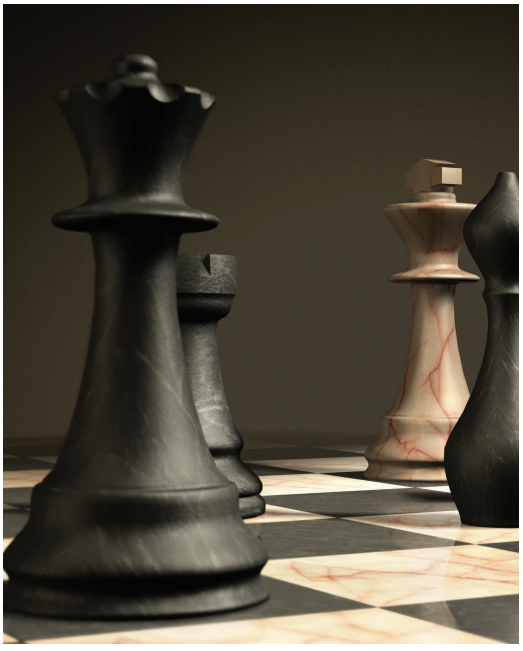

Moral Hazards, Negative Externalities, and the Surveillance Economy

Hal Berghel, *University of Nevada, Las Vegas*

Modern economics includes the art of making common sense abstruse. Terms like *moral hazard* and *negative externality* both describe states of transactional imbalance. And this imbalance isn't limited to economics. When governments are involved, even digital technology can be threatening

Pedantic economists might explain *moral hazard* in terms of information imbalances and the like, but don't be fooled. The meaning is much simpler.

A classic illustration of moral hazard's role can be found in the passage of the Depression-era Glass-Steagall Act, which separated investment from commercial banking and provided that commercial banking deposits would be insured to assuage depositors and avoid bank runs. With the passing of Glass–Steagall, Congress allowed commercial banks to transfer their major risk to the government. To make this increased risk /palatable to the public, Congress insisted that commercial banks be heavily regulated.

Flash forward to 1999 when commercial banking interests convinced Congress to overturn Glass–Steagall through the passage of the Gramm–Leach–Bliley Act, which deregulated commercial banking. From that point on, commercial banking couldn't get enough of risky investments: collateralized debt obligations, derivatives, junk bonds—you name it. But the deposit insurance remained unchanged from Glass–Steagall. As David Stockman put it in his recent book *The Great Deformation*, all that was left after GLB was naked moral hazard. The moral hazards were largely kept hidden from the public until the financial meltdown of 2007 – the first major *negative externality* of GLB.

Where moral hazard is shorthand for offloading risk, negative externalities is shorthand for getting someone else to pick up the tab for the collateral damage. The superfund cleanup sites are examples of negative externalities of commerce where the taxpayer foots the bill for undoing the damage caused by profit-makers. In a quest for symmetry, economists have developed elaborate models that explain costs in terms of negative and positive externalities, but this is a ruse. Negative externalities are real and consequential, whereas the positive externalities are usually contrived, infrequent, and trivial.

ENTER THE SURVEILLANCE ERA

The 1975–1976 Congressional hearings into domestic surveillance by Senator Frank Church, Representative Otis Pike, and Representative Bella Abzug were an attempt to address the moral hazards and

0018-9162/14/$31.00 © 2014 IEEE Published by the IEEE Computer Society

negative externalities created by government surveillance.

President Gerald Ford tried unsuccessfully to distract Congress from investigating the government intelligence community with his creation of the Rockefeller Commission in 1975 after Seymour Hersh's revelations in *The New York Times* about the domestic surveillance of the antiwar, minority rights, and women's liberation movements by the CIA. Operation CHAOS disabused Congress from deferring to executive privilege and prompted investigations in the House (Pike) and Senate (Church) Intelligence Committees, as well as Bella Abzug's House Subcommittee on Government Information and Individual Rights. Although initially targeting the CIA, these investigations quickly led to an examination of the NSA's domestic surveillance activities—exactly what the Ford administration and the Rockefeller Commission wanted to avoid.

Committee testimonies by CIA Director William Colby and NSA Director Lew Allen gave up some of the "family jewels," like Operation Shamrock's domestic surveillance program, Project Minaret's watch lists of US citizens, and the FBI's COINTELPRO operation to subvert political dissent. By the time Bella Abzug's committee heard testimony from telephone and telegraph company executives, the true extent of the illegal surveillance became clear. This motivated the Foreign Surveillance Intelligence Act (FISA) introduced by Senator Edward Kennedy and signed into law by President Carter in October 1978.

There we have it. The intelligence community's surveillance and efforts to discredit political dissenters was a negative externality – it cost the government credibility and the taxpayer resources for Congressional involvement. that began as legitimate government intelligence gathering. However, the inclusion of Jane Fonda, Dr. Benjamin Spock, and Martin Luther King, Jr., in the sweep went a step too far for Congress. Because of inadequate oversight, the intelligence agencies were found to be using public funds for political ends—the moral hazard.

There was no penalty for constitutional abuses by the intelligence agencies. Congress introduced FISA to restore a sense of balance, but it was always a fragile creature of compromise that could only work in the context of strict "minimization" and a self-constrained intelligence community. Its partisan nature—since its inception, the FISA justices have all been appointed by conservative Supreme Court Chief Justices (Burger, Rehnquist, and Roberts)—and the fact that deliberations were always ex parte (only the government was allowed to participate), made it vulnerable to pro-government bias and invited constitutional abuse. Still, it did tend to prevent some egregious abuses until 2001, when legislation such as the USA PATRIOT Act rendered it all but impotent.

The USA PATRIOT Act and related legislation left behind naked moral hazard in intelligence gathering, just as GLB did for banking.

A moral hazard is an environment in which the benefits and risks are disproportionately distributed among participants—one side gets the reward and the other gets the risk. It's just that simple. Any school child will tell you that moral hazards are inherently unfair. But, in the world of politicians, business lobbyists, PACs, and the like, moral hazards are a camoufleur's coin of the realm.

JUDICIAL CONFUSION

In a judicial surprise, conservative District Court Judge Richard Leon's opinion (*Klayman v. Obama*) ruled on 16 December 2013 that the NSA's harvesting of metadata might violate the Fourth Amendment (https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2013cv0851-48). The provocative part of the opinion begins on page 35, challenging the relevance of the 1979 Supreme Court decision (*Smith v. Maryland*) to the NSA's Bulk Telephony Metadata collection, because the latter is far more expansive than anything anticipated in the *Smith* decision. Leon's opinion likens the NSA surveillance capabilities to an "almost Orwellian technology" (p. 49). Leon then asserts "the Government does *not* cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature" (p. 61). In other words, Leon agrees with the civil libertarians whose position is that the NSA bulk metadata surveillance program accomplished little at an enormous cost in loss of civil liberties. Hold that thought.

On 27 December 2013, federal judge William H. Pauley dealt with the same issue in *ACLU v. Clapper* (https://www.aclu.org/files/assets/order_granting_governments_motion_to_dismiss_and_denying_aclu_motion_for_preliminary_injunction.pdf). What a difference a week makes.

Pauley is convinced that the metadata program is

constitutionally valid, and that the plaintiffs haven't made a statutory argument that their rights were violated because Congress specifically blocked the opportunity to make such claims by precluding all citizens from participation in the FISA process in the first place. The government, according to Pauley, had sovereign immunity (p. 21ff).

Further, Pauley disagrees with Leon regarding the relevance of *Smith*. The volume of data and nature of the technology is irrelevant according to Pauley (p. 44). Moreover, Pauley accepts government claims that the bulk telephony metadata collection is effective at face value (p. 50). And, he argues, even if there were less intrusive means to achieve the same results, that wouldn't matter (p 41), for the government is under no obligation to use it. Pauley also reaffirms that under *Smith*, "when a person voluntarily conveys information to a third party, he forfeits his right to privacy in the information…. The collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search" (p. 42).

But the clincher is Pauley's claim that the executive power of the President "reaches its zenith when wielded to protect national security (p. 48)…. The right to be free from searches and seizures is fundamental, but not absolute" (p. 51). This wording is reminiscent of the divine right of kings. So on Pauley's account, FISA targets have no Constitutional rights, and the government's claims on the value of surveillance programs are sufficient to justify them (pp. 48–49).

I can't speak to the validity of Pauley's legal reasoning, but his narrative is inconsistent with the historical record. For example, he claims that "There is no evidence that the government has used any of the bulk telephony metadata it collected for any purpose other than investigating and disrupting terrorist attacks," (pp. 50–51), where contradictory evidence has been widely reported in the media throughout 2012 and 2013. For example, Reuters correspondents John Shiffman and Kristina Cooke published an investigation on the NSA's distribution of extrajudicial information to the US Drug Enforcement Agency (DEA) for purposes of criminal prosecutions that have nothing at all to do with national security (www.theguardian.com/world/2013/aug/05/secret-dea-unit-surveillance-authorities).

Equally troubling is Pauley's claim that the bulk metadata program might have permitted the NSA to notify the FBI that 9/11 terrorists were living in San Diego. According to journalist James Bamford (*A Pretext for War*, Anchor Publishing, 2004), the leading chronicler of the NSA, the CIA and NSA were aware of the terrorists in San Diego before 9/11, but didn't notify the FBI. Ironically, the terrorists were actually living in a room rented to them by an FBI informant (pp. 229–231)! According to Bamford, the breakdown wasn't technical, it was procedural. Pauley later cites unsupported government claims as definitive evidence of bulk metadata effectiveness (pp. 48–49).

So there you have it, judicial confusion: Leon and the civil libertarians versus Pauley and the government intelligence community. It should be noted that abuses of civil liberties were anticipated by Senator Russ Feingold at the very time the USA PATRIOT Act was debated in the Senate in 2001 (https://epic.org/privacy/terrorism/usapatriot/feingold.html). Recently, several members of Congress have indicated that the executive branch misled Congress on the matter of legal interpretations of the USA PATRIOT Act. Pauley responded to this in his decision as well: Congressional ignorance of the law is no excuse (p. 31ff). This was after he ruled in an earlier case that Congress isn't entitled to see relevant classified reports regarding Executive interpretation. (see the footnote on p. 31). Congress would have been well served by listening to Feingold.

THE REPORT

Prior to the judicial opinions, on 12 December 2013 the Obama administration released the report entitled "Liberty and Security in a Changing World" (www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf). The bad news, from the civil libertarian perspective, is that it calls for no substantive changes to current policy. The good news is that if any or all of the recommended changes are made, we shouldn't be much worse off than we are.

The presence of illogic in the Presidential Report is likely due to the fact that the committee members were lawyers and political insiders—careers in which illogic bears little if any penalty, and in some circles, is highly sought after.

It would be a mistake of the first order to assume that this report is an objective, independent, unbiased review of the NSA policies, as the committee members were political friends of President Obama. Given the President's strong support for the NSA surveillance programs, he could be expected to avoid selection of anyone who might wander off page.

REPORT RECOMMENDATIONS

The report focuses on minor tactical modifications geared more toward palliation than reform. Consider the following recommendations.

Palliation

- Recommendation 1: amend section 215 to broaden the discretion of the government on what constitutes "reasonable" surveillance. This doesn't look good.
- Recommendation 5: insist that telephony metadata be retained by the ISP or other third-party private providers. This falls under the "big whoop" category, as it proposes third party digital sumps to deflect public wrath from the NSA. I would call your attention to the fact that third- party private contractors are subject to even less oversight than the government!
- Recommendation 8: section 215 and National Security Letter gag orders be limited to 180 days without judicial re-approval, and never be issued in a manner that prevents the recipient from receiving legal counsel. Not a bad idea, until you read the caveats, recommendations 9 and 10, that limit accountability to programs that are unclassified, and even then only when the government decides that the disclosure would not endanger national security. This gives the government the second bite of the apple: first they can over-classify a program, and if the public gets wind of it, they can seek confidentiality under the national security rubric.
- Recommendation 11: this one says the American public may be kept in the dark about large surveillance programs ("of the magnitude of section 215 bulk telephony meta-data program") only when it's in the government's interest to do so. Boy that's a game changer!

You can see where this is going. Recommended changes tend toward the cosmetic. Through it all, page after page, any mention of judicial oversight remains ex parte, and suggestions for congressional reforms are strategically inert.

More minor changes

A few progressive changes appear under Organizational Reforms, highlights of these are described below.

- Recommendation 22 calls for Senate confirmation of the Director of the NSA rather than the current Presidential appointment. I can see no downside to this idea. I can also see no major upside to this idea given the dysfunctional state of Congress. It also suggests that civilians be eligible to hold this position. No news there. That idea was anticipated by the Brownell Commission at the time the NSA was created in 1952: "If, as things develop, it should ultimately appear that a civilian could better qualify for the position, it is strongly recommended that no sense of tradition or vested military interest be allowed to stand in the way of his appointment." (James Bamford, Puzzle Palace, Penguin Books, 1983, p. 79). Limiting this position to a 3-star officer or above was never required by law, it was required by Presidents so they could maintain tighter control over the agency. If this recommendation is accepted, expect Senate confirmation along party lines.
- Recommendation 24 proposes that the head of the military US Cyber Command not be the same individual as the Director of the NSA. (Note that 24 is a consequence of 22 if the DIRNSA is a civilian.) This is a good idea. The present arrangement creates excessive concentrations of power in one government official.
- Recommendation 26 creates a privacy and civil liberties policy official—not surprisingly, a political appointee (cut from the same bolt as the members of the committee).
- Recommendation 27 proposes a new Civil Liberties and Privacy Protection Board, albeit from the same Executive Branch insiders that inhabit the present privacy board, PCLOB. Similarly, there is a provision for an "authorized recipient for whistleblower complaints relating to privacy and civil liberties concerns from employees in the Intelligence Community." However, there is no provision for any oversight, transparency, or objectivity in this review. The only people in the room will be government insiders—no defense attorneys, no civil libertarian lawyers, just insiders operating under the cloak of secrecy. I would be remiss if I failed to point out that NSA whistleblowers William Binney, J. Kirk Wiebe, Ed Loomis, and Thomas Drake used appropriate internal channels to bring attention to the NSA mismanagement and potential Fourth Amendment abuses without effect. There is no point in creating a whistleblower-recipient unless (a) the person is incentivized to act independently, (b) there is external accountability to impartial, objective, non-government interests, and (c) the recipient is held accountable by the Congress and the Courts.
- Recommendation 28 is uninspired except for section (4) that suggests (finally) making the FISA court less partisan by distributing the appointment power among all Supreme Court Justices. Certainly an improvement.

The report concludes with technical recommendations. Recommendation 29 recommends that the government do nothing to "subvert, undermine, weaken, or make vulnerable generally available commercial software." And here we thought that was obvious!

The report is not without strengths, such as its emphasis on multiplicity of risks (p. 46) and that the Bill of Rights isn't subject to "balancing" against competing government interests (p. 49). But the repeated appearance of informal fallacies detracts from its value. On page 75, for example, in response to criticism that the NSA surveillance is both indiscriminate and pervasive, the report responds, "NSA focuses on collecting foreign intelligence information that is relevant to protecting the national security of the United States and its allies." This is a textbook case of question begging. What the NSA "focuses on" is precisely the issue in question. Saying that the NSA does no wrong because what the NSA does is right is semantically, if not viciously, circular. The very next sentence is, "Moreover, what the NSA collects is shared with governments of many other nations for the purpose of enhancing their national security and the personal security of their citizens." Here, the fallacy of irrelevance rears its ugly head. We'll pass over the remaining bulk illogic in silence, in search of substance.

Another deficiency of the report is that it focuses on minor tactical modifications that might make the programs more acceptable to an alarmed public. This report is better understood as palliation than reform (see the "Report Recommendations" sidebar).

The report's authors claim that they're "unaware of any vulnerability created by the US Government…" (p. 217). The timing of these remarks is interesting given recent revelations about the TAO project (www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html) and the Reuters report that the NSA paid RSA to embed a flawed random number generator in its encryption software (www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220) to make it easier to break. Ars Technica subsequently ran a story that suggests that the cochair of the Internet Engineering Task Force (IETF) cryptography panel was an NSA mole instrumental in ensuring that the NSA has a backdoor to common security products (http://arstechnica.com/security/2013/12/critics-nsa-agent-co-chairing-key-crypto-standards-body-should-be-removed). And just when we thought we had the NSA Clipper Chip behind us!

There are several recommendations to review the process of issuing and maintaining security clearances, which looks like a good idea. At this point, over 1 percent of the US population has a clearance—probably way beyond the limits of prudence. The suggested employment of a "work-related access" model is also a welcome idea, although the problem was never in the security model but rather in enforcement and accountability (see this column, March 2012).

As expected from the membership of the committee, this report falls in the Shakespearean category of much ado about nothing. Though it doesn't accomplish much, it doesn't seem to do much harm either, and that's a good thing.

Noteworthy moral hazards are much harder to detect and less likely to inflame than noteworthy in-your-face negative externalities. The 2007 collapse of the financial sector didn't escape anyone's attention, but the causal connection with the passage of Gramm–Leach–Bliley Act is still actively denied by those who benefitted from its passage. Similarly, the world took note of the NSA's interception of Angela Merkel's phone calls, but few seem willing to draw the connection between it and such draconian legislation as the USA PATRIOT Act, the Protect America Act of 2007, and the FISA Amendments Act of 2008.

Privacy and civil rights abuses and a fear of Orwellian totalitarianism incite some people (Chelsea Manning and Edward Snowden, to name two) to take drastic measures. The most effective way to deal with these consequences is to call attention to the antecedent moral hazards, and bring them in line with public expectations of civil liberties.

Hal Berghel, *Out of Band column editor, is a professor of computer science at the University of Nevada, Las Vegas, where he is the director of the Identity Theft and Financial Fraud Research and Operations Center (http://itffroc.org)/ Contact him at hlb@computer.org.*