I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Making No Secrets About It

REED E. HUNDT*

When Big Government cajoles Big Companies to share Big Data, the question inescapably follows: What should be the governing rules for digital information?

Law, regulation and norms relating to the analog world–that which people see, hear, smell, touch, and taste–do not translate well to the digital world. Everything that can be known is being memorialized in the domain of electromagnetic signals that codify information in volume too vast and patterns too complex for humans to understand. The five senses have no presence in the digital world. Flesh and blood people can send messages–queries, instructions, information–into the digital network of circuits and electromagnetic waves. Responses come back: the restaurant expects you and your five senses at 8 p.m. and here are the directions to get there.

But behind the response, in the near infinitude of electrical circuits, no human can even pretend to keep up with the digital collection and use of information. All information can be recorded, and almost all soon will be, in the computers of the digital domain. "Information" must be meant as any observation, transmission, calculation or memorialization. The information may relate to something at rest (the restaurant door recorded by a surveillance camera, the restaurant's seating chart and menu) or in motion (a tweet about the menu, a credit card payment for dinner). It will include, in Peirce's taxonomy, evidence of "signs," assumptions about "objects," and the provision of "interpretants." [1]

---

* Reed E. Hundt is the former chairman of the Federal Communications Commission. He currently sits on the boards of a number of technology companies, including Intel Corporation, and is an attorney in Washington, D.C.

[1] See "The Commens Dictionary of Peirce's Terms," *Commens*, accessed January 26, 2014, http://www.helsinki.fi/science/commens/dictionary.html.

The networked computers of the digital domains not only preserve the "signs," but they draw conclusions about the "objects" to which the signs relate: with that prix fixe meal, amuse-bouches are to be expected. They constantly seek and create patterns from which they draw conclusions ("interpretants") of at least two kinds: what caused an action to occur in the past and what is causing actions probably to occur in the future. People have gone to this restaurant because they know it serves paté off the menu and under the table; people will continue to go because San Francisco has banned paté. The computers know everything that can be known. They also opine and predict. They will keep their views to themselves or share them with humans, at least in simplified form.

The computers keep most of their data to themselves because the volume of digital data is too large for any person to review within the span of human life. The computers manage that data too quickly for any human to follow by hand or eye. Humans can understand the digital domain only in two ways: in theory and in the practical form of receiving answers to questions (yes, that particular San Francisco restaurant offers paté off the menu).

Some may draw the corollary that humans should be indifferent if machines turn every sign and symbol of an individual's "thoughts, sentiments, and emotions"[2] into computer code. No one needs to be concerned about computers knowing everything about everyone. Similarly, you should not worry if the shining sun sees you lounging naked in your back yard. If some are not much troubled by learning how much data lies in data banks, they may believe humans have a right of privacy only as against the intrusions of other humans.

The digital domain may well be as inaccessible and mysterious as the stars. It may operate under rules as seemingly irrelevant to our analog world as Einsteinian relativity. Yet when the nuclear reactors of Fukushima melt down, the most abstruse laws of physics have manifold impact on the world that humans do feel with their five senses. When the digital domain intersects with the analog, its vast power can completely alter the way we live. Humans, or at least those possessing state-granted authority, can command that point of intersection. They can and do decide when and how the digital will have impact on the analog, when and how the opinions and predictions of the digital domain will lead to inquisition or incarceration in the physical world. Because the digital does impact the analog, none of us should be unconcerned about what computers know about us. Only machines should be indifferent to machines.

---

[2] Samuel D. Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890).

I argue here that the doyens of the digital domain, comprised of big businesses with big access to nearly infinite data and big government with nearly overwhelming persuasive power, are crafting the operational rules for governing digital information. Constraining the government's behavior is, as since the beginning of the United States, the Constitution. But the companies, courts, Congress, and the Executive Branch are reinterpreting our rights for the digital domain. However, secrecy, in both corporations and the government, makes the rules difficult to discern.

Based on what little we humans (can) know, the emerging practices and constitutional interpretations applicable to the digital domain are likely to allow government to make more errors in preventing criminal acts or apprehending bad actors than will be acceptable to the sense of justice most of us hold. Under the developing practices for digital information, government will be allowed to use information for ends that most individuals would find unacceptable, even repugnant, potentially edging toward tyrannical. Further, the currently developing practices for big government's use of big data will lead to staggering expenditures of taxpayer funds. That in turn will cause the government to delegate its tasks to big data-collecting companies, turning them into satrapies of the central state. If allowed to flower, such corporatism would prove destructive to both economic and social freedom. Finally, I argue that government and private sector secrecy about the current rules enhances these three risks: error, misuse, and corporatism. If any or all of these trends develop, they will cause a deterioration of the trust relationship between any American and the government.[3] Without trust among individuals, firms, and the state, even the most effective police force cannot assure a coherent, well-functioning society.

No one involved in the technological breakthroughs that raise these possibilities wants a part in creating such a dystopian future. Almost all want to preserve for Americans, if not the whole world, what playwright Tom Stoppard called "autonomous freedom, the freedom to think for oneself, to use one's discretion . . . to apply common sense, and common humanity."[4] Therefore, for the purpose

---

[3] To quote Richard Thaler: "Trust is really important in society, and anything we can do to increase trust is worthwhile. There's probably nothing you could do to help an economy grow faster than to increase the amount of trust in society." See Douglas Clement, "Interview with Richard Thaler," *The Region,* October 3, 2013, accessed January 26, 2014, http://www.minneapolisfed.org/publications_papers/pub_display.cfm?id=5184.

[4] Tom Stoppard, "Tom Stoppard: Information is Light," *The Guardian,* October 11, 2013, accessed January 26, 2014, http://www.theguardian.com/stage/2013/oct/11/tom-stoppard-pen-pinter-lecture.

of such preservation, the new rules should be identified and debated. Better rules should be adopted than those being put in place. The Constitution should be applied to the digital domain, not *in hoc verba*, because those 18th century precepts do not translate clearly,[5] but in practical ways that continue to protect everyone who is relatively powerless against those who are relatively powerful.

What, then, are the current rules? At the appellate level, the large mobile carrier, Verizon, is now arguing that no law or regulation can govern access to the digital domain.[6] Verizon claims that the First Amendment does translate from analog to digital, and that it anoints Internet access as a kind of apostolic successor to the printing press. Because Verizon provides access to the Internet and the near infinitude of digital information therein, it is like a newspaper with a printing press that provides access to analog information. Hence, no government can make any law that constrains Verizon's behavior. Specifically, Verizon can decide who has access at what price (a newspaper can decide to whom it should sell and at what price). And Verizon can decide what to give access to (a newspaper can decide what to print). Verizon can choose, for example, what emails to send, on the other hand a newspaper can decide what letters to the editor to print.

This argument mistakes conduit for content, according to the brief on behalf of Susan Crawford, a well-known law professor, and me.[7] Verizon is a newspaper delivery truck, but not a newspaper or a printing press. Analogy, it seems, is the way that law maps the analog world of the drafters of the First Amendment to the digital domain. Analog values, like autonomous freedom, as well as analog objects like "printing presses," also must be restated in forms that make sense in the fusion of digital and analog experience that is the way we live now.

---

[5] In an interview published October 6, 2013, Justice Scalia said as to originalism, "Words have meaning. And their meaning doesn't change." See Jennifer Senior, "In Conversation Antonin Scalia," *New York Magazine,* October 6, 2013, accessed January 26, 2014, http://nymag.com/news/features/antonin-scalia-2013-10. However, technology can alter what words mean. When the Bill of Rights was adopted, purple meant to most people a color verging on red. Then in 1856, William Perkin invented a synthetic dye that made a more bluish color widely marketed and sold as "purple," the commercial success of which effectively shifted the meaning of the "purple" toward mauve. More recently, Facebook seems to have changed "friend" into a verb with evolving connotations.

[6] Verizon v. Federal Communications Commission, No. 11-1355 (D.C. Cir. January 14, 2014).

[7] See Susan Crawford, "Verizon v. FCC: Why It Matters," *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age,* September 8, 2013, accessed January 26, 2014, http://scrawford.net/verizon-v-fcc-why-it-matters.

Without waiting for the court of appeals or Congress, Internet access providers (primarily telephone and cable companies) and over-the-top-of-Internet-access companies (Google, Facebook, Amazon, Yahoo, and others) are creating and following new rules to the digital domain. I will call these firms "OTT," for "over the top." I will call the access providers "carriers."

The carriers keep track of the parties, geographic location and duration of all digital communication.[8] They could ask the computers in their networks to examine and save the content of communications but as far as I know, they do not. Almost all digital communication goes over one or more of the networks owned by a mere handful of carriers.[9] For many years, these carriers have shared with government what they know about digital communication, sometimes after receiving warrants, and sometimes without such formality.[10]

The OTT firms (think: Gmail, Instagram, PayPal) transmit words, pictures, numbers. They use the carriers' networks, but while transmitting the content they can and do have their computers review it. They save what they choose to save, which is a lot. They presumably believe, like the carriers, that the First Amendment bars government from interfering with their content practices. But as of this writing, no OTT firm has chosen to be the protagonist in a digital version of the *Pentagon Papers* case.[11] I suspect that none wants to reveal how it gathers information or how skimpy the proof of consent is from all of us who provide the information.

Besides, the OTT firms' case would not align them with the public interest. In *Pentagon Papers*, the newspaper championed the public's right to understand its government's actions against the government's attempt to keep its conduct secret.[12] In opposing the government's efforts to get its hands on the OTT's firms' information about the

---

[8] Siobhan Gorman and Devlin Barrett, "White House Weighs Options for Revamping NSA Surveillance," *Wall Street Journal*, February 25, 2014, accessed March 5, 2014, http://online.wsj.com/news/articles/SB10001424052702303880604579405640624409748.

[9] See Warren Grimes, "Competition Will Not Survive the Comcast-Time Warner Merger," *Forbes*, February 27, 2014, accessed March 5, 2014, http://www.forbes.com/sites/realspin/2014/02/27/competition-will-not-survive-the-comcast-time-warner-merger/.

[10] "Google Transparency Reports," *Google*, accessed April 9, 2014, http://www.google.com/transparencyreport/userdatarequests.

[11] New York Times Co. v. United States, 403 U.S. 713 (1971) (per curiam).

[12] See ibid.

public, the OTT firms would be arguing that their own largely secret data gathering is privileged over the government's secret actions.[13] They would not be contending that they are the agents of individuals who use their services. If they invoked a right of privacy, it would be a business's right to keep its practices secret from users, customers and competitors. Although such self-interest would not prejudice their claims in court, it would hardly inspire trust between the OTT firms and the users who provide the information which makes the firms successful.

For decades the government has been able to learn from carriers the location, parties and duration of telephone calls. It also has been able to wiretap lines and listen to conversations. Often government has obtained warrants in order to hear content, but not always.[14] This is because half or more than half of all global telephone communication went to, from, or through the United States, government in this country has also been able to eavesdrop on the bulk of global traffic. Other obliging countries presumably have filled in such gaps as existed. But in only the last few years has the government been able to collect and review the substance of almost every communication.[15] Here again, the global reach of American OTT firms has enabled the American government to take a look at much of the world's digital content. Technological breakthroughs, more than executive or judicial action, have enabled these developments. Technology has preceded law. Law has been obedient to what is technologically possible; law has also been perplexed about technology, worried about taking any action that might enable another 9/11, and incapable of conceiving of a new paradigm for the digital domain.

---

[13] See Federal Communications Commission v. AT&T., 131 S. Ct. 1177 (2011) for a failed attempt.

[14] "In Practice...An American's communication could be read without a warrant, another U.S. official says." Siobahn Gorman and Jennifer Valentino-Devries, "New Details Show Broader NSA Surveillance Reach," *Wall Street Journal*, August 20, 2013, accessed January 26, 2014, http://online.wsj.com/news/articles/SB10001424127887324108204579022874091732470.

[15] "The system has the capacity to reach roughly 75% of all U.S. Internet traffic . . ." Ibid. See also James Risen and Laura Poitras, "N.S.A. Gathers Data on Social Connections of U.S. Citizens," *New York Times*, September 28, 2013 ("The agency can augment the communications data with material from . . . commercial and other sources, including bank codes, insurance information, Facebook profiles, passenger manifests, . . . and GPS location information, as well as property records and unspecified tax data...").

In the United States, and worldwide, a small number of big firms have garnered huge market shares in search, on-line media, digital payments, and other sorts of digital communications. The rise of Google and its ilk has enabled the American government to think big. If the American OTT firms had not been able to seduce from users all the information imaginable, government could not have considered the uses it might make of this data.[16] Certainly government could never have gathered so much data about so many dimensions of human activity if the big companies had not obtained that data from users. The rise of the big firms has also narrowed the group with which the government has had to negotiate in order to get almost all information it can imagine it wants. The government can make offers these firms cannot refuse.

Nor could anyone in government have made much use of the data but for the technological breakthroughs in storage, retrieval, and calculation that commercial innovators have produced. A decade ago, microprocessors were neither fast enough nor cheap enough to store and analyze the volume of digital information generated in America, much less worldwide. Moore's Law, the prediction that microprocessing would double in performance or drop half in price every two years,[17] has enabled government and the really big OTT firms to save and analyze even the vast quantities of digital information that Americans now create and consume. Computers now have programs that permit them to analyze data without first organizing it into columns and rows. Other programs permit computers to learn from their own mistakes. Still other software divides requests (do people really like the paté served under the table at that restaurant?) into discrete tasks to be performed by many different computers, as a result of which answers are delivered when they matter (yes, go ahead and order that paté right now!).[18] Progress

---

[16] In many countries, government has long cemented the symbiotic relationship between telecommunications firms and government's desire to monitor communications by taking ownership stakes in the firms or by tightly regulating such firms. The OTT firms, however, have risen to become the chief data mongers in an era of privatization, in which the United States government, among others, has argued against mixing public and private capital in the same entity, on the grounds that such ownership distorts efficient market conduct. For this reason, government in the United States and philosophically aligned nations has been using tools other than ownership to obtain access to the data gathered by OTT firms.

[17] See "Moore's Law or how overall processing power for computers will double every two years," *Moore's Law,* accessed April 9, 2014, http://www.mooreslaw.org.

[18] See Michael Hickins, "How the NSA Could Get So Smart So Fast," *Wall Street Journal,* June 12, 2013, http://online.wsj.com/news/articles/SB10001424127887324049504578541271020665666.

in antennas, wireless transmission, drones, satellite cameras, facial recognition, smartphones, and many other technologies have extended further the scale and scope of digitizing and gathering information.

As a result of the new combination of big firms, big data and big government, government now routinely asks computers to suggest who has committed crimes. The government also asks computers to predict criminal activities at specific locations, and requests that computers identify people who intend to commit crimes.[19] Presumably, government instructs the computers to generate lists of threats on a continuous basis, ranking them according to probabilities. The computers do machine learning; that is, they constantly refine their analytical skill. The humans in charge of the government's digital domain of course hope the predictions are accurate. But they cannot know for sure how reasonable the computations are,[20] and short of wrestling admissions from every identified suspect, they cannot validate every prediction.[21] Some of the criminals, in the past and predicted in the future, are terrorists; that is, some hideous fervor drives them to kill civilians and destroy facilities integral to society. But we are not discussing here only terrorist activities. That category is too permeable and broad. The uses of the digital domain for analog police work are too plentiful for government to resist applying them to any and all criminal matters.

So this is the way the digital domain actually works. We assume. Little by little newspapers, still putting ink on paper for fingers to touch and eyes to see in the analog world, are reporting the vastness of its reach. Little by little, individuals are grasping that the government is well on the way to becoming the panopticon.[22]

What does this tell us about the application of the Constitution to the digital domain? If we want to be grounded in the emerging reality

---

[19] See "Don't Even Think About It," *The Economist*, July 20, 2013, accessed January 26, 2014, http://www.economist.com/news/briefing/21582042-it-getting-easier-foresee-wrongdoing-and-spot-likely-wrongdoers-dont-even-think-about-it.

[20] See George Dyson, "NSA: The Decision Problem," *Edge*, July 27, 2013, accessed January 26, 2014, http://www.edge.org/conversation/nsa-the-decision-problem ("In modern computational terms...,there is no systematic way to determine, in advance, what every given string of code is going to do except to let the codes run, and find out.").

[21] If suspects are apprehended before they commit the act the computers say they intend – exactly what anti-terrorist efforts try to do – then the ultimate proof of accurate prediction, namely, the deed itself, is obviously never provided. See ibid ("The ultimate goal of signals intelligence and analysis is to learn not only what is being *said*, and what is being *done*, but what is being *thought*.").

[22] Jeremy Bentham's late 18th century design of a building where a watchman could secretly observe the behavior of all occupants. See "Theory of Surveillance: The Panopticon," *Cartome*, June 16, 2001, accessed April 9, 2014, http://cartome.org/panopticon1.htm.

of governmental conduct, at least some of the amendments we call our Bill of Rights should be read with the modifications stated below:

First Amendment: But the Government can learn where and how you worship, what you say, and with whom you meet or communicate.

Second Amendment: But the Government can discover who has bought Arms and can keep track of those persons.

Third Amendment: But the Government can "quarter" virtually in any house, "without the consent of the Owner," technologies that permit the Government to learn any digitized activity by any person or by any device owned by any person.

Fourth Amendment: But the Government can search any device recording digital activity by any person, without obtaining a warrant or having any reason to believe any such person has committed or intends to commit any criminal act; Government can copy any record of any person's digital activity.

Fifth Amendment: But Government can place anyone under examination, as many times and as long as a computer declares such likelihood of having done, or possibly intending to do, a crime. Any person's digital information can be used against such person. Government can take and hold any person's digital information without any process of law specific to such person: a general mandate as to a class of persons or information suffices to justify any taking. No one has a property interest in any digital information at least as against government's possession of such information, no matter how obtained. At least until and unless the Supreme Court decides more cases involving digital information, the rights of individuals in the digital domain at least appear to be curtailed in these procrustean ways. The capabilities of big firms and big government currently are paramount as to digital data.

So what can go wrong? The answer depends on motive, competence, and constraints.

The carriers profit from transmitting the most information and seeking bottleneck pricing power over access. Saving and analyzing information is a cost they cannot recover, save in respect of learning better ways to send information. They do share freely with government, but they do not collect and store much content, at least as far as we know. Their motives to misuse digital data are limited; their competence is fairly high; they face constraining regulation at the FCC and in state regulatory authorities.

OTT firms, like the government, use digital data about past behavior in order to predict each person's future behavior. On the strength of that prediction—who might go to a particular restaurant, what might they order?—they sell placement to advertisers. The OTT firms will give anything away for free or nearly for free (operating systems, maps, news) in order to attract attention to the free material.

Knowing the proclivities of those whose attention is thus captured on a screen the firms control, they sell to advertisers the opportunity to present, visibly, on the handheld or desktop screen, the specific goods and services they wish to sell to those whose previously gathered information suggests are likely to buy these categories of goods and services.

Supposedly it was 19th century merchant John Wanamaker who said, "Half the money I spend on advertising is wasted; the trouble is I don't know which half."[23] Many of the OTT firms aim to persuade modern day Wanamakers that in return for money they can reduce the waste by reporting exactly who saw the ad and then made the purchase.

Perhaps in the near future, OTT firms will also use the information they have gathered from all of us to provide answers to questions (what is the increase in my probable mortality before 70 if I eat that paté?) in return for money. But for now, the principal use is to provide advertisers solutions to the Wanamaker problem. OTT firms are hoisted on their own digital petard, however, because the digital domain also records patterns that seem to show the causal connection between advertising and purchase. As a result, OTT firms face the traditional constraint of capitalism. If they do not perform for their customers—give accurate predictions—then their customers can go elsewhere.

The government wants to use the same data for predictions. It is predicting not consumer purchases but criminal acts. However, the techniques of storing and analyzing the data are much the same for predicting both the benign and the malign acts of humans.

Now we come to the problem of error. The carriers' information (called "metadata") permits the government to assemble a narrative of a suspect's behavior. But its predictive capability is low. The OTT content is richer, more useful, but it neither is nor needs to be perfect in its forecasting. If OTT firms are 75 percent accurate, or even 65 percent accurate, in predicting possible purchases, they offer much better value to advertisers than other media. If the government's predictions of terrorist activity were as far off as that, however, they would be of little use. Moreover, when it comes to the conviction of perpetrators of crimes, government needs to be even more accurate. Did someone steal the paté? What does the camera in the kitchen show? Government needs proof beyond a reasonable doubt. The

---

[23]"Quotation Details," *The Quotations Page*, accessed April 9, 2014, http://www.quotationspage.com/quote/1992.html.

computers managing the digital domain will struggle to give this level of accuracy.[24]

Even if the percentage of accuracy in prediction is 95 percent, the false positive problem is huge. Assume a population of 300 million, and assume terrorists number 1,500. Assume further the computers identify all the terrorists. The problem is that the computers will include in the identification 5 percent of 300 million, or 15 million people. So of those, one out of every 10,000 will be a terrorist; for every terrorist, about 10,000 people will be misidentified as terrorists.[25] Given that these overbroad predictions are made every day, in short order millions of Americans would be identified as terrorists. Misuse of information is of course possible for both OTT firms and government. Anyone at an OTT firm might leak information to those who want to harm the reputations of those surveilled. An OTT firm might follow the bad idea of selling personal information—like a private investigator in the analog era taking photos of cheating spouses. But the market really will mete out quick and serious punishment to OTT firms that misuse information. Trust is the key to the relationship of individuals to OTT firms. Moreover, individuals can have recourse to civil action if and when an OTT firm causes harm in ways cognizable as slander or defamation.

Misuse of data by government is potentially far more draconian and subject to almost no remedy. Misuse by the government means: (a) disclosure that causes reputation and/or career harm to the innocent, (b) threat of disclosure that in turn silences opposition, competing points of view, dissent, and so threatens democracy's successful functioning, or (c) false arrest based on unjustified targeting.[26] These are not the effects of misuse that OTT firms are likely to cause. We can assume with good grounds that the

---

[24] Law avoids stating its time-honored verbal standard in mathematical terms, but perhaps 95% probability is "beyond a reasonable doubt." See Jon O. Newman, "Quantifying the Standard of Proof Beyond a Reasonable Doubt: A Comment on Three Comments," *Law, Probability, and Risk* 5 (2006), 267-69, accessed January 26, 2014, http://lpr.oxfordjournals.org/content/5/3-4/267.full.pdf.

[25] See Corey Chivers, "How Likely is the NSA PRISM Program to Catch a Terrorist?" *Baynesian Biologist,* June 6, 2013, accessed January 26, 2014, http://bayesianbiologist.com/2013/06/06/how-likely-is-the-nsa-prism-program-to-catch-a-terrorist/. See also Carl Bialik, "Ethics Aside, Is NSA's Spy Tool Efficient?" *Wall Street Journal,* June 14, 2013, accessed January 26, 2014, http://online.wsj.com/news/articles/SB10001424127887324049504578543542258054884.

[26] See Barton Gellman, "U.S. Surveillance Architecture Includes Collection of Revealing Internet, Phone Metadata," *Washington Post,* June 15, 2013 ("[NSA data] can...expose medical conditions, political or religious affiliations, confidential business negotiations and extramarital affairs.").

overwhelming proportion of government actors with access to the nearly infinite data of OTT firms do not intend any such harm. But it is said that more than a million people have access to classified information.[27] As the Snowden case illustrates, all kinds of people appear to know a lot about what government, through its computers at any rate, knows. And we don't have to go back farther than the Nixon Presidency to get a history lesson on the potential for data to be used for political purposes that make a mockery of democracy.

In sum, OTT firms have reasonably benign motives for wanting to obtain, store and analyze digital records of everything knowable in the world. They do not need to be completely competent in their predictions and yet can still add much value to the economy. They face meaningful checks and constraints on their potential misuse of everyone's data. The harm OTT firms are likely to do even in dire circumstances can be addressed by civil action and marketplace reaction.

By contrast, government's motives may be of the highest nobility, but government includes within its walls so many people that some surely harbor ill intentions on occasion or are merely clumsy in handling private information.[28] Under current rules and practices, bad government intentions are not, in the digital domain, much constrained. Nor can government be expected to predict with truly refined accuracy the bad acts intended by terrorists, or any criminals, from computer processes alone. Finally, under the current actual practices in the digital domain, checks and constraints on government misuse of data are not commensurate with the sort of harm to innocents that government action can inflict.

Now let us turn to the next category of difficulty: expense. The more data gathered by winning OTT firms, the more profits they make. The more data gathered by government, the more costs go up. There are no incoming streams of revenue to be obtained by government. Of course, if government can forfend a terrorist attack by obtaining predictions from databases, the savings measured in lives and also impact on the economy may be incalculable. A budget

---

[27] Nicholas D. Kristof, "How Could We Blow This One," *New York Times*, July 3, 2013, http://www.nytimes.com/2013/07/04/opinion/kristof-how-could-we-blow-this-one.html ("some 1.4 million people (including, until recently, Snowden) hold 'top secret' clearances.").

[28] Ezra Klein and Evan Soltas, "Wonkbook: Two Gamechanging NSA Stories You Must Read," *Washington Post*, August 16, 2013, accessed January 26, 2014, http://www.washingtonpost.com/blogs/wonkblog/wp/2013/08/16/wonkbook-two-gamechanging-nsa-stories-you-must-read (NSA broke privacy rules or overstepped legal authority thousands of time every year since 2008).

problem remains: there is no way to link the benefits of stopping crime with the cost of preventing it.

The OTT firms can be left to strike their own compromises with how much data to gather and the cost of collecting, storing and analyzing it. Typically the lines are crossed with respect to storage. OTT firms do not much need old information. When the data is old and cold, they will throw it away. Government would like to hold all information forever, because sleeper cells and clandestine agents might spend years formulating their plots. But storage is not free.

Moreover, OTT firms tend to specialize. By contrast, in government, agencies compete on the basis of gathering similar information for similar purposes. It is possible that one person running one entity will emerge as the steward of all government data; certainly General Alexander of the National Security Agency would be the leading candidate as of now. But when he retires in 2014, or when a new President arrives in 2017, there is no telling what person or agency may become the leading data analyzer. This governmental competition can provide Presidents with useful conflict in points of view and judgment. But it can lead to astonishingly expensive duplication in the digital domain.

In any event, the volume of data is growing too fast for almost any government, and perhaps even the extraordinary American government, to manage. It is said that 90 percent of all digital information was created in the last two years.[29] In the next two years, even a greater volume will swell the data centers of the world. Few if any countries can afford to keep up. Perhaps only America and China can manage the data desired for national security purposes. Then, the United States may offer allies a digital umbrella, under which any participating nation can get access to the predictive capabilities of the American security system. They will be expected to use their police forces appropriately to apprehend suspects. In a system not unlike but far less dangerous than the nuclear umbrella erected in the Cold War, the United States could become a global peacekeeper without nearly the number of boots on the ground, and without the casualties that have come from the interventions in Iraq and Afghanistan.

Nevertheless, not even the United States can afford to gather, store and analyze all digital data.[30] Private firms simply must cooperate with

---

[29] See Leslie Bradshaw, "Big Data and What It Means," *U.S. Chamber of Commerce Foundation*, May 28, 2013, accessed January 26, 2014, http://emerging.uschamber.com/library/2013/05/big-data-and-what-it-means.

[30] See Ian Welsh, "The Logic of the Surveillance State," *Ian Welsh,* June 9, 2013, accessed January 26, 2014, http://www.ianwelsh.net/the-logic-of-the-surveillance-state/ ("The problem with surveillance states...is the cost...both direct, in the resources that are required, and indirect in the lost productivity and creativity...").

government. If America is to offer its digital security capabilities to allies, then OTT firms in those allied countries also must cooperate in collecting and managing data.

At present, OTT firms are leery of being involved with government. Many of the larger OTT firms joined together in December to write a letter protesting existing government data collection.[31] But government needs that access, and the firms need governmental protection against cybersecurity threats. Therefore, the compact between OTT firms and government must be renewed, under new rules. Those who are surveilled–the people who provide the data–can seek a seat at the table in this negotiation.

Now we move to the ultimate problem: secrecy. As the late Senator Pat Moynihan wrote in his brilliant book by that name, secrecy in government is a form of regulation.[32] It is a rule that alters other rules. Specifically, secrecy impairs the rule against misuse of data and exacerbates the problem of expense.

When the government's activities in the digital domain are secret, motives and competence are not subject to beneficial scrutiny. Bad actors in government are far less likely to be sussed out when few, even in government, know who knows what about whom. The problems of inaccurate predictions and false positives are not even likely to be admitted, when secrecy precludes the problems from being discussed. No one will try to fix these problems, if wrong predictions are as likely to be acted upon as right ones; yet under conditions of secrecy that will be the case.

You might say that the agency with the data will do the checking. But everyone needs a boss to force thorough reviews from time to time. With secrecy there are not many bosses, if any. This is what various Senators have been saying for some time about the data gathering in the Executive Branch.

Secrecy also limits human judgment. If hardly anyone has sanctioned access to information, then hardly anyone can debate decisions in front of, say, the President. The individual who reports what the computers have concluded is who holds the single trump card. It may be the Queen of Spades in a game of Hearts, but secrecy does not permit anyone to know what is really on the card.

Secrecy also increases expenses in at least two ways. Agencies whose activities are largely secret from each other do not know how to

---

[31] Dan Roberts and Jemima Kiss, "Twitter, Facebook and more demand sweeping changes to US surveillance," *The Guardian*, December 9, 2013, accessed March 4, 2014, http://www.theguardian.com/world/2013/dec/09/nsa-surveillance-tech-companies-demand-sweeping-changes-to-us-laws.

[32] Daniel Patrick Moynihan, *Secrecy* (Yale, 1998), 59.

share resources, and secrecy within government also exacerbates competition among agencies. In the private sector, consumers benefit if Microsoft secretly develops a faster, better, cheaper version of an Apple product. But in government, taxpayers pay more, not less, when agencies try to outdo each other.

The ultimate detriment of secrecy is that it inspires distrust between the governed and their government. Since the founding of the United States of America, the citizens of our country have had more reason to believe in the good intentions of their government than, say, the Russians or the Chinese. But the United States was not founded on the assumption that citizens simply must trust their government. Indeed, the opposite.[33] The Constitution, especially as amended by the Bill of Rights, is very much about constraining government in order to make it trustworthy.

When Americans do not know what government knows about each person, or what it does with that knowledge, distrust will surely be on the rise. Eventually, there is a tipping point. When enough people distrust the government on enough topics for long enough a time, there is no police power that can prevent that same distrust from affecting all social and business relations in society. The country will fall apart. It has happened to other countries; it is not impossible for distrust to be the cancer that kills the American idea.

These are some, if perhaps not all, the reasons why the new rules that are emerging are not good enough for the long run of the digital era. These rules are not terrible first drafts. For example, it is probably best for private firms to gather digital information from each of us, rather than having government do it directly, as General Alexander seemed to suggest he would prefer.[34] But they are only first drafts. Here is an outline for a next draft of the governing rules of the digital domain.

Secrecy enhances both misuse and expense. Here is what should be open either to individuals or to society, as appropriate:

a. Any individual should be able to know everything that an OTT firm knows about that person. This may encourage some to opt out of OTT data collection efforts. Then, security forces can focus limited

---

[33] See Peter Shane, *Madison's Nightmare* (Chicago, 2009).

[34] See Gorman Siobhan, "NSA Chief Opens Door to Narrower Data Collection; Gen. Keith Alexander Gives Unexpected Option: Surveillance Could Target Only Terrorism-Related Data," *Wall Street Journal*, February 27, 2014, accessed April 9, 2014, http://online.wsj.com/news/articles/SB10001424052702304071004579409582715306814 for General Alexander's most recent take on possible practices for the programs.

resources on the class of opt-outs, which is more likely to include bad actors, actual or potential.

b. Any individual should be able to know whether the government has identified that person as a suspected criminal any time in the past, up to five years ago. If so identified, that individual should be able to go to a court to seek exoneration and receive a monetary payment for the intrusion on his or her privacy if there was no reasonable basis for the government's conclusion. This should constrain government excess, reduce cost, and improve trust, at least a little (as well as accuracy).

c. Everyone in society should be able to know in the abstract what the government is doing–not whose phone numbers and emails the government thinks are revealing a crime, but the fact that there are categories of such information being gathered. This will improve trust and accuracy and permit a debate about appropriate expense.

d. Everyone in society should know clearly where digital data is gathered and who in the government is using it. There should be one central data gathering agency. There must be clear accountability. Responsibility for good stewardship must lie in named people, not in "government" writ broadly and ambiguously. Those responsible for misuse of data must be held accountable.

e. The public should have access to records of all Presidential knowledge of surveillance results within five years of a presidential term ending, or 10 if need be shown to a court to keep secrets longer. This information will improve the quality of reports to the President and constrain the likelihood of inappropriate requests by the President or staff.

A bureau of declassification should constantly reduce the amount of information treated as secret. Hardly anyone should be allowed security clearances that permit access to conclusions from digital data. The second step is to institute safeguards against abuse:

a. Those who have access to conclusions from the government's digital data banks should have term limits. We do not need a digital era Hoover. Five-year terms would suffice; it is particularly important to minimize the political power of the executives running the government's digital domain by increasing the likelihood that they will not serve much longer than a Presidential term.

b. We should expand the requirement for the government to obtain warrants for obtaining certain information. The process of getting a warrant focuses the information gatherers.

c. The judiciary should have access to a standing technical oversight committee to review the methods and accuracy of government's digital domain. This sort of committee serves most expert agencies; judges should have the same sort of technical advice.

d. Individuals who have good grounds to believe they have been wronged by government misuse of data should be able to have a lawyer appointed for them to investigate what has occurred.

e. Defense lawyers should be able to examine the accuracy of what the government's digital domain concludes and predicts.

f. Government officials should face criminal sanctions for intentional misuse of data from the digital domain, and civil sanctions for unintended misuse.

g. Monetary awards should go to any individual who can prove that digital data about that person, regardless of how obtained, was misused by government or a private firm. Consequential damages should be allowed. No punitive damages or attorney's fees should be awarded.

The third step is to constrain the expense of managing the digital domain:

a. The government and the private sector should enter into an agreement of cooperation the terms of which are public.

b. The government should obtain continuous technical advice on efficient data storage and retrieval practices at use in the private sector. If government does not choose to adopt best commercial practices, it should explain its reasons to a select Congressional committee.

c. The United States should propose the creation of a global anti-terrorism cyber task force. All participating nations should contribute to defray the expense.

The rules for the digital domain must enable government to try to uncover and prevent criminal activity of all sorts, especially terrorism. At the same time the rules must balance trust between individuals on the one hand and data-gathering firms and the government on the other. To achieve this balance, the government should operate under rules that minimize secrecy, not security. We want less secrecy and greater security, not the opposite. Part of security is the protection of individuals against abuse, intentional or accidental, by data-gathering firms and the government. Every person needs to know that in the digital domain, as well as in the analog world in which the Constitution was written, the government protects the less powerful from the more powerful.

The dystopian modification of the Bill of Rights outlined above need not necessarily emerge as the prevailing jurisprudence of the digital age. Many cases have yet to be decided. The Supreme Court is still far from stitching together a coherent doctrine for the digital domain. However, it is high time for Congress to curtail the spread of secrecy in government culture. It is past time for Congress to establish safeguards against governmental abuse of digital data. Congress should not wait for the Judiciary before giving individuals the right to know what private firms and the government know about each person, and giving the public in general the right to know what sort of information in the abstract that the government is gathering. By taking these steps, Congress will assure that the Constitution continues to underpin our cherished ideals of freedom even if we find ourselves living, speaking, and being remembered in the digital domain.