.Personal Data and Government
.Dan Geer, 7 October 13, Cambridge

Thank you for the invitation to speak with you today, which, let me be clear, is me speaking as myself and not for anybody or anything else. As you know, I work the cybersecurity trade, and I am gratified that ten days ago the U.S. National Academy of Sciences, on behalf of the Department of Homeland Security, concluded that cybersecurity should be seen as an occupation and not a profession because the rate of change is too great to consider professionalization.[%] That rate of change is why cybersecurity is perhaps the most intellectually demanding occupation on the planet.

I am not yet old in chronologic years when compared to the life expectancies that obtain in the United States of 2013, but measured in Internet years I'm an ancient. Ancient-ness makes it tempting to just tell stories that begin with "In my day" which, if nothing else, proves that you are no longer in the century in which you actually belong. Stories are good, but as economist Roger Brinner so succinctly said, "The plural of anecdote is not data."

Except that maybe it, or something like it, is. In a gathering of this size you can play a game that I'll just describe rather than play. Ask for an audience volunteer willing to answer a mildly embarrassing question, something as mild as "How many pairs of never-used underwear do you own?" Then see if that volunteer will take a second question, and make it similarly mild such as "Have you ever had an evil grin while wrapping a birthday gift?" If you keep going at this game, the volunteer will become uneasy and no one will get to the proverbial "twenty questions." Why? Because the subject realizes that you are publicly triangulating them, that data fusion of even mild, innocuous questions has the effect of painting a picture. In this game, the questions cannot be mild enough to be innocuous in sum. In point of fact, the more inane the questions are, the more inane the picture painted becomes.

If you get to pick the questions and the subject is sufficiently willing to keep answering them, then you can pretty much box in your subject however you like. Politicians know that the surest way to win an argument is, as they say, to "frame the question" by which they mean painting a picture that their opposition has to work to overcome. The better practitioners at the political version of this game can impose a considerable work factor on their opponents, one that is not unlike what we here call a denial of service. Every time there is a televised debate where some self-important interlocutor asks a question that is impossible to answer succinctly, and then gives the candidate sixty seconds of airtime, painting into a corner by way of selective disclosure is what is happening.

I previously worked for a data protection company. Our product was, and I believe still is, the most thorough on the market. By "thorough" I mean the dictionary definition, "careful about doing something in an accurate and exact way." To this end, installing our product instrumented every system call on the target machine. Data did not and could not move in any sense of the word "move" without detection. Every data operation was caught and monitored. It was total surveillance data protection. Its customers were companies that don't accept half-measures. What made this product stick out was that very thoroughness, but here is the point: Unless you fully instrument your data handling, it is not possible for you to say what did not happen. With total surveillance, and total surveillance alone, it is possible to treat the absence of evidence as the evidence of absence. Only when you know everything that *did* happen with your data can you say what did *not* happen with your data.

The alternative to total surveillance of data handling is to answer more narrow questions, questions like "Can the user steal data with a USB stick?" or "Does this outbound e-mail have a Social Security Number in it?" Answering direct questions is exactly what a defensive mindset says you must do, and that is "never make the same mistake twice." In other words, if someone has lost data because of misuse of some facility on the computer, then you either disable that facility or you wrap it in some kind of perimeter. Lather, rinse, and repeat. This extends all the way to such trivial matters as timer-based screen locking.

The difficulty with the defensive mindset is that it leaves in place the fundamental strategic asymmetry of cybersecurity, namely that while the workfactor for the offender is the price of finding a new method of attack, the workfactor for the defender is the cumulative cost of forever defending against all attack methods yet discovered. Over time, the curve for the cost of finding a new attack and the curve for the cost of defending against all attacks to date cross. Once those curves cross, the offender never has to worry about being out of the money. I believe that that crossing occurred some time ago.

The total surveillance strategy is, to my mind, an offensive strategy used for defensive purposes. It says "I don't know what the opposition is going to try, so everything is forbidden unless we know it is good." In that sense, it is like whitelisting applications. Taking either the application whitelisting or the total data surveillance approach is saying "That which is not permitted is forbidden."

The essential character of a free society is this: That which is not forbidden is permitted. The essential character of an unfree society is the inverse, that which is not permitted is forbidden. The U.S. began as a free society without question; the weight of regulation, whether open or implicit, can only push it toward being unfree. Under the pressure to defend against offenders with a permanent structural advantage, defenders who opt for forbidding anything that is not expressly permitted are encouraging a computing environment that does not embody the freedom with which we are heretofore familiar.

This brings us to the larger question. No one in this room needs to be told that more and more data is collected and more and more of that data is in play. The general dynamics of change are these:

Moore's Law continues to give us two orders of magnitude in compute power per dollar per decade while storage grows at three orders of magnitude and bandwidth at four. These are top-down economic drivers. As such, the future is increasingly dense with stored data but, paradoxically, despite the massive growth of data volume, that data becomes more mobile with time.

Everyone here knows the terminology "attack surface" and knows that one of the defender's highest goals is to minimize the attack surface wherever possible. Every coder adhering to a security-cognizant software lifecycle program does this. Every company or research group engaged in static analysis of binaries does this. Every agency enforcing a need-to-know regime for data access does this. Every individual who reserves one low-limit credit card for their Internet purchases does this. I might otherwise say that any person who encrypts their e-mail to their closest counterparties does this, but because consistent e-mail encryption is so rare, encrypting one's e-mail marks it for collection and indefinite retention by those entities in a position to do so, regardless of what country you live in.

Data retention for observable data is growing by legislative fiat seemingly everywhere. The narrow logic is sound, namely if data has passed through your hands then that you retain it has no new risk for the transmitter and may contain valuable protections against malfeasance. In parallel with the game I proposed at the outset, neither you nor I would be concerned with some entity having access to one of our transmitted messages, but 1000 of them is a different story, and all-of-them forever is a different world.

I have not yet said the phrase that is the title of this talk, which is "Personal Data and Government." Perhaps you will soon see why I am slow to do so. As is frequently noted, in the United States 90+% of the critical infrastructure is in private hands. With each passing day Internet-dependent services become more essential to what I will for the moment call "normal life." As we have seen, the Government's response to the growing pervasiveness of Internet services held in private hands is deputize the owners of those services against their will. The entire imbroglio around ISPs, the NSA, and so forth and so on comes down to that -- if the government does not itself own the critical infrastructure, those that do own it can and will be compelled to become government agents. In the 21st century, we have a physical army of volunteers but a digital army of conscripts.

At the core of it all there is data. The great majority of attacks target data acquisition. The work of surveillance is, per se, targeted data acquisition. There is considerable irony in the Federal Communications Commission classifying the Internet as an information service and not a communications service insofar as while that may have been a gambit to relieve ISPs of telephone-era regulation, the value of the Internet is ever more the bits it carries, not the carriage of those bits. The FCC decisions are both several and now old, the FCC classified cable as an information service in 2002, classified DSL as an information service in 2005, classified wireless broadband as an information service in 2007, and classified broadband over power lines as an information service in 2008. A decision by the D.C. Circuit Court of Appeals on this very point is pending as we speak: Is the Internet a telecommunications service or an information service?

If I ran the zoo, I would call up the ISPs and say

> Hello, Uncle Sam here.
>
> You can charge whatever you like based on the contents of what you are carrying, but you are responsible for that content if it is illegal; inspecting brings with it a responsibility for what you learn.
> -or-
> You can enjoy common carrier protections at all times, but you can neither inspect nor act on the contents of what you are carrying and can only charge for carriage itself. Bits are bits.
>
> Choose wisely. No refunds or exchanges at this window.

We humans can design systems more complex than we can then operate. The financial sector's "flash crashes" are an example of that; perhaps the fifty interlocked insurance exchanges for Obamacare will soon be another. Above some threshold of system complexity, it is no longer possible to test, it is only possible to react to emergent behavior. Even the lowliest Internet user is involved -- one web page can easily touch scores of different domains. While writing this, the top level page from cnn.com had 400 out-references to 85 unique domains each of which is likely to be similarly constructed and all of which move data one way or another.

We have known for some time that traffic analysis is more powerful than content analysis. If I know everything about to whom you communicate including when, where, with what inter-message latency and at what length, then I know you. If all I have is the undated, unaddressed text of your messages, then I am an archaeologist, not a case officer. The soothing mendacity of proxies for the President saying "It's only metadata" relies on the ignorance of the listener.

But this is not an attack on the business of intelligence. The Intelligence Community is operating under the rules it knows, most of which you, too, know, and the goal states it has been tasked to achieve. The center of gravity for policy is those goal states.

We all know the truism, that knowledge is power. We all know that there is a subtle yet important distinction between information and knowledge. We all know that a negative declaration like "X did not happen" can only proven true if you have the enumeration of *everything* that did happen and can show that X is not in it. We all know that when a President says "Never again" he is asking for the kind of outcome for which proving a negative, lots of negatives, is categorically essential. Proving a negative requires omniscience. Omniscience requires god-like powers.

Perhaps the point is that the more technologic the society becomes, the greater the dynamic range of possible failures. When you live in a cave, starvation, predators, disease, and lightning are about the full range of failures that end life as you know it and you are well familiar with all of them. When you live in a technologic society where everybody and everything is optimized in some way akin to just-in-time delivery, the dynamic range of failures is incomprehensibly larger and largely incomprehensible. The wider the dynamic range of failure, the more prevention is the watchword. Cadres of people charged with defending masses of other people must focus on prevention, and prevention is all about proving negatives. Therefore, one must conclude that as technologic society grows more interdependent within itself, the more it must rely on prediction based on data collected in broad ways, not targeted ways.

Spoken of in this manner, intelligence agencies that hoover up everything are reacting rationally to the demand that they ensure "Never again" comes true. Not only that, the more complex the society they are charged with protecting becomes, the more they must surveil, the more they must analyze, the more data fusion becomes their only focus.

Part of the picture is that it is categorically true that technology is today far more democratically available than it was yesterday and less than it will be tomorrow. 3D printing, the whole "maker" community, DIY biology, micro-drones, constant contact with whomever you choose to be in constant contact with -- these are all examples of democratizing technology. This is perhaps our last fundamental tradeoff before the Singularity occurs: Do we, as a society, want the comfort and convenience of increasingly technologic, invisible digital integration enough to pay for those benefits with the liberties that must be given up to be protected from the downsides of that integration?

This is not a Chicken Little talk, it is an attempt to preserve if not make a choice while choice is still relevant. We are ever more a service economy, but every time an existing service disappears into the cloud, our vulnerability to its absence increases. Every time we ask the government to provide goodnesses that can only be done with more data, we are asking government to collect more data. Let me ask a yesterday question: How do you feel about traffic jam detection based on the handoff rate between cell towers of those cell phones in use in cars on the road? Let me ask a today question: How do you feel about auto insurance that is priced from a daily readout of your automobile's black box? Let me ask a tomorrow question: In what calendar year will compulsory auto insurance be more expensive for the driver who insists on driving their car themselves rather than letting a robot do it? How do you feel about public health surveillance done by requiring Google and Bing to report on searches for cold remedies and the like? How do you feel about a Smart Grid that reduces your power costs but reports minute-by-minute what is on and what is off in your home? Have you or would you install that toilet that does a urinalysis with every use?

How do you feel about using standoff biometrics as a solution to authentication? At this moment in time, facial recognition is possible at 500 meters, iris recognition is possible at 50 meters, and heart-beat recognition is possible at 5 meters. Your dog can identify you by smell; so, too, can an electronic dog's nose. Your cell phone's accelerometer is plenty sensitive enough to identify you by gait analysis. There are 3+ billion new photos online each month, and even if you've never uploaded photos of yourself someone else has. All of these are data dependent, cheap, convenient, and none of them reveal anything that is a secret as we currently understand the term "secret" yet the sum of them is greater than the parts.

Everyone in this room knows how and why passwords are a problem. At the same time, passwords may be flatly essential for a reason that requires I read a paragraph from Marcia Hofmann's September 12th piece in Wired[*]

> If the police try to force you to divulge the combination to a wall safe, your response would reveal the contents of your mind and so would implicate the Fifth Amendment. (If you've written down the combination on a piece of paper and the police demand that you give it to them, that may be a different story.)
>
> To invoke Fifth Amendment protection, there may be a difference between things we have or are -- and things we know. The important feature about PINs and passwords is that they're generally something we know. These memory-based authenticators are the type of fact that benefit from strong Fifth Amendment protection should the government try to make us turn them over against our will. Indeed, last year a federal appeals court held that a man could not be forced by the government to decrypt data.
>
> But if we move toward authentication systems based solely on physical tokens or biometrics -- things we have or things we are, rather than things we remember -- the government could demand that we produce them without implicating anything we know. Which would make it less likely that a valid privilege against self-incrimination would apply.

As Hofmann notes, a Court could find otherwise and set a different precedent, but her analysis is cautionary. Perhaps a balance of power requires the individual actually does have some secrets. But is having some secrets the same as having some privacy?

No society, no people need rules against things which are impossible. Today I observe a couple fornicating on a roof top in circumstances where I can never know who the couple are. Do they have privacy? The answer is "no" if your definition of privacy is the absence of observability. The answer is "yes" if your definition of privacy is the absence of identifiability.

Technical progress in image acquisition guarantees observability pretty much everywhere now. Those standoff biometrics are delivering multi-factor identifiability at ever greater distances. We will soon live in a society where identity is not an assertion like "My name is Dan," but rather an observable like "Sensors confirm that is Dan." With enough sensors, concentration camps don't need to tatoo their inmates. How many sensors are we installing in normal life?

If data kills both privacy as impossible-to-observe and privacy as impossible-to-identify, then what might be an alternative? If you are an optimist or an apparatchik, then your answer will tend toward rules of procedure administered by a government you trust or control. If you are a pessimist or a hacker/maker, then your answer will tend towards the operational, and your definition of a state of privacy will be mine: the effective capacity to misrepresent yourself.

Misrepresentation is using disinformation to frustrate data fusion on the part of whomever it is that is watching you. Misrepresentation means paying your therapist in cash under an assumed name. Misrepresentation means arming yourself not at Walmart but in living rooms. Misrepresentation means swapping affinity cards at random with like-minded folks. Misrepresentation means keeping an inventory of misconfigured webservers to proxy through. Misrepresentation means putting a motor-generator between you and the Smart Grid. Misrepresentation means using Tor for no reason at all. Misrepresentation means hiding in plain sight when there is nowhere else to hide. Misrepresentation means having not one digital identity that you cherish, burnish, and protect, but having as many as you can. Your identity is not a question unless you work to make it be.

The Obama administration's issuance of a National Strategy for Trusted Identities in Cyberspace is case-in-point; it "calls for the development of interoperable technology standards and policies -- an 'Identity Ecosystem' -- where individuals, organizations, and underlying infrastructure -- such as routers and servers -- can be authoritatively authenticated." If you can trust a digital identity, that is because it can't be faked. Why does the government care about this? It cares because it wants to digitally deliver government services. Is having a non-fake-able digital identity for government services worth the registration of your remaining secrets with that government? Is there any real difference between a system that permits easy, secure, identity-based services and a surveillance system? Do you trust those who hold surveillance data on you over the long haul by which I mean the indefinite retention of transactional data between government services and you, the individual required to proffer a non-fake-able identity to engage in those transactions? If you are building authentication systems today, then you have to play in this league.

Standoff biometry by itself terminates the argument over whether security and privacy are a zero sum game -- the sum is nowhere near that good, and it is the surveilled who are capitalizing the system. As with my game, entirely innocuous things become problematic when surveilled. Shoshana Zuboff, Harvard Business School Emerita, called this "anticipatory conformity" and said:

> [W]e anticipate surveillance and we conform, and we do that with

> awareness. We know, for example, when we're going through the security line at the airport not to make jokes about terrorists or we'll get nailed, and nobody wants to get nailed for cracking a joke. It's within our awareness to self-censor. And that self-censorship represents a diminution of our freedom. We self-censor not only to follow the rules, but also to avoid the shame of being publicly singled out. Once anticipatory conformity becomes second nature, it becomes progressively easier for people to adapt to new impositions on their privacy, their freedoms. The habit has been set.

Leonard Downie, the former executive editor of The Washington Post, wrote in that very paper on October 4th:

> Many reporters covering national security and government policy in Washington these days are taking precautions to keep their sources from becoming casualties in the Obama administration's war on leaks. They and their remaining government sources often avoid telephone conversations and e-mail exchanges, arranging furtive one-on-one meetings instead. A few news organizations have even set up separate computer networks and safe rooms for journalists trained in encryption and other ways to thwart surveillance.[&]

Once again, this is all about data and, to the exact point, about fused data from many sources. Do you like it? Do you not like it? All you engineers know that for the engineer, it is "fast, cheap, reliable: choose two." I am here to argue that for policy makers working the cybersecurity beat, it is "freedom, security, convenience: choose two." But so long as policy makers in a democracy eventually come around to the people's desires, my argument, such as it is, is with the public at large, not with those who are trying to deliver failure-proof protection to an impatient, risk-averse, gadget-addicted population.

We learned in the financial crisis that there are levels of achievable financial return that require levels of unsustainable financial risk. We learned that lesson on the large scale and on the small, on the national scale and on the personal one. I would like us to not have to learn the parallel lesson with respect to data that powers the good versus data that powers the bad. If we can, for the moment, think of data as a kind of money, then investing too much our own data in an institution too big to influence is just as insensate as investing too much of our own money in an institution too big to fail.

I have become convinced that all security tools and all the data that they acquire are, as they say in the military, dual use -- the security tools and their data can be used for good or for ill. I am similarly convinced that the root cause, the wellspring of risk is dependence, especially dependence on expectations of system state. If you would accept that you are most at risk from the things you most depend upon, then damping dependence is the cheapest, most straightforward, lowest latency way to damp risk. This is, in further analogy, just like the proven fact that the fastest and most reliable way to put more money on the bottom line is through cost control. John Gilmore famously said, "Never give a government a power you wouldn't want a despot to have." I might amend that to read "Never demand the government have a power you wouldn't want a despot to have."

I have also become convinced that a state of security is one in which there is no unmitigatable surprise, that is to say that you have reached a state of security when you can mitigate the surprises you will face. Note that I did not say a state of security is the absence of surprise, but rather the absence of unmitigatable surprise. California Senate Bill 1386, the first of the state-level data breach laws, did not criminalize losing credit card data; rather, it prescribed the actions that a firm which has lost the credit card data of its customers must take. SB1386 is wise in that regard.

But only rarely do we ask our Legislatures to make mitigation effective. Instead, over and over again we ask our Legislatures to make failure impossible. When you embark on making failure impossible, and that includes delivering on statements like "Never again," you are forced into cost-benefit analyses where at least one of the variables is infinite. It is not heartless to say that if every human life is actually priceless, then it follows that there will never be enough money. One is not anti-government to say that doing a good job at preventing terrorism is better than doing a perfect job.

And there is the Gordian Knot of this discussion: As society becomes more technologic, even the mundane comes to depend on distant digital perfection. Our food pipeline contains less than a week's supply, just to take one example, and that pipeline depends on digital services for everything from GPS driven tractors to robot vegetable sorting machinery to coast-to-coast logistics to RFID-tagged livestock. Is all the technologic dependency and the data that fuels it making us more resilient or more fragile?

In cybersecurity practice, in which most of us here work, we seem to be getting better and better. We have better tools, we have better understood practices, and we have more colleagues. That's the plus side. But I'm interested in the ratio of skill to challenge, and as far as I can estimate, we are expanding the society-wide attack surface faster than we are expanding our collection of tools, practices, and colleagues. If you are growing more food, that's great. If your population is growing faster than your improvements in food production can keep up, that's bad. As with most decision making under uncertainty, statistics have a role, particularly ratio statistics that magnify trends so that the latency of feedback from policy changes is more quickly clear. Yet statistics, too, require data.

In medicine, we have well established rules about medical privacy. Those rules are helpful. Those rules also have holes big enough to drive a truck through. Regardless, when you check into the hospital there is an accountability-based, need-to-know regime that governs your data most days. However, if you check in with Bubonic

Plague or Anthrax, you will have zero privacy as those are mandatory data reporting conditions. So I ask you, would it make sense in a public health of the Internet way to have a mandatory reporting regime for cybersecurity failures? Do you favor having to report penetrations of your firm or household to the government or face criminal charges for failing to make that report? Is that data that you want to share? Sharing it can only harm you. It might help others.

This is not, in fact, about you personally. Even Julian Assange, in his book _Cypherpunks_, said "Individual targeting is not the threat." It is about a culture where personal data is increasingly public data, and assembled en masse. All we have to go on now is the hopeful phrase "A reasonable expectation of privacy" but what is reasonable when one inch block letters can be read from orbit? What is reasonable when all of your financial or medical life is digitized and available primarily over the Internet? Do you want ISPs to retain e-mails when you are asking your doctor a medical question (or, for that matter, do you want those e-mails to become part of your Electronic Health Record)? Who owns your medical data anyway? Until the 1970s, it was the patient but regulations then made it the provider. With an Electronic Health Record, it is likely to revert to patient ownership but if the EHR belongs to you, do you get to surveil the use that is made of it by medical providers and those that they outsource to? And if not, why not?

Observability is fast extending to devices. Some of it has already appeared, such as the fact that any newish car is broadcasting four unique Bluetooth radio IDs, one for each tire's valve stem. Some of it is in a daily progression, such as training our youngsters to accept surveillance by stuffing a locator beacon in their backpack as soon as they go off to Kindergarten. Some of it is newly technologic, like through the wall imaging, and some of it is simply that we are now surrounded by cameras that we can't even see where no one camera is important but they are important in the aggregate when their data is fused. Anything that has "wireless" in its name creates an opportunity for traffic analysis.

In the days of radio, there was Sarnoff's Law, namely that the value of a broadcast network was proportional to N, the number of listeners. Then came packetized network communications and Metcalfe's Law, that the value of a network was proportional to N squared, the number of possible two-way conversations. We are now in the era of Reed's Law where the value of a network is proportional to the number of groups that can form in it, that is to say 2 to the power N. Reed's Law is the new reality because it fits the age of social networks. In tune with my claim that everything is dual use, any entity (such as a government) that can acquire the entirety of all social media transactions learns nearly everything there is to learn, and all in one place, and all courtesy of the participants themselves. The growth of social networks is a surveiller's dream come true.

Total system complexity from a security person's point of view is essentially just geometry. Security is non-composable -- we can get insecure results even when our systems are assembled from secure components. The more components, the less likely a secure result. Might the same be said of data? Of course it can -- search for the term "reidentification" and you'll find that incomplete data, even intentionally anonymized data, can be put together if there is enough of it, and what is enough seems to be a lower hurdle every year. Put differently, if you share one fact each with ten different people, how many of the ten have to be compromised before you are exposed?

Howard Brin was the first to suggest that if you lose control over what data is collected on you, the only freedom-preserving alternative is that if everyone else does, too. If the government or the corporation can surveil you without asking, then the balance of power is preserved when you can surveil them without asking. Bruce Schneier countered that preserving the balance of power doesn't mean much if the effect of new information is non-linear, that is to say if new information is the exponent in an equation, not one more factor in a linear sum.[#] Solving that debate requires you have a strong opinion on what data fusion means operationally to you, to others, to society.

There is some axiom of nature at work here. Decision making under uncertainty is what we do in the small, and what policy makers do in the large. Uncertainty is partial information, so it is natural to want information that is less partial. We are closing in on having more information than we can use. The Intelligence Community has felt the heat of too much information to handle for some time. The business community is feeling it now insofar as it is far cheaper to keep everything than it is to do careful selective deletion. The individual is feeling pretty warm, too, as evidenced by something as simple as how much they depend on the ability to search their e-mail rather than folderizing it after reading.

I have amassed all the fortune I am going to amass. I have raised all the children I am going to raise. I have made all the commitments I am going to make. I am old enough that I can opt out of many of the corporate data collection schemes and live out the remainder of my days unaffected by what I might be missing out on. That those corporations are agents of government data collection means that for now I am opting out of some of that as well. Anyone under 40 has no such option, or at least no such easy option. Everything I am talking about here is a young person's problem, just like the National Debt, which the young will soon inherit. It is your choice and responsibility whether to demand protections and conveniences and services that can only be done with pervasive data. It is your choice and responsibility whether to fear only fear itself or to fear the absence of fear. It is your choice and responsibility to be part of the problem or part of the solution.

Any finite tolerance for risk caps the amount of information you will want in play. This has nothing whatsoever to do with whether you have anything to hide, and therefore it is your choice and responsibility to make it understood that just as "..there is nothing sinister in so arranging one's affairs as to [minimize] taxes" [$]

neither is there anything sinister in minimizing the data collectible from you. The price of freedom is the probability of crime. But as technology progresses, your choice will not be between Big Brother or no Big Brother, rather it is already between one Big Brother and lots of Little Brothers. Think carefully, yours is the last generation that will have a choice.

As Dylan Thomas wrote, "Do not go gentle into that good night// Rage, rage against the dying of the light."

Thank you for hearing me out.

[%] Professionalizing the Nation's Cyber Workforce?
http://www.nap.edu/openbook.php?record_id=18446

[*]
http://www.wired.com/opinion/2013/09/the-unexpected-result-of-fingerprint-authentication-that-you-cant-take-the-fifth

[&]
http://www.washingtonpost.com/opinions/in-obamas-war-on-leaks-reporters-fight-back/2013/10/04/70231e1c-2aeb-11e3-b139-029811dbb57f_print.html

[#]
http://www.wired.com/politics/security/commentary/securitymatters/2008/03/securitymatters_0306
http://www.wired.com/politics/security/news/2008/03/brin_rebuttal

[$] Judge Learned Hand, Commissioner v. Newman, 1947