temerity for the President to loftily promise a "Consumer Privacy Bill of Rights"[14] – while doing nothing to protect the *real* Bill of Rights, the Fourth Amendment that is the crown jewel of the civil liberties: the warrant requirement that was among the chief inspirations for the American Revolution.[15]

This Administration's Department of Justice has sought warrants for email content only when ordered to do so by the Sixth Circuit in *Warshak* and even then, did not take the requirement seriously, as the recent magistrate decision makes scathingly clear. Worse, the Administration has actively worked to sabotage ECPA reform by orchestrating opposition to ECPA reform from

---

[10] *U.S. v. Warshak*, 631 F.3d 266 (6th Cir. 2011).

[11] *U.S. v. Jones*, 565 U.S. 945 (2012).

[12] In Matter of United States of America for a Search Warrant for a Black Kyocera Corp Model C5170 Cellular Telephone with FCC ID: V65V5170 (D.D.C. March 7, 2014), available at https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2014mj0231-2

[13] H.R. 1852: Email Privacy Act, https://www.govtrack.us/congress/bills/113/hr1852

[14] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[15] See Testimony of Berin Szoka, TechFreedom, before the House Energy & Commerce Committee Subcommittee on Commerce, Manufacturing, and Trade, hearing on *Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?*, at 4-5, March 29, 2012, available at http://democrats.energycommerce.house.gov/sites/default/files/documents/Testimony-Szoka-CMT-Balancing-Privacy-and-Innovation-President-Proposal-2012-3-29.pdf

nominally independent agencies, which appear in fact to be working in conjunction with the Department of Justice. In particular, the fanatic insistence by the Securities and Exchange Commission, now joined by the Federal Trade Commission and other agencies, that administrative agencies should be exempt from the general requirement for a warrant to access content information, has stalled ECPA reform in the Senate.

Meanwhile, the Administration has simply ignored a WhiteHouse.gov petition signed by 110,423 Americans entitled "Reform ECPA: Tell the Government to Get a Warrant."[16] Despite promising to respond "in a timely fashion" to any petition that receives 100,000 signatures within 30 days,[17] the Administration has done nothing[18] – yet it has found plenty of time to respond to a petition by *Star Wars* fans urging the Administration to begin building a Death Star by 2016 with the clever title "This Isn't the Petition Response You're Looking For."[19] We are *not* amused.

This stubborn opposition to sensible, bi-partisan privacy reform is outrageous and shameful, a hypocrisy outweighed only by the Administration's defense of its blanket surveillance of ordinary Americans – a problem so well known that it requires no special description here.

It's time for the Administration to stop dodging responsibility or trying to divert attention from the government-created problems by pointing its finger at the private sector, by demonizing private companies' collection and use of data while the government continues to flaunt the Fourth Amendment.

This inquiry offers the Administration a chance to redeem itself, at least in part. This report should assess the full costs, both in economic terms and in constitutional values, of easy surveillance and access to private data by law enforcement and national security agencies. The report should recommend ECPA reform as outlined by the Digital Due Process Coalition, especially a clear email requirement for access to content and location data that applies to *all* law enforcement agencies, including regulators. OSTP's report should support real and meaningful reforms to national security agencies' collection of, and access to, private communications, both their content and metadata.

Regulating the Private Sector

---

[16] https://petitions.whitehouse.gov/petition/reform-ecpa-tell-government-get-warrant/nq258dxk

[17] https://petitions.whitehouse.gov/how-why/terms-participation

[18] Mark Stanley, Center for Democracy & Technology, *White House Still Silent on Warrantless Email Snooping*, March 31, 2014, https://cdt.org/blogs/mark-stanley/3103white-house-still-silent-warrantless-email-snooping

[19] https://petitions.whitehouse.gov/response/isnt-petition-response-youre-looking

Getting government's own house in order does not mean ignoring legitimate concerns raised by Big Data, such as how privacy companies may use data they collect and how they secure it against breaches. This inquiry can proceed along both tracks. But rather than get bogged down in abstract debates about the ideal regulatory regime for privacy and data security, an intellectual quagmire in which Washington has been stuck since the FTC first endorsed comprehensive privacy legislation in 2000 (over the vigorous objections of two Commissioners),[20] this inquiry should at least begin with, if not focus on, the legal regime that currently exists for regulating Big Data and other new technologies. That means assessing not merely what the FTC has done about privacy and data security in the past but, more importantly, *how* it has operated.

FTC leadership increasingly point to what they call a "common law" of digital consumer protection, meaning the dozens of enforcement actions they have settled across a wide range of cases, from online fraud to data brokers to data security to user interface design. A case-by-case method does indeed have great virtues over *ex ante* regulation for precisely the reasons mentioned above: it is difficult to predict the future, especially the unknowable benefits of new technologies, and attempts to encode today's expectations in law often do more harm than good. As the FTC declared in its 1980 Policy Statement on Unfairness: "[Section 5 of the FTC act] was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion."[21]

But even if the FTC has reached the right policy outcome in many, or even most cases, its version of the "common law" is a hollow one, devoid of the very analytical rigor by which the adversarial process of litigation weighs competing theories and advances doctrine.

The FTC regulates privacy, and will regulate Big Data, primarily through its deception and unfairness powers. Yet in over seventeen years of dealing with digital consumer protection cases, the FTC has done little to develop these rich legal concepts beyond their application in the traditional marketing contexts, which the FTC was originally created to police.

This is chiefly because companies so rarely challenge enforcement actions and when the Commission settles an enforcement action, Section 5(b) requires only that (a) the Commission has "reason to believe" a violation of law has occurred and (b) believes that *opening* the enforcement action would be in the public interest. Section 5(b) does not require *any*

[20] http://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission

[21] http://www.ftc.gov/ftc-policy-statement-on-unfairness

justification or process for *settling* a case unless the Commission seeks a monetary penalty (e.g., for violations of existing consent decrees). Thus, the settlements cited by the Commission as "guidance" do not even, by their own terms, purport to reach the merits of underlying issues. The Bureau of Economics, which has played a vital role in helping to shape what may far more accurately be called the "common law" of antitrust over the course of decades, has played little apparent role in guiding the FTC's approach to consumer protection. This has led the FTC to prioritize creative theories of harm and issues that might make compelling law review topics over clear consumer harms such as identity theft. While identity theft remains far and away the leading source of consumer complaints to the FTC,[22] the FTC has not held a workshop on the topic under this Administration.

The FTC has, commendably, begun to remedy its shortcomings in other areas, most notably by trying to build an in-house technologist capability. But it has resisted changing its overall approach for the simple, understandable reason that law enforcement agencies rarely, if ever, want to make their jobs even slightly more difficult. It is no more realistic to expect the FTC to reform its own processes without significant external pressure than it is to expect the NSA to do so. Once again, what is required is leadership from the Administration and Congress into the FTC's processes.

We believe the FTC's underlying legal standards are fundamentally sound and already provide basis for "comprehensive privacy regulation," including Big Data. But if the FTC is to be trusted with the sweeping, vague power it currently holds over nearly every company in America, it is critical that a serious inquiry begin into *how* the FTC operates. Clearly, the courts have failed to play the role both the FTC and Congress assumed they would when the FTC declared, in an effort to defuse a heated stand-off with an outraged Congress over the FTC's abuse its authority,[23] that:

> The present understanding of the unfairness standard is the result of an evolutionary process. The statute was deliberately framed in general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. The task of identifying unfair trade practices was therefore assigned to the Commission, **subject to judicial review**, in the expectation that the

[22] http://www.ftc.gov/news-events/press-releases/2014/02/ftc-announces-top-national-consumer-complaints-2013

[23] Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, May 30, 2003, http://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection

> underlying criteria would evolve and develop over time. As the Supreme Court observed as early as 1931, the ban on unfairness "belongs to that class of phrases which do not admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the **gradual process of judicial inclusion and exclusion**.'"[24]

Our FTC: Technology & Reform Project, composed of leading FTC experts and veterans, has begun an inquiry into how the FTC operates and how its processes could be improved to draw on many of the benefits of a true common law. [25] Like this inquiry, we see our own project as the beginning of an ongoing dialog. But already it has become clear that a series of relatively small changes could vastly improve how the FTC weighs concerns raised by new technologies, most notably ensuring clearer analysis of the component elements of its unfairness and deception powers, and greater incorporation of economics and First Amendment values in its analysis. By carefully amending Section 5 to create procedural safeguards for how the FTC settles cases and by examining why defendants essentially *always* settle, Congress may be able to help the FTC better execute its mission of advancing consumer welfare by focusing on clear harms to consumers that are not outweighed by greater benefits and that consumers themselves cannot effectively avoid.

OSTP's inquiry offers an invaluable opportunity to refocus the endless, unconstructive "privacy debate" on the concrete "how" of privacy law: FTC process. This, more than any abstract legal theory, will ultimately shape the regulation of Big Data.

---

[24] http://www.ftc.gov/ftc-policy-statement-on-unfairness

[25] *Consumer Protection & Competition Regulation in a High-Tech World: Discussing the Future of the Federal Trade Commission: Report 1.0 FTC: Technology & Reform Project*, (Dec. 2013) http://docs.techfreedom.org/FTC_Tech_Reform_Report.pdf