

*An Independent Socialist Magazine Founded in 1949.*

LEO HUBERMAN, *EDITOR, 1949-1968* ♦ PAUL M. SWEETZ, *EDITOR, 1949-2004* ♦ HARRY MAGDOFF, *EDITOR, 1969-2006*

JOHN BELLAMY FOSTER, *EDITOR* ♦ MICHAEL D. YATES, *ASSOCIATE EDITOR* ♦ R. JAMIL JONNA, *ASSOCIATE EDITOR, TECHNOLOGY*  
SPENCER SUNSHINE, *ASSISTANT EDITOR* ♦ YOSHIE FURUHASHI, *MRZINE EDITOR* ♦ SUSIE DAY, *CIRCULATION* ♦ MARTIN PADDIO, *BUSINESS MANAGER*

ELLEN MEIKSINS WOOD (1997-2000) and ROBERT W. MCCHESENEY (2000-2004), *FORMER EDITORS*

146 WEST 29TH ST., SUITE 6W  
NEW YORK, NY 10001

TEL: 212-691-2555; FAX: 212-727-3676

EDITORIAL: [mrmag@monthlyreview.org](mailto:mrmag@monthlyreview.org)

CIRCULATION: [mrs@monthlyreview.org](mailto:mrs@monthlyreview.org)

MRZINE: [mrzine@monthlyreview.org](mailto:mrzine@monthlyreview.org)

<b>OVERVIEW</b> Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age JOHN BELLAMY FOSTER AND ROBERT W. MCCHESENEY	1
Electronic Communications Surveillance LAUREN REGAN	32
The New Surveillance Normal: NSA and Corporate Surveillance in the Age of Global Capitalism DAVID H. PRICE	43
The Zombie Bill: The Corporate Security Campaign That Would Not Die BEATRICE EDWARDS	54
Surveillance and Scandal: Weapons in an Emerging Array for U.S. Global Power ALFRED W. MCCOY	70
“We’re Profiteers”: How Military Contractors Reap Billions from U.S. Military Bases Overseas DAVID VINE	82
U.S. Control of the Internet: Problems Facing the Movement to International Governance PRABIR PURKAYASTHA AND RISHAB BAILEY	103
Merging the Law of War with Criminal Law: France and the United States JEAN-CLAUDE PAYE	128
The National Security State: The End of Separation of Powers MICHAEL E. TIGAR	136

---

### Notes from the Editors

Allusions to Marx seem to be emanating from all points of the political compass these days in the context of the current political-economic crisis of capitalism, reflecting the remarkable resurgence of both Marxism and anti-Marxism. What is especially notable in this respect is the extent to which such allusions have come to focus on the saying, “from each according to his ability, to each according to his needs”—usually identified with Marx’s famous 1875 *Critique of the Gotha Programme*. Conservatives frequently quote “from each according to his ability” (ignoring the rest of the saying) and use it as a kind of code phrase for “Marxism” to attack all progressive measures. Thus U.S. Supreme Court Justice Antonio Scalia’s dissenting opinion in the April 29, 2014 Supreme Court decision (*Environmental Protection Agency, et al. v. EME Homer City Generation, L.P., et. al.*) quoted “from

*(continued on inside back cover)*

(continued from inside front cover)

each according to his ability” three times as a way of attacking federal bureaucratic authority over interstate air pollution—crucial to regulating emissions from coal-fired plants. Others in conservative circles have recently used the phrase to criticize Thomas Piketty’s influential new book *Capital in the Twenty-First Century*, which tries to incorporate the reality of inequality into neoclassical economics. All of this caused Paul Krugman to observe ironically in his *New York Times* column on May 11, 2014, that, “Everywhere you look these days, you see Marxism on the rise. Well, O.K., maybe you don’t—but conservatives do.”

Not only the right has been drawing attention to this memorable saying associated with Marx; many on the left have been calling it to mind as well. In his 2013 book, *The Democracy Project*, anthropologist David Graeber employs it to advance the anarchist notion that “all societies are communistic at base.” He stresses that the famous saying did not originate with Marx’s *Critique of the Gotha Programme*, but was taken from the French socialist Louis Blanc’s *Organization of Work*, published “in 1840” (Graeber, *Democracy Project*, 293–95). The same point is made in the *Random House Dictionary of Popular Proverbs and Sayings* (1996) and in many other places.

Although it is true that “from each according to his ability, to each according to his needs,” appeared in Blanc’s *Organization of Work*, it cannot be found in the 1840 edition of his book, where he referred to what he called “the St. Simonian doctrine. . . ‘from each according to his ability, to each ability according to its works.’” Rather, it wasn’t until nine years later that Blanc in *Le Nouveau Monde*, no. 6 (December 15, 1849) coined the very different phrase “from each according to his ability, to each according to his needs.” He then inserted it into the ninth (1850) edition of his *Organization of Work*. (A lot of credit is also due to Étienne Cabet, who had inscribed on the title page of his 1840 Fourierist *Voyage en Icarie*: “to each according to his needs, from each according to his strength”—and even more credit, as we shall see, goes to François-Noël Babeuf, in the late eighteenth century.) Blanc’s slogan was a popular one and was to be taken up by socialists generally. In an article on Proudhon in 1851 Engels explicitly quoted: “From each according to his ability, to each according to his needs,” attributing the saying to Blanc. (Louis Blanc, *Organisation du travail*, 1840 edition, 166; Karl Marx and Frederick Engels, *Collected Works*, vol. 11, 555; Frank Manuel, *A Requiem for Karl Marx*, 1995, 163, 171–72, 248; Paul Meier, *William Morris: Marxist Dreamer*, vol. 1, 186–87.)

All of this would seem at first glance to push Marx into the background with respect to the single most important statement on the egalitarian principle governing communist society, relegating him to the position of being a mere popularizer of a French socialist conception. However, here the story takes still another twist. In volume 2, chapter 5 of Marx and Engel’s 1845–1846 work *The German Ideology*,

(continued on page 160)

(continued from inside back cover)

completed three years before Blanc's use of the phrase (but remaining unpublished in Marx and Engels's lifetime), one finds the following extraordinary passage:

But one of the most vital principles of communism, a principle which distinguishes it from all reactionary socialism, is its empirical view, based on a knowledge of man's nature, that differences of *brain* and of intellectual ability do not imply any differences whatsoever in the nature of the *stomach* and of physical *needs*; therefore the false tenet, based upon existing circumstances, "to each according to his abilities," must be changed, insofar as it relates to enjoyment in its narrower sense, into the tenet, "to each according to his need"; in other words, a *different form* of activity, of labour, does not justify *inequality*, confers no *privileges* in the respect of possession and enjoyment (Marx and Engels, *Collected Works*, vol. 5, 537).

Here we see already, more than a quarter-century before the *Critique of the Gotha Programme*, and prior to Blanc's 1849 article, the development of Marx's distinctive approach to human productivity and needs. Moreover, the emphasis is clearly on *needs*. Thus the St. Simonian focus on "to each according to his abilities" is seen as too narrow and limited, and is countered (or rather supplemented) with the notion of "to each according to his needs." *The German Ideology* and the *Critique of the Gotha Programme* both take their stand *contra mundum* with the deeper egalitarianism of Babeuf and his "conspiracy of equals." According to Babeuf: "Equality must be measured by the *capacity* of the worker, and the *need* of the consumer, not by the intensity of the labour and the quantity of things consumed" (Philippe Buonarroti, *Conspiration pour l'égalité dite de Babeuf* [1828]; quoted in István Mészáros, *Beyond Capital*, 221). This is clearly the broad tradition out of which Marx arises, and it is to Babeuf that we must ultimately attribute this deeply communistic view.

In fact, like all great ideas, the conception of "from each according to his ability, to each according to his needs" was a *social* or *collective*, not merely an *individual*, product. In this respect it is significant that it was probably Moses Hess, a German socialist/communist thinker with whom Marx and Engels were closely associated in the early 1840s—and not Marx and Engels themselves—who drafted chapter 5 in volume 2 of *The German Ideology*. The chapter appears to have been an adaptation of an earlier article by Hess, edited (and perhaps refined) by Marx. Hess's name is noted on the manuscript version of the chapter (Marx and Engels, *Collected Works*, vol. 5, 606–7). This means that the core conception underlying the best known description of communist principles can be said to have originated with Babeuf and Cabet, was elaborated by Hess and Marx/Engels (and inserted into Marx and Engels's *The German Ideology*), put into a slightly more succinct form by Blanc, and finally explored in depth decades later by Marx—in what was to be his most detailed explanation of the transition to socialism/communism.

In the end what is significant is that the saying, *from each according to one's ability, to each according to one's need*—the gender-neutral way in which it needs to be referred to today—constitutes the hard core of what István Mészáros calls "substantive equality," the revolutionary culmination (at the level of thought) of socialist theory. As *El Libertador*, Simón Bolívar, was to express it: equality is "the law of laws." (István Mészáros, *The Challenge and Burden of Historical Time*, 258–64, 302, 461.)



(continued on page 159)

48. The reference is only for purposes of comparison. The review of grand jury proceedings is far from perfect, and grand jury abuse in the name of "national security" and crime-fighting has been widespread. For an overview of the relevant law, see Wayne R. LaFave, Jerold H. Israel, and Nancy J. King, *Principles of Criminal Procedure: Investigation*, 4th edition (St. Paul, MN: Thomson/West2004), chapter 15.

49. *New York Times Co. v. Department of Justice*, 915 F.Supp.2d 508 (S.D.N.Y. 2013).

50. Seekers of information on government surveillance have also been frustrated. See, e.g., *Electronic Frontier Foundation v. Department of Justice*, 739 F.3d 1 (2014).

51. --- F.3d ---, 2014 WL 1569514 (No. 13-422-cv).

52. See, e.g., *First Amendment Coalition v. U.S. Dep't of Justice*, 2014 WL 1411333 (N.D. Calif. 2014). See also *ACLU v. CIA*, 710 F.3d 422 (D.C. Cir. 2013).

53. The tally of suits and their status is set out in 82 U.S. Law Week 1409 (March 25, 2014).

54. Rand Paul, "Show Us the Drone Memos," *New York Times*, May 11, 2014, <http://nytimes.com>.

55. U.S. Atomic Energy Commission, In the Matter of J. Robert Oppenheimer: Transcript of Hearing Before Personnel Security Board 173 (1954). This was the hearing at which General Groves, Edward

Teller and others attacked Oppenheimer's "loyalty" and revealed much about U.S. Cold War strategy. Indeed, the atomic bombs were dropped on Hiroshima and Nagasaki to prevent the USSR from having any role in the post-war events in the Far East; see P.M.S. Blackett, *The Military and Political Consequences of Atomic Energy* (London: Turnstile Press, 1948), and Gar Alperowitz, et. al., *The Decision to Use the Atomic Bomb and the Architecture of an American Myth* (New York: Knopf, 1995). I reached and documented this conclusion in my senior thesis "Atomic Science and Social Responsibility" (University of California, Berkeley, History Dept., 1962).

56. See elsewhere in this issue David Vine, "'We're Profiteers': How Military Contractors Reap Billions from U.S. Military Bases Overseas," *Monthly Review* 66, no.3 (July-August 2014): 82–102.

57. See William Blum, *Killing Hope* (Monroe, ME: Common Courage Press, 2000).

58. Childe Harold's Pilgrimage, Canto iv. Stanza 10.

59. For the Argentina case, see Jim Yardley, "Facing His Torturer as Spain Confronts Its Past," *New York Times*, April 6, 2014. The French case and related matters are discussed at "Universal Jurisdiction: Accountability for U.S. Torture," <http://ccjustice.org>. An important caveat: the fact that judicial forums distant from the place of harm may

be available does not mean that all such forums are legitimate, or that exercises of their power are proper. For example, the International Court of Justice (ICJ) in 2002 wisely held that Belgium could not proceed against a government official of the Democratic Republic of Congo for alleged human rights abuses in the Congo. See Christian J. Tams and James Sloan, eds., *The Development of International Law by the International Court of Justice* (Oxford University Press, 2013), 120 et. seq. The court explicitly denied an exception for war crimes and crimes against humanity to existing international law standards of personal immunity. While the ICJ opinion was a sharp reassertion of traditional standards of personal immunity, it is also possible to read the opinion as influenced by the idea that Belgium giving human rights lessons to the Congo was ludicrously inappropriate. This was brilliantly set out in the Separate Opinion of ad hoc Judge Sayeman Bula-Bula ("Opinion Individuelle de M. Bula-Bula," <http://icj.cj.org>) which persuasively insists on the placing of so-called "universal jurisdiction" in the context of history, and the power of the predominant imperialist jurisdictions. He concludes that the ICJ opinion, properly understood, "should call for greater modesty from the new fundamentalist crusaders on behalf of humanitarianism 'skilled at presenting problems in a false light in order to justify damaging solutions' including a certain trend of legal militancy."

(continued from page 160)

William Franklin ("Bill") Ash, who wrote for *Monthly Review* in the 1960s and was the author of the *Monthly Review* Press book, *Marxism and Moral Concepts* (1964), died at age 96 on April 26, 2014. Ash was an American-born British Spitfire pilot (he had enlisted in the Royal Canadian Air Force early in the war) who was shot down in 1942, and made numerous escapes from Nazi prison camps. He became perhaps the chief inspiration for Steve McQueen's character "the cooler king" in the 1963 Hollywood film, "The Great Escape." After the war Ash studied politics, and became head of the BBC's Indian operations. He was a cofounder of the Communist Party of Britain (Marxist-Leninist) and became the chair in the 1970s and '80s of the Writers' Guild of Great Britain. His wartime experiences were depicted in his 2005 book *Under the Wire*, on which he collaborated with Brendan Foley. An excellent obituary of Ash by Foley appeared in the *Guardian*, April 29, 2014 ("Bill Ash obituary"). The best way to remember Bill Ash is in the terms that he himself used when writing an obituary for Bill Blake in MR in June 1968. Quoting Mao, Ash said: "Though death befalls all men alike, it may be weightier than Mount Tai or lighter than a feather.' The death of one who spent his life serving other people and spreading a knowledge of the liberating force of Marxism is 'weightier than Mount Tai.'"



**Correction:** In Samir Amin, "Popular Movements Toward Socialism" (MR, June 2014), page 17, due to an editing error, the CPI-M was misidentified as the Communist Party of India-Maoist; it is the Communist Party of India-Marxist.

# Surveillance Capitalism

## *Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age*

JOHN BELLAMY FOSTER AND ROBERT W. McCHESNEY

The United States came out of the Second World War as the hegemonic power in the world economy. The war had lifted the U.S. economy out of the Great Depression by providing the needed effective demand in the form of endless orders for armaments and troops. Real output rose by 65 percent between 1940 and 1944, and industrial production jumped by 90 percent.<sup>1</sup> At the immediate end of the war, due to the destruction of the European and Japanese economies, the United States accounted for over 60 percent of world manufacturing output.<sup>2</sup> The very palpable fear at the top of society as the war came to a close was that of a reversion to the pre-war situation in which domestic demand would be insufficient to absorb the enormous and growing potential economic surplus generated by the production system, thereby leading to a renewed condition of economic stagnation and depression.

Assistant Secretary of State Dean Acheson declared in November 1944 before the Special Congressional Committee on Postwar Economic Policy and Planning, that if the economy slipped back to where it was before the war “it seems clear that we are in for a very bad time, so far as the economic and social position of the country is concerned. We cannot go through another ten years like the ten years at the end of the twenties and the beginning of the thirties [i.e., the Stock Market Crash and the Great Depression], without the most far-reaching consequences upon our economic and social system.” Acheson made it clear that the difficulty was not that the economy suffered from a lack of productivity, but rather that it was *too* productive. “When we look at the problem we may say it is a problem of markets. You don’t have a problem of production. The United States has unlimited creative energy. The important thing is markets.”<sup>3</sup>

Postwar planners in industry and government moved quickly to stabilize the system through the massive promotion of a sales effort in the form

---

**JOHN BELLAMY FOSTER** is editor of *Monthly Review* and professor of sociology at the University of Oregon. **ROBERT W. McCHESNEY** is the Gutzwiller Endowed Professor in the Department of Communication at the University of Illinois. They are the coauthors of *The Endless Crisis: How Monopoly-Finance Capital Creates Stagnation and Upheaval from the USA to China* (Monthly Review Press, 2012).

of a corporate marketing revolution based in Madison Avenue, and through the creation of a permanent warfare state, dedicated to the imperial control of world markets and to fighting the Cold War, with its headquarters in the Pentagon. The sales effort and the military-industrial complex constituted the two main surplus-absorption mechanisms (beyond capitalist consumption and investment) in the U.S. economy in the first quarter-century after the Second World War. After the crisis of the 1970s, a third added surplus-absorption mechanism, financialization, emerged, propping up the underlying system of accumulation as the stimulus provided by the sales effort and militarism waned. Each of these means of surplus absorption were to add impetus in different ways to the communications revolution, associated with the development of computers, digital technology, and the Internet. Each necessitated new forms of surveillance and control. The result was a universalization of surveillance, associated with all three areas of: (1) militarism/imperialism/security; (2) corporate-based marketing and the media system; and (3) the world of finance.

### **The Warfare State**

Soon after the war a new Pentagon capitalism was formed in Washington. A crucial element in the post-Second World War economy of the United States was the creation of the warfare state, rooted in a military-industrial complex. On April 27, 1946, General Dwight D. Eisenhower, chief of staff of the Army, issued a “Memorandum for Directors and Chiefs of War Department General and Special Staff Divisions and Bureaus and the Commanding Generals of the Major Commands” on the subject of “Scientific and Technological Resources as Military Assets.” Seymour Melman later referred to this memo as the founding document of what President Eisenhower—in his famous January 17, 1961 farewell address to the nation—was to call the “military-industrial complex.” In this memo General Eisenhower emphasized that a close, continuing contractual relationship be set up between the military and civilian scientists, technologists, industry, and the universities. “The future security of the nation,” he wrote, “demands that all those civilian resources which by conversion or redirection constitute our main support in time of emergency be associated closely with the activities of the Army in time of peace.” This required an enormous expansion of the national security system, bringing civilian scientists, industry, and contractors within this expanding and secretive arm of government. “Proper employment of this [civilian] talent requires that the [given] civilian agency shall have the benefit of our estimates of future military problems

and shall work closely with Plans and the Research Development authorities. A most effective procedure is the letting of contracts for aid in planning. The use of such a procedure will greatly enhance the validity of our planning as well as ensure sounder strategic equipment programs.” Eisenhower insisted that scientists should be given the greatest possible freedom to conduct research but under conditions increasingly framed by the “fundamental problems” of the military.

A crucial aspect of this plan, Eisenhower explained, was for the military state to be able to absorb large parts of the industrial and technological capacity of the nation in times of national emergency, so that they become “*organic parts of our military structure*.... The degree of cooperation with science and industry achieved during the recent [Second World] war should by no means be considered the ultimate;” rather, the relationship should expand. “It is our duty,” he wrote, “to support broad research programs in educational institutions, in industry, and in whatever field might be of importance to the Army. Close integration of military and civilian resources will not only directly benefit the Army, but indirectly contribute to the nation’s security.” Eisenhower therefore called for “the utmost integration of civilian and military resources and...securing the most effective unified direction of our research and development activities”—an integration that he said was already “being consolidated in a separate section on the highest War Department level.”<sup>4</sup>

Eisenhower’s emphasis in 1946 on an organic integration of the military with civilian science, technology, and industry within a larger interactive network was not so much opposed to, as complementary with, the vision of a warfare economy, based on military Keynesianism, emanating from the Truman administration. The Employment Act of 1946 created the Council of Economic Advisers charged with presenting an annual report on the economy and organizing the White House’s economic growth policy. The first chairman of the Council of Economic Advisers was Edwin Nourse, famous for his role in the 1934 publication of the Brookings Institution study, *America’s Capacity to Produce*, which pointed to the problem of market saturation and excess productive capacity in the U.S. economy. The vice chairman was Leon Keyserling, who was to emerge as the foremost proponent of military Keynesianism in the United States. In 1949 Nourse stepped down and Keyserling replaced him. Meanwhile, the National Security Council was created with the passage of the National Security Act of 1947 (which also created the CIA). Together, the Council of Economic Advisors and the National Security Council were to construct the foundation of the U.S. warfare state. Truman formed the ultra-shadowy National

Security Agency (NSA) in 1952 as an arm of the military charged with conducting clandestine electronic monitoring of potential foreign (and domestic) subversive activities.<sup>5</sup>

In 1950 Paul H. Nitze, director of the Department of State's Policy Planning Staff under Acheson, was given the leading role in drafting National Security Council Report 68 (NSC-68), which established an overall U.S. geopolitical grand strategy for waging the Cold War and global imperialism. Significantly, NSC-68 saw a great boost to government spending as a crucial element in preventing economic stagnation: "There are grounds for predicting that the United States and other free nations will within a period of a few years at most experience a decline in economic activity of serious proportions unless more positive government programs are developed than are now available." This provided an added justification, beyond geopolitical concerns, for a massive rearmament based on military Keynesian "guns and butter" principles. The economic analysis of NSC-68 was the result of direct consultations that Nitze had with Keyserling, who was to exert a strong influence on the report.

NSC-68 raised the possibility of a greatly expanded U.S. economy, based on the experience of the Second World War, in which increased military procurement and sustained domestic consumption were seen as fully compatible in the context of a full employment economy, but not obtainable otherwise. Such an economy could provide both guns and butter. "The United States," the report said, "could achieve a substantial absolute increase in output and could thereby increase the allocation of resources to a build-up of economic and military strength of itself and its allies without suffering a decline in its real standard of living." Indeed, "in an emergency the United States could devote 50 percent of its gross national product" to military expenditures, foreign assistance, and investment—"or five to six times as much as at present." The report strongly stressed that the huge rearmament program being advocated did not require any hard choices economically, as it "might not result in a real decrease in the standard of living" but could even produce the opposite:

The economic effects of the program might be to increase the gross national product by more than the amount being absorbed for additional military and foreign assistances purposes. One of the most significant lessons of our World War II experience was that the American economy, when it operates at a level approaching full efficiency [full capacity], can provide enormous resources for purposes other than civilian consumption while simultaneously providing for a high standard of living. After allowing for price changes, personal consumption expenditures rose by about one-fifth between 1939 and 1944, even though the economy had in



the meantime increased the amount of resources going into Government \$60-\$65 billion (in 1939 prices).<sup>6</sup>

Keyserling, in his capacity as chairman of the Council of Economic Advisers, was asked to provide an economic assessment of NSC-68, despite his direct input into the report itself. In a memorandum that he wrote on December 8, 1950, he indicated the planned buildup of expenditure on national security for 1952 envisioned in NSC-68 was well below the capacity of the economy. It would reach only 25 percent of national output in 1952, whereas national security expenditures had risen to 42 percent in 1944. Although likely cutting into domestic consumption “the general civilian consumption standards which would be possible under the proposed programs could hardly be described as severe,” while overall output and employment in the economy would increase.<sup>7</sup>

NCS-68 called for a more than tripling of military spending. The rearmament strategy advocated in the report was couched primarily in Cold War terms, as a means of promoting the so-called “Containment” doctrine announced by Truman in March 1947, and only secondarily in terms of the economy.<sup>8</sup> But the two objectives were seen as congruent. In April 1950, two months before the United States entered the Korean War, *Business Week* declared that the calls for increased government spending, particularly on the military, were the result of “a combination of concern over tense Russian relations and a growing fear of a rising level of unemployment here at home.”<sup>9</sup> This reflected the general character of the political economy of the Cold War. As Harry Magdoff ironically noted at the end of his *Age of Imperialism* in 1969: “Just as the fight against Communism helps the search for profits, so the search for profits helps the fight against Communism. What more perfect harmony of interests could be imagined?”<sup>10</sup>

The NSC-68 plan for rearmament was soon implemented for the U.S. political economy, with the shift to continuing high military expenditures made possible by the Korean War. By the time that war was brought to an end a much larger military system was in place. Although Eisenhower made efforts to cut military spending after the war, it was to remain “more than three times higher than it was before NSC-68 and the Korean conflict.”<sup>11</sup> In 1957, at the beginning of Eisenhower’s second term, military spending was 10 percent of U.S. GDP.<sup>12</sup> This reflected the rise of a warfare state, which Scott Nearing, writing in *Monthly Review* in 1964, defined as a state “which uses war and the threat of war as the decisive instruments of its foreign policy. In a warfare state the body politic places at the top of its list of state activities, planning for war, preparing for war, and waging war when opportunity offers.”<sup>13</sup>

Already by the end of the Korean War the new warfare state was deeply entrenched. As Eisenhower's first defense secretary, Charles Erwin Wilson (sometimes referred to as "General Motors Wilson," as a former president of General Motors, and to distinguish him from Charles E. Wilson [see below]), was to tell Congress, the ascendancy of the military, once in place, was virtually irreversible: "One of the most serious things about this defense business is that so many Americans are getting a vested interest in it: properties, business, jobs, employment, votes, opportunities for promotion and advancement, bigger salaries for scientists and all that. It is a troublesome business.... If you try to change suddenly you get into trouble.... If you shut the whole business off now, you will have the state of California in trouble because such a big percentage of the aircraft industry is in California."<sup>14</sup> Indeed, what had already been put into place to a considerable degree was what the president of General Electric and executive vice chairman of the War Production Board, Charles E. Wilson (sometimes referred to as "General Electric Wilson"), had strenuously lobbied for in 1944: the maintenance of a permanent war economy, in which "an industrial capacity for war, and a research capacity for war" were linked to the state and the armed forces.<sup>15</sup>

In all of this the role of military spending as a means of creating effective demand was obvious to economists and business alike. Harvard economist Sumner Slichter noted at a banking convention in late 1949 that given the level of Cold War expenditures, a return to conditions of severe depression was "difficult to conceive." Military spending, he explained, "increases the demand for goods, helps sustain a high level of employment, accelerates technological progress and helps the country to raise its standard of living." U.S. business's view of the heightened military budget, as reflected in the sentiments expressed in the U.S. corporate media, was ecstatic. Celebrating the development of the hydrogen bomb in 1954, *U.S. News and World Report* wrote: "What H-bomb means to business. A long period... of big orders. In the years ahead, the effects of the new bomb will keep on increasing. As one appraiser puts it: 'The H-bomb has blown depression-thinking out the window.'"<sup>16</sup>

On the left, Paul A. Baran and Paul M. Sweezy's classic work, *Monopoly Capital*, published in 1966, saw militarism and imperialism as motivated first and foremost by the needs of the U.S. empire, and secondly by its role (along with the sales effort) as one of the two main absorbers—beyond capitalist consumption and investment—of the rising economic surplus generated by the economy. All other options for government stimulus spending ran into political roadblocks established by powerful corporate

interests. Civilian government spending as a percentage of GDP, excluding transfer payments, Baran and Sweezy argued, had reached its “outer limits” by the late 1930s, when civilian government consumption and investment had risen to 14.5 percent in 1938–1939—a proposition that has remained true ever since, with civilian government spending (consumption and investment) standing at 14 percent of GDP in 2013. (That, however, exaggerates the government’s maintenance of a commitment to “social welfare,” as prisons and domestic policing have come to provide an outsized share of “civilian” government spending in the past three decades.) Consequently, military spending was viewed as more variable than civilian government spending, more readily turned to by the system as a means for “pump-priming” the economy.<sup>17</sup>

Nevertheless, military spending, Baran and Sweezy argued, faced its own contradictions, and was “not a perfectly free variable through manipulation of which the leaders of the oligarchy can maintain the right head of steam in the economic engine.” The main limitations were of course the total destructiveness of war itself, which meant that a Third World War between the major powers had to be avoided. Open warfare was therefore mainly directed at the periphery of the imperialist world economy, with the United States maintaining a “global military machine to police a global empire,” including over a thousand military bases abroad by the mid-1960s, as a means of propelling U.S. forces around the world.

This reality was bound to generate increased resistance, as in the case of Vietnam, both in the periphery and amongst the U.S. population.<sup>18</sup> Indeed, the open revolt of the U.S. ground troops in Vietnam by the early 1970s (along with protests at home) all but forced the military to abandon the military draft as impractical for the types of Third World invasions and occupations that had become standard—compelling it to turn, instead, to a professional army.<sup>19</sup> The invasions of the past two decades would have faced much greater popular resistance if they had required a draft to field the armed forces.

Inherent in such attempts to police a world empire were two requirements: First, a widespread propaganda campaign to make empire appear benevolent, necessary, essentially democratic, inherently “American,” and therefore unquestionable in legitimate debate. For an empire, the flip side of propaganda is popular ignorance. Vietnam’s “greatest contribution,” according to Defense Secretary Robert McNamara in its immediate aftermath, was teaching the U.S. government that in the future it was essential “to go to war without arousing the public ire.” McNamara said this was “almost a necessity in our history, because this

is the kind of war we'll likely be facing for the next fifty years."<sup>20</sup> Here the U.S. news media do yeoman's work legitimizing the imperial system and obstructing popular understanding at every turn. Second, there is the stick to go with the propaganda carrot—a heavy reliance on covert intervention in the periphery and domestic surveillance and oppression.

### The Sales Effort

The sales effort headquartered in Madison Avenue was to be the main success story of U.S. monopoly capitalism in the 1950s, and a key means of absorbing economic surplus. Outside of capitalist luxury consumption, the sales effort absorbed economic surplus chiefly by means of what Baran and Sweezy called “profits by deduction,” giving higher wages to workers (or to a relatively privileged element of the working class) and then manipulating them to buy largely wasteful conveniences and unnecessary, ultimately unsatisfying, packaged goods of all kinds. The end result was to chain most people to their jobs without improving their real standard of living or position vis-à-vis the means of production.<sup>21</sup> Production, as Thorstein Veblen anticipated in the 1920s, became more and more about the manufacturing of “saleable appearances” rather than genuine use values.<sup>22</sup> In the postwar years a qualitatively new phase of consumer capitalism emerged based, as Martin Mayer wrote in 1958 in *Madison Avenue*, on “a tripartite business, composed of clients (the companies which make the branded products and pay to advertise them), agencies (which prepare and place the ads), and media (the newspapers, magazines, broadcasting stations—each an individual *medium* for advertising—which carry the message to the public).”<sup>23</sup> Beyond advertising itself was the much larger realm of corporate marketing, involving such areas as targeting, motivation research, product design, sales promotion, and direct marketing.<sup>24</sup>

Marketing evolved quickly in its period of greatest advance in the 1950s into a highly organized system of customer surveillance, targeting propaganda, and psychological manipulation of populations. Consumer savings during the Second World War had grown enormously and the “Ad Men” of Madison Avenue became almost synonymous with the new “consumer culture” of the 1950s aimed at the promotion of innumerable, supposedly distinct brands. The result was an encouragement of high levels of consumer spending and a general lifting of the economy, as workers were conditioned to see themselves as consumers in all their non-working hours, reinforcing their dependence on their jobs while feeding the economic juggernaut. In this way the sales effort emerged as the dominant process governing the entire cultural apparatus of monopoly capitalism.<sup>25</sup>

There is no doubt that the growth of marketing expenditures in the 1950s, with advertising jumping in nominal terms from \$3 billion in 1929, to \$10 billion in 1957, to \$12 billion in 1962, served to expand total effective demand in the economy, creating new employment and markets, and stimulating investment in new product lines, while also encouraging prodigious amounts of commercial waste in superfluous packaging, product obsolescence, the production of useless goods foisted on consumers, etc. The entire marketing system constituted “a relentless war against saving and in favor of consumption.”<sup>26</sup> By the late 1950s, U.S. annual advertising spending was about 20–25 percent of military spending. And since advertising has always been a small part of overall marketing expenditures—the total size of which is, however, notoriously difficult to measure since it permeates all aspects of the system—the surplus-absorbing effect of the entire sales effort during the so-called “golden age” of the 1950s and ‘60s was likely roughly comparable to that of military spending as a means of surplus absorption, particularly in those years when an actual war was not taking place.<sup>27</sup>

The tremendous growth of marketing in these years was inseparable from the consolidation of monopoly capitalist accumulation. Price competition no longer occupied the central place in the competitive structure of the economy, as oligopolies operating in tandem through a process of indirect collusion ensured that the general price level went only one way—up. Instead, the oligopolistic rivalry that increasingly prevailed in the economy took the form of what came to be known as “monopolistic competition,” in which the competitive struggle was mainly over market share for particular brands, and thus centered on the sales effort. As welfare economist Tibor Scitovsky observed: “The secular rise in advertising expenditures is a sign of a secular rise of profit margins and decline of price competition.” In Baran and Sweezy’s analysis “price competition” had “largely receded as a means of attracting the public’s custom,” yielding “to new [wasteful] ways of sales promotion: advertising, variation of the products’ appearance and packaging, ‘planned obsolescence,’ model changes, credit schemes, and the like.”<sup>28</sup>

The corporation that spent the most on advertising in the United States in the 1950s was General Motors, then the largest corporation in the world, which had pioneered in product differentiation based on cosmetic model changes (such as chrome or tailfins). It built into its cars both (physical) product obsolescence and psychological obsolescence, and was the price leader in the industry—with the other giant automakers readily falling in line and sharing in the loot.

The largest marketer of packaged goods in the United States, and (next to General Motors) the largest purchaser of advertising, was Procter & Gamble. The company manufactured soaps, cleaners, and detergents such as Ivory, Tide, Cheer, Camay, Oxydol, Cascade, Comet, Joy, and Lava; Crest and Gleem toothpastes; Crisco shortening; Jif peanut butter; and many other branded products. Procter & Gamble is credited with having invented modern brand management beginning with Neil McElroy's famous May 13, 1931 internal corporate memorandum. Dismayed by having the job of promoting Camay soap as a subsidiary product in an environment dominated by Procter & Gamble's own Ivory soap, McElroy proposed that Procter and Gamble's various brands be managed by separate teams and marketed as completely distinct businesses, within a context of product differentiation in which the brands were targeted at different consumer markets. Later, as president of Procter & Gamble, McElroy embraced the soap opera, developing programing that was designed to be conducive to commercialism first and foremost, based on constant repetition both of story lines and product pitches. Procter & Gamble also emerged as a pioneer in conducting market research aimed at its potential customers. In addition, McElroy established large-scale "blue sky" scientific research laboratories at Procter & Gamble where the researchers were relatively free to explore new ideas with respect to consumer products.<sup>29</sup>

Procter & Gamble's considerable success in the 1950s in integrating advertising and programing in private broadcasting could be seen as symbolizing the triumph of commercialism in the U.S. media system in the post-Second World War era. "As early as the general advent of radio in the 1920s," Herb Schiller was to write in *Mass Communications and Empire*, "and deepening with the introduction of television in the late 1940s and early 1950s, the electronic apparatus has been largely at the disposal of the business system and the 'national advertiser' in particular. . . . The comprehensive employment of sophisticated communication facilities and ancillary services such as surveys, to the instruction and persuasion of consumers, is the foremost identifying feature of developed capitalism. . . . Scarcely a cultural space remains. . . that is outside the commercial web."<sup>30</sup> The government readily handed over the airwaves for free to corporations, while maintaining only the most minimal regulatory structure aimed primarily at protecting rather than restraining commercial privileges.<sup>31</sup>

### **The Military Industrial Complex and ARPANET**

After nine years heading Procter & Gamble, McElroy agreed to become Eisenhower's new Secretary of Defense. On October 4, 1957 the defense

secretary nominee was in Huntsville, Alabama touring the Redstone Arsenal, the Army's rocket program, and conversing with German émigré Wernher von Braun, considered the founder of modern rocketry, when news of the Soviet launching of Sputnik arrived. Five days later McElroy was sworn in as secretary of defense with all of Washington discussing the question of Soviet technological dominance. The launch of Sputnik II a month later only increased the pressure on the Eisenhower administration. After conferring with Ernest O. Lawrence, a major figure in the Manhattan Project, McElroy proposed the launching of a centralized agency for advanced scientific research projects, drawing on a broad network of scientific talent in universities and corporate manufacturing firms across the country. On November 20, 1957, he went to Capitol Hill for the first time and presented his idea of a "single manager" for all defense research, which would initially focus on ballistic missile, satellite, and space research and development programs, but which would have clear contracting authority and an unlimited, unconstrained research agenda. On January 7, 1958, Eisenhower requested Congress to provide startup funds for the new Advanced Research Projects Agency (ARPA). McElroy chose Roy Johnson, a vice president of General Electric, as the first ARPA director.

Right away ARPA set the goal of the militarization of space, including global surveillance satellites, communications satellites, and strategic orbital weapons systems, plus a moon mission. However, following the creation of the National Aeronautic and Space Agency (NASA) in the late summer of 1958, the civilian space programs were gradually stripped away from ARPA; and by 1959 most of its military space programs, along with the larger part of its funds, were also gone. Johnson resigned. However, rather than abolishing ARPA, McElroy, before leaving the Defense Department and returning as CEO of Procter & Gamble in 1959, revised ARPA's charter to make it more clearly a blue sky technology operation of the Department of Defense, superseding all of the armed forces. ARPA (renamed the Defense Advanced Research Projects Agency or DARPA in 1972) worked on developing anti-ballistic missile systems, and on Transit, the predecessor to the Global Positioning System (GPS). Its most remarkable work in its early years, though, was associated with the development of packet-switching digital communications technology, incorporating the insights of engineer Paul Baran at the Rand Corporation, which led to the original Internet and the packet satellite network. In the 1980s DARPA concentrated on the promotion of Ronald Reagan's Star Wars initiative in what has been

called the Second Cold War. In the 1990s and early 2000s it was to develop technologies of digital surveillance in close alliance with the NSA, along with military drone technology.<sup>32</sup>

It was with the appointment in 1961 of ARPA's third director, Jack P. Ruina, a scientist who was formerly a deputy assistant director of the Air Force, that the organization became a major force in computer research. Ruina purchased a massive Q-32 computer from the Air Force to allow ARPA to research military command and control issues. Ruina brought in J.C.R. Licklider of MIT, a behavioral scientist and computer programmer, to run ARPA's command and control and behavioral science divisions. Licklider created contractual relations with the best computer scientists at universities across the country, and introduced an internal culture that focused on the idea of networking based on interconnected computers. Over the course of the 1960s ARPA became the center of work on computer networking, resulting by the early 1970s in the creation of ARPANET, the precursor of today's Internet.

The product of the Eisenhower administration, ARPA existed alongside hundreds of other defense agencies formed in the Truman and Eisenhower years, yet it alone was conceived as the scientific-technological apex of the rapidly developing military-industrial complex. Under Eisenhower, at McElroy's instigation, the United States invaded Soviet air space with its U-2 spy plane, shot down by the Soviets in May 1960, and became engaged in counterinsurgency operations in Indochina and elsewhere.<sup>33</sup> The military policy of his administration remained expansive. Yet, Eisenhower's farewell address to the nation on January 17, 1961, showed his own second thoughts, uncertainty, ambivalence, and even fear at what had been created. Eisenhower pointed to the fact that the United States had developed "a permanent armaments industry of vast proportions.... We annually spend on military security more than the net income of all United States corporations." He went on to urge that the government "guard against the acquisition of unwarranted influence... by the military industrial complex," and to warn that society could become "captive of a scientific technological elite" under circumstances where "the power of money is ever present."

Eisenhower's warnings were deliberately vague. He did not define the "military-industrial complex," using the term only once in his speech. Yet, his comments were directed at the reality of the military-technological-corporate complex that he had himself played the leading role in instituting beginning in 1946, and that had been massively



extended in his years in the White House. By 1962, 56.2 percent of the sales of the electronics industry in the United States were going to the military and the closely allied civilian space industry.<sup>34</sup>

### The Vietnam War Era and Domestic Surveillance

The peak years of economic growth and near-full employment in the 1950s and '60s coincided with the years of the Korean and Vietnam Wars. Although these wars were fought under slogans of the "Containment of Communism" and the "Defense of the Free World," the real purpose in the case of both conflicts was to maintain the security of the world capitalist economy and U.S. hegemony in the face of forces seeking to break free. Yet if the geopolitics of empire and the Cold War were first and foremost in motivating these wars, the fact that they also required huge bursts of military spending that lifted the whole economy was not, as we have seen, lost on the dominant political-economic forces, and indeed entered directly into the calculations of the power elite.

Such a system of military-imperial dominance and capital accumulation naturally creates not only its own external enemies but its "internal enemies" as well—which in the eyes of the power structure consists of all those opposed to capitalism and the warfare state, along with all those forces in society that are seen as potentially disruptive. A warfare state thus naturally militates into a surveillance state.

The growth in the late 1950s and '60s of social protest, first over civil rights, and later the anti-Vietnam War movement and other causes, led to a massive increase in the military and quasi-military (or secret police) surveillance of the U.S. population. The years 1970–1971 saw the emergence of the "Army Files" (or CONUS) scandal, when it was revealed that the Army had been spying on and keeping dossiers on over seven million U.S. citizens. These dossiers were originally housed in its Investigative Records Library—with most of the files kept in a steel room, two stories high and half-a-block long—at Fort Holabird, Maryland. Along with these dossiers were satellite files, including a "vast subversives file" on civil rights and anti-war protestors and separate file cabinets devoted to incidents involving "civil disturbances" more generally, or dissent within the Army. In 1967 the military had completed construction of a secret national teletype service to allow rapid communication of intelligence gathered on the population. The Counterintelligence Analysis Branch was in charge of the construction of a huge *Compendium*, combining information from the surveillance files with the object of computerizing the data. Surveillance was carried out on participants in the Poor Peoples' March on Washington in

1968, visitors to Martin Luther King, Jr.'s grave, black nationalists, socialist organizations, and those engaged in anti-war demonstrations of more than twenty people across the entire country. The Army had 1,500 plain-clothes agents, working out of three hundred offices.<sup>35</sup>

In the continuing Congressional investigations into the Army intelligence files, and its subversives file in particular—which the Army said had been destroyed—it was later discovered that the data had been transmitted to the NSA,

via the ARPANET, a computer network connecting more than 50 government agencies and universities throughout the country. The network is funded by the Department of Defense Advanced Research Projects Agency (ARPA)... The information, according to intelligence sources, was transferred and stored at the headquarters of the National Security Agency (NSA), at Fort Meade, Maryland. The Army files were transmitted on the ARPANET in about January 1972, sources say, more than two years after the material—and the data banks maintained at the [Army's] Fort Holabird facility—were ordered destroyed.<sup>36</sup>

For many Americans this was the first indication that such a thing as ARPANET existed. Already in the 1970s the NSA was thus implicated in using the early proto-Internet system as part of its surveillance operations of the U.S. public. Stung by such revelations, Senator Sam Ervin, best known for his role as chairman of the Senate Watergate Committee, but long involved in the Army Files investigation, delivered a speech at MIT in April 1975 declaring that the danger to privacy had accelerated due to the presence of computers which allowed “limitless storage of data, and retrieval at lightening-like speed.”<sup>37</sup> The Senate investigations into the Army surveillance of the population and its databases caused University of Michigan law professor Arthur R. Miller to declare, as early as 1971, before the Senate Subcommittee on Constitutional Rights, chaired by Ervin:

Whether he knows it or not, each time a citizen files a tax return, applies for life insurance or a credit card, seeks government benefits, or interviews for a job, a dossier is opened under his name and an informational profile is sketched. It has now reached the point at which whenever we travel on a commercial airline, reserve a room at one of the national hotel chains, or rent a car we are likely to leave distinctive electronic tracks in the memory of a computer—tracks that can tell a great deal about our activities, habits, and associations when collated and analyzed. Few people seem to appreciate the fact that modern technology is capable of monitoring, centralizing, and evaluating these electronic entries—no

matter how numerous they may be—thereby making credible the fear that many Americans have of a womb-to-tomb dossier on each of us.

Even though the threat to our informational privacy is growing constantly, most Americans remain unaware of the extent to which federal agencies and private companies are using computers and microfilm technology to collect, store, and exchange information about the activities of private citizens. Rarely does a day go by without the existence of some new data bank being disclosed.... Consider the information practices of the United States Army. Early this year it was revealed that for some time Army intelligence systematically was keeping watch on the *lawful* political activity of a number of groups and preparing “incident” reports and dossiers on individuals engaging in a wide range of *legal* protests.<sup>38</sup>

The 1970s also revealed the FBI’s massive surveillance and movement-disruption program, COINTELPRO (an acronym for Counterintelligence Program). Between 1956 and 1975 the FBI, under J. Edgar Hoover, engaged in a wide array of surveillance and illegal activities (break-ins, forgeries, agent-provocateur actions, wrongful imprisonment, and violence) modeled after earlier actions taken against the Communist Party—directed at dissident groups, including socialist organizations, civil rights leaders, journalists, and New Left war critics. These actions were seen as “justified” by the FBI in cases where groups, such as the Socialist Workers Party, ran candidates for public office that supported causes like “Castro’s Cuba and integration...in the South.” New Left groups were targeted on the basis that they commonly “urge revolution” and “call for the defeat of the United States in Vietnam.”<sup>39</sup>

Under the codename Project MINARET, during the Johnson and Nixon years the NSA tapped the electronic communications of leading U.S. critics of the war, including over 1,600 U.S. citizens who were put on the NSA watch list. Among the individuals targeted were such figures as Martin Luther King, Jr., Whitney Young, Eldridge Cleaver, Stokely Carmichael, Jane Fonda, Tom Hayden, and Muhammad Ali. Beyond these, the NSA watch list also included such prominent establishment figures as U.S. Senators Frank Church and Howard Baker, *New York Times* columnist Tom Wicker, and *Washington Post* columnist Art Buchwald. The revelations on the NSA’s Project MINARET together with COINTELPRO led to the passage of the Foreign Intelligence Surveillance Act of 1978, which limited the powers of the federal government to conduct surveillance of U.S. citizens.<sup>40</sup>

In the early 1970s the NSA launched its code name Project ECHELON, conducted jointly with Britain, Canada, Australia, and New Zealand (collectively known as the Five Eyes), aimed at the interception of

civilian telecommunications conveyed by means of communication satellites. As William Blum wrote in *Rogue State* in 2005, “the ECHELON system works by indiscriminately intercepting huge quantities of communications and using computers to identify and extract messages of interest from the unwanted ones. Every intercepted message—all the embassy cables, the business deals, the sex talk, the birthday greetings—is searched for key words, which could be anything the searchers think might be of interest.” The NSA’s listening base in England encompassed 560 acres. Aside from collecting national security information, the NSA has been involved in commercial espionage on behalf of corporations, including stealing technology. In 1994 the NSA and the CIA turned over data that caused the European Airbus Industries to lose lucrative international contracts to their U.S. counterparts.<sup>41</sup>

### **Financialization, Data Mining, and Cyberwar**

Following the drawing down and end of the Vietnam War, the U.S. economy entered an economic crisis, which developed into a long period of deepening stagnation, characterized by declining real economic growth rates and rising unemployment and underemployment.<sup>42</sup> If military spending and an expanded Madison Avenue-based sales effort were the main added factors allowing for the absorption of economic surplus in the 1950s and ‘60s, their stimulative effect lessened in the 1980s and after, despite sharp increases in consumer credit (including credit cards) to boost the sales effort, and despite the Second Cold War unleashed by Reagan, inflating military spending. Reagan promoted a de facto military Keynesianism, lowering taxes primarily on corporations and the rich while giving a big boost to military spending. This included his expensive Star Wars program of anti-missile defense in which DARPA was to play a leading part. Attacks on labor unions, wages, and civilian government spending on behalf of workers and the poor became more severe, ushering in the age of neoliberalism.

A light was shown briefly on the scale and illegality of Reagan-era warfare state and secret government activities with the exposure of the Iran-Contra Affair in Washington. It led to the conviction on August 7, 1990, of Reagan’s National Security Advisor, Admiral John Poindexter, for five counts of lying to Congress and obstructing the investigations of Congressional Committees into Iran-Contra, involving the illegal selling of arms to Iran as a means of secretly funding the Contras waging war on the Nicaraguan government. (The convictions were later overturned on the basis that several witnesses against him had been

affected by Poindexter's testimony to Congress, even though he had been given immunity for his testimony.)

At the same time, Poindexter was also caught in another scandal through his authorship of National Security Decision Directive (NSDD)-145 (signed by Reagan). NSDD-145 would have centralized control over all computer databases in the United States, allowing the military to examine private computer databases for "sensitive but unclassified information"—making the NSA a computer czar. Faced with an outcry from private industry, and in the midst of the fallout over Iran Contra—both of which focused on Poindexter—NSDD-145 was withdrawn. After a period working for Syntek, a private firm contracting with DARPA, Poindexter reemerged in 2002 as the head of the Information Awareness Office in DARPA, designed to implement the technological basis for the Total Information Awareness (TIA) Program, to be carried out by the NSA, and directed at aggregating and analyzing all digitalized communications of the U.S. population. The Defense Department itself described it as creating a "virtual centralized grand database" on all electronic transmissions. One of the big contractors for the TIA program was Booz Allen Hamilton, a giant defense contractor. The head of the intelligence business at Booz Allen, Mike McConnell (former NSA director in the George H.W. Bush administration and later director of national intelligence under George W. Bush), was a close associate of Poindexter. Congress intervened to defund the program (then renamed Terrorism Information Awareness) in 2003, with the intention of closing it down completely—after a scandal arose from its development of an online futures trading market speculating on terrorist attacks, drawing attention to Poindexter and TIA.<sup>43</sup>

However, it was neoliberal financialization, even more than the warfare state, that characterized the Reagan era. With economic surplus no longer finding sufficient profitable outlets in what economists called the "real economy," more and more money capital flowed into speculation in the financial sector. Meanwhile, decades of imperial expansion, particularly in the Vietnam War period, had created a huge overhang of dollars abroad in the form of what came to be called the "Eurodollar market," generating a growing demand from abroad for outlets for this surplus money capital within the U.S. economy. Financial institutions responded to this increased demand for speculative products by creating an endless array of new speculative instruments in the form of various kinds of futures, options, and derivatives. The U.S. and the world economy saw a skyrocketing growth of speculative activity, visible in the growth of debt leverage—with financial corporate debt

rising from around 10 percent of U.S. GDP in 1970 to over 40 percent in 1990, and continuing to soar thereafter.<sup>44</sup> Not only did this help absorb surplus through the growing expenditures on fixed investment (chiefly business structures and computers) and employment (a growing army of financial analysts) in the real economy, but the speculative increase in the value of financial assets increased the wealth of the capitalist class independently from production, resulting in a certain percentage of this increased financial wealth being spent as luxury goods, thereby effectively absorbing surplus and stimulating the economy.

As early as May 1983, in an article entitled “Production and Finance” in *Monthly Review*, Harry Magdoff and Paul M. Sweezy described the massive long-term shift to an economy in which a huge “financial superstructure” dominated over the underlying production system. The result was the advent of a seemingly permanent financial-bubble prone economy. Such an economy was unstable and parasitic to the extreme, with constant fears of financial meltdown, and hence a growing role of central bankers as lenders of last resort, intervening periodically to prop up an increasingly fragile financial system. Sweezy was later to refer to this as “the financialization of the capital accumulation process.”<sup>45</sup>

Alan Greenspan, appointed chair of the Federal Reserve Board by Reagan in 1987, presided over two decades of rapid financial expansion, made possible by frequent interventions of the Federal Reserve Board to provide greater liquidity as the lender of last resort, and by an increasingly deregulated market environment in which to operate. All of this increased Wall Street’s power in Washington, to the point where it has come to dominate governance at the upper levels, in a manner even greater than that enjoyed by manufacturers in the immediate postwar years.<sup>47</sup> This then accelerated policies promoting financialization.

Financialization was spectacularly enhanced by high-speed computer networks, which became critical mechanisms for the newly created speculative markets, and no small amount of financial chicanery.<sup>47</sup> But financialization’s encouragement of surveillance capitalism went far deeper. Like advertising and national security, it had an insatiable need for data. Its profitable expansion relied heavily on the securitization of household mortgages; a vast extension of credit-card usage; and the growth of health insurance and pension funds, student loans, and other elements of personal finance. Every aspect of household income, spending, and credit was incorporated into massive data banks and evaluated in terms of markets and risk. Between 1982 and 1990 the average debt load of individuals in the United States increased by 30 percent and with

it the commercial penetration into personal lives. As Christian Parenti wrote in his 1991 book, *The Soft Cage*, “the records produced by credit cards, bankcards, discount cards, Internet accounts, online shopping, travel receipts and health insurance all map our lives by creating digital files in corporate databases.”<sup>48</sup> By 2000, as Michael Dawson reported in *The Consumer Trap*, nearly all major corporations in the United States were building huge databases, and were linked to data mining enterprises. “Symmetrical Research was advertising services such as its Advanced Analytic Solutions, which promised corporate clients ‘the power of one of the world’s most advanced marketing data analytics teams, with proprietary tools enabling the statistical analysis of... [data of the size of] the 35 terabyte Mastercard data set.’ A terabyte... is one *trillion* units of computerized information.”<sup>49</sup>

The largest data broker in the United States today, the marketing giant Acxiom has 23,000 computer servers processing in excess of 50 trillion data transactions annually. It keeps on average some 1,500 data points on more than 200 million Americans, in the form of “digital dossiers” on each individual, attaching to each person a thirteen-digit code that allows them to be followed wherever they go, combining online and offline data on individuals. Much of the data is now gleaned from social media, such as Facebook. Acxiom organizes this information into “premium proprietary behavioral insights.” Each person is also placed in one of seventy lifestyle clusters, focusing particularly on class, spending habits, and geographical location. Acxiom sells this data (giving varying access to its data banks) to its customers, which include twelve of the top fifteen credit-card issuing companies; seven of the top ten retail banks; five of the top ten insurance companies; six of the top ten brokerage firms; eight of the top ten media/telecommunication companies; seven of the top ten retailers; eleven of the top fourteen global automakers; and three of the top ten pharmaceutical firms. Its clients include about half of the largest one-hundred corporations in the United States.

Since September 2001 Acxiom has worked closely at sharing data with the FBI, the Pentagon, and Homeland Security. In 2001, Acxiom appointed General Wesley Clark, the former NATO Supreme Allied Commander in Europe in the Kosovo War and a future U.S. presidential candidate, to its board of directors. The company paid Clark over \$800,000 as a lobbyist, primarily in relation to the Department of Defense and Homeland Security. Through Clark, Acxiom began working with Poindexter’s DARPA-based TIA, helping set up the technological systems for total surveillance of the U.S. and global population.<sup>50</sup>

CBS's *60 Minutes* reported in March 2014 that clicking on the *New York Times* website can mean that more than a dozen third parties are "on the page that are essentially tracking your movements." Most of the 50 million people who downloaded the "Brightest Flashlight Free" app on to their smartphone did not recognize that "the companies that gave them to you for free were using the apps to track your every movement and pass it along to other companies." The iPhone app "Path Social," which was ostensibly designed to help people share photos and memories with their friends, tapped into user's digital address books and contact lists, taking all of that information. The data broker firm Epsilon has a marketing database containing more than 8 billion consumer transactions. The data broker firm Choicepoint, now part of the data giant Elsevier, maintains 17 billion records on businesses and individuals, which it has sold to around 100,000 clients, including numerous government agencies.<sup>51</sup>

Financial institutions themselves sell such data. *Forbes* magazine wrote in 2013 that "in most aspects of our lives, companies and marketers can freely collect details about us and sell to whomever they like without restriction." However, financial institutions, it pointed out, were legally prohibited in most cases from directly selling such information. Nevertheless, *Forbes* explained that many financial institutions do market their data in various ways, and some 27 percent violate all aspects of the legal regulations.<sup>52</sup>

Financialization—or the long-term growth of speculation on financial assets relative to GDP—meant the intrusion of finance into all aspects of life, requiring new extensions of surveillance and information control as forms of financial risk management. As the economy became more financialized, it became increasingly vulnerable to financial meltdowns, increasing risk perceptions on the part of investors and the perceived need for risk management, encryption of data, and security.

Today the fears of cyberwar aimed at financial institutions, the entire financial system, and the military system, is at the top of national security concerns. McConnell, who had left his job at Booz Allen to become director of national intelligence in 2007 under George W. Bush, informed the president that, "If the 9/11 perpetrators had focused on a single U.S. bank through cyberattack, and it had been successful, it would have had an order of magnitude greater impact on the U.S. economy than the physical attack." Secretary of the Treasury Henry Paulson, former CEO of Goldman Sachs, agreed. Bush was so alarmed that within a short time the Comprehensive National Cybersecurity Initiative (2008) was in place, which greatly expanded the NSA's authority to carry out surveillance



on the Internet domestically, leading to the construction of its \$1.5 billion data center in Utah.<sup>53</sup> Leon Panetta, U.S. defense secretary under Obama, warned that a cyberattack on the U.S. financial system might be the “next Pearl Harbor.” In July 2011 Barack Obama signed an executive order declaring that the infiltration of financial markets by transnational criminal organizations constituted a national emergency. Symantec, a cybersecurity firm, estimated in 2010 that three-quarters of “phishing” attacks designed to get people to give up financial data were not aimed at individuals but were directed at the financial sector.<sup>54</sup>

In addition to hackers breaking into databases, large scale attacks on entire security systems are feared. The sudden drop in the stock market on May 6, 2010, attributed to high speed algorithmic trading, was thought to prefigure a new possible form of cyberwar aimed at dragging reeling markets down further using short-selling, options, and swaps—a kind of “force multiplier” in military-speak. Hackers using malicious codes to crash or jam whole networks can mobilize Botnets or robotic networks of hundreds of thousands of machines. According to Mortimer Zuckerman, chairman and editor-in-chief of *U.S. News and World Report*, writing in the *Wall Street Journal*, digitalized systems are extraordinarily vulnerable to attack: “the average [offensive] malware has about 175 lines of code, which can attack defense software using between 5 million and 10 million lines of code.” The U.S./Israeli-developed “Stutnex” worm aimed at Iran, which reportedly infiltrated the computers controlling Iranian nuclear centrifuge facilities, is seen as an indication of the scale and precision with which cyberattacks can now demobilize whole systems.<sup>55</sup>

### **The Internet and Monopoly Capital**

ARPANET was connected only to those universities and their computer science departments that had Department of Defense funding and security clearances. With the success of the system, computer science departments at universities and private industry were all eager to be connected to the network. This resulted in the creation by the National Science Foundation of the Computer Science Research Network (CSNET), which consisted of ARPANET, a Telenet system, and PhoneNet for email. Soon other, private internets were created. In 1985 the National Science Foundation constructed five supercomputers across the country to be the backbone of a larger NSFNET, which brought universities in general and private corporations into what had merged into a much wider Internet with a common protocol, resulting in a massive growth of users who could access it through personal computers, via Internet Service Providers.

ARPANET ceased operations in 1989. In the early 1990s the World Wide Web was developed, leading to an astronomical increase in users, and the rapid commercialization of the Internet. Three key developments followed: (1) In 1995 NSFNET was privatized, and NSFNET itself decommissioned, with the backbone of the system being controlled by private Internet Service Providers;<sup>56</sup> (2) the Telecommunications Act of 1996 introduced a massive deregulation of telecommunications and media, setting the stage for further concentration and cenoentralization of capital in these industries;<sup>57</sup> (3) the Financial Services Modernization Act of 1999, promoted by Federal Reserve Chairman Alan Greenspan, Treasury Secretary Robert Rubin, and Deputy Treasury Secretary Lawrence Summers under the Clinton administration, deregulated the financial sector in an attempt to feed the financial bubble that was developing.<sup>58</sup> These three elements coalesced into one of the biggest merger waves in history, known as the dot-com or New Economy bubble. The ongoing concentration of capital was thus given a huge boost in the technology and finance sectors, leading to ever greater levels of monopoly power.

The dot-com bubble burst in 2000. But by that time a virtual Internet cartel had emerged, despite all the rhetoric of “friction-free capitalism” by Bill Gates and others.<sup>59</sup> By the end of the decade the Internet had come to play a central role in capital accumulation, and the firms that ruled the Internet were almost all “monopolies,” by the way economists use the term. This did not mean that these firms sold 100 percent of an industry’s output, but rather that they sold a sufficient amount to control the price of the product and how much competition they would have. (Even John D. Rockefeller’s Standard Oil monopoly at its peak controlled just over 80 percent of the market.) By 2014, three of the four largest U.S. corporations in market valuation—Apple, Microsoft, and Google—were Internet monopolies. Twelve of the thirty most valuable U.S. corporations were media giants and/or Internet monopolies, including Verizon, Amazon, Disney, Comcast, Intel, Facebook, Qualcomm, and Oracle. These firms used network effects, technical standards, patent law, and good old-fashioned barriers-to-entry to lock in their market power, and they used their monopoly gushers to broaden their digital empires. With this economic power comes immense political power, such that these firms face no threat from regulators in Washington. To the contrary, the U.S. government is little short of a private army for the Internet giants as they pursue their global ambitions.<sup>60</sup>

The major means of wealth generation on the Internet and through proprietary platforms such as apps is the surveillance of the population,

allowing for a handful of firms to reap the lion's share of the gains from the enormous sales effort in the U.S. economy. The digitalization of surveillance has radically changed the nature of advertising. The old system of advertisers purchasing ad space or time in media with the hope of getting the media user to notice the advertisement while she sought out news or entertainment is becoming passé. Advertisers no longer need to subsidize journalism or media content production to reach their target audiences. Instead, they can pinpoint their desired audience to a person and locate them wherever they are online (and often where they are in physical space) due to ubiquitous surveillance. The premise of the system is that there is no effective privacy. The consequences are that the commercial system of media content production, especially journalism, is in collapse, with nothing in the wings to replace it.

These monopolistic corporate entities readily cooperate with the repressive arm of the state in the form of its military, intelligence, and police functions. The result is to enhance enormously the secret national security state, relative to the government as a whole. Edward Snowden's revelations of the NSA's Prism program, together with other leaks, have shown a pattern of a tight interweaving of the military with giant computer-Internet corporations, creating what has been called a "military-digital complex."<sup>61</sup> Indeed, Beatrice Edwards, the executive director of the Government Accountability Project, argues that what has emerged is a "government-corporate surveillance complex."<sup>62</sup>

This extends beyond the vast private contractor network to "secret collaboration" with the main Internet and telecom companies.<sup>63</sup> Notable examples of partly cooperative, partly legally coerced sharing of data include:

- A 2009 report by the NSA's inspector general leaked by Snowden stated that the NSA has built collaborative relationships with over "100 companies."<sup>64</sup>
- Microsoft provided the NSA with pre-encryption "back door" access to its popular Outlook.com email portal, to its Skype Internet phone calls and chat (with its 663 million global users), and to SkyDrive, Microsoft's cloud storage system (which has 250 million users). The Snowden files show that Microsoft actively collaborated with the NSA. Glenn Greenwald writes: "Microsoft spent 'many months' working to provide the government easy access to that [the SkyDrive] data." The same was the case for Skype, while in the case of Outlook.com it took only a few months for the Microsoft and the NSA working together to ensure the NSA's complete access.<sup>65</sup>

- The NSA paid \$10 million to the computer security company RSA to promote a back door to encryption products. The NSA devised a flawed formula for generating random numbers for encryption with RSA inserting it into its software tool Bsafe, which had been designed to enhance security in personal computers and other digital products.<sup>66</sup>
- AT&T voluntarily sold metadata on phone calls to the CIA for over \$10 million a year in connection with the latter's counterterrorism investigations.<sup>67</sup>
- Verizon (and likely AT&T and Sprint as well) provided the NSA with metadata on all calls in its (their) systems, both within the United States and between the United States and other countries. Such metadata has been supplied to the NSA under both the Bush and Obama administrations.<sup>68</sup>
- Microsoft, Google, Yahoo, and Facebook turned over the data from tens of thousands of their accounts on individuals every six months to the NSA and other intelligence agencies, with a rapid rise in the number of accounts turned over to the secret government.<sup>69</sup>

In 2012 DARPA Director Regina Dugan left her position to join Google. During her period as director, DARPA had been at the forefront of drone research, presenting the first prototype demonstrations in the early 1990s. However, the outgrowth of this in the deployment of General Atomic Aeronautical System's Predator drones in warfare did not occur until the late 1990s in the Kosovo War, with Clark as the Supreme Allied Commander. The first use of such drones for global, extra-territorial assassination, outside a field of war—now a staple of Obama's "anti-terrorism" strategy—took place in 2002.<sup>70</sup> In the opening years of this century DARPA extended its research to developing drones that could be used for mobile wi-fi capabilities. Dugan's switch to Google in the private sector—at a time when she was under governmental investigation for giving hefty DARPA contracts to RedX, a bomb-detection corporation that she had co-founded and partly owned—was connected to Google's interest in developing high-altitude drones with wi-fi delivering capabilities. In 2014 Google announced that it was buying Titan Aerospace, a U.S.-based start-up company for building drones which cruise at the very edge of the atmosphere. Facebook meanwhile bought the UK corporation, Ascenta, which specializes in making high-altitude solar drones. Such drones would allow the spread of the Internet to new areas. The goal was to capitalize on a new military technology and create larger global Internet monopolies, while expanding the military-digital complex.<sup>71</sup>

By 2005–2007 broad estimates suggested that U.S. marketing expenditures (defined fairly narrowly) were running at about \$1 trillion a year; real (both acknowledged and unacknowledged) military expenditures at about \$1 trillion annually; and FIRE (finance, insurance, and real estate) expenditures at approximately \$2.5 trillion.<sup>72</sup> In the digital age, these three sectors of the political economy, each of which arose parasitically on the production base of the economy, were increasingly connected in a web of technology and data sharing. As the most advanced technologies (usually military developed) went private, many of those involved in the warfare economy, such as DARPA’s Dugan, were in a position to exploit the knowledge and connections that they had accumulated by shifting to the private sector, crossing fairly easily from one system of security and surveillance to another.

A kind of linguistic convergence mirrored the centralized structure of monopoly-finance capital in the age of digital surveillance with “securitization” increasingly standing simultaneously for a world dominated by: (1) financial derivatives trading, (2) a network of public and private surveillance, (3) the militarization of security-control systems, and (4) the removal of judicial processes from effective civilian control.<sup>73</sup>

### **Total Information Awareness, Prism, and Snowden**

Close watchers of the U.S. empire recognized that Congress’s attempt to close down Poindexter’s TIA Program had only been partly successful. Faced with Congressional opposition DARPA and the NSA shifted the program to private industry, where a deeper level of secrecy existed, since government accountability was less. As Chalmers Johnson wrote in his *Dismantling the Empire* in 2010:

However, Congress’s action did not end the “total information awareness” program. The National Security Agency secretly decided to continue it through its private contractors. The NSA easily persuaded SAIC [Science Applications International Corporation] and Booz Allen Hamilton to carry on with what Congress had declared to be a violation of the privacy rights of the American public—for a price. As far as we know, Admiral Poindexter’s “Total Information Awareness Program” is still going strong today.<sup>74</sup>

Such a transfer was more readily carried out, given that McConnell, in his capacity as director of the intelligence business at Booz Allen, was already contracting with Poindexter and the Total Information Awareness program. Hence program design, technology, and funding could be readily shifted out of the government into the shadowy world of military contracting. It remained linked to the NSA and its overall

super-secret, post-9/11 operation for the domestic surveillance of all Americans. Known in official documents as the “President’s Surveillance Program,” intelligence insiders referred to it simply as “The Program.” It was carried out under the supervision of NSA Director General Michael V. Hayden until 2005, who then moved on to become director of the CIA. Hayden’s replacement was the single-minded General Keith Alexander, whose motto was “Collect It All.” Alexander stepped down as head of the NSA in March 2014, in the midst of the Snowden revelations, and was succeeded by Admiral Mike Rogers.<sup>75</sup>

The relation between the intelligence establishment and the private contracting industry is a revolving door. McConnell, Bush’s director of national intelligence, is once again at Booz Allen, now as vice chairman; while James Clapper, Obama’s current director of national intelligence, is a former Booz Allen executive. Booz Allen is majority owned by the Carlyle Group, which specializes in private equity investment and ownership of military contractors. The Carlyle Group has been involved in some of the largest leveraged buyouts, and has long had a close relationship to the Bush family.<sup>76</sup>

The Snowden files clearly reveal that while Poindexter’s TIA program within DARPA was being defunded by an irate Congress, the NSA had already commenced its own related secret program, part of the President’s Surveillance Program, beginning shortly after 9/11 with Boundless Informant, a warrantless wiretapping program directed at both telephony and email. It took considerably longer to get Prism, which (like Poindexter’s TIA) was directed at total Internet surveillance, up and running, since this required both new technology and cooperation with the major Internet corporations. The technological development and much of the actual surveillance work was to be increasingly centered in Booz Allen and other private contractors. Although the NSA itself has as many as 30,000 employees, it relies on a larger workforce of some 60,000 employed by private contractors.<sup>77</sup>

In May 2013, Edward Snowden, a middle-level technician at Booz Allen Hamilton who had access to 1.7 to 1.8 million documents, placed large numbers of NSA documents on several thumb drives and fled the country for Hong Kong. From there he courageously revealed the magnitude of NSA spying on the U.S. and global populations.<sup>78</sup> Snowden provided documentary evidence, in the form of an NSA power point, that indicated that the NSA, in its own words, had managed to gain “direct access”—i.e., independent of all intermediaries—to practically all data circulating on the Internet within the U.S. sphere. It also

gained access to data from mobile phones emanating from hundreds of millions of Americans as well as populations abroad—operating thorough Boundless Informant, Prism, and other secret projects within “The Program.” According to one NSA slide, nine technology companies (Microsoft, Apple, Google, Yahoo, Facebook, Youtube, PalTalk, Skype, AOL), had all signed up and become, in some sense, corporate partners with Prism. The slide states that the data is collected “directly from the servers of these U.S. Service Providers.”<sup>79</sup> The NSA acquisitions director, in a document provided by Snowden, indicated that its back door allowed the NSA access to hundreds of millions of user accounts. According to Snowden himself, speaking from Hong Kong:

The US government co-opts US corporate power to its own ends. Companies such as Google, Facebook, Apple and Microsoft all get together with the NSA. [They] provide the NSA direct access to the back ends of all of the systems you use to communicate, to store data, to put things in the cloud, and even just to send birthday wishes and keep a record of your life. They give [the] NSA direct access, so that they don't need to oversee, so they can't be held liable for it.<sup>80</sup>

Snowden explained that even a middle-level technician in a private corporation engaged in intelligence, such as himself, could tap into the data of any individual in the United States:

While they may be intending to target someone associated with a foreign government or someone they suspect of terrorism, they are collecting your communications to do so. Any analyst at any time can target anyone. Any selector, anywhere. Whether these communications may be picked up depends on the range of the sensor networks and the authorities an analyst is empowered with. Not all analysts have the ability to target everybody. But I, sitting at my desk, certainly had the authority to wiretap anyone, from you, to your accountant, to a federal judge, and even the president, if I had a personal email [address].<sup>81</sup>

The Snowden documents reveal that increasingly the NSA did not need the active cooperation of the major Internet and telecom firms but could tap directly into their systems. By 2010, as a result of its BULLRUN and EDGEHILL programs, the NSA had made huge progress in breaking almost any encryption, using supercomputers that could crack algorithms, the building blocks of encryption, thus hacking into nearly all messages. Further, the documents show that the NSA put a back door into the cyberspace security norms established by the National Institute of Standards and Technology. The NSA claims that it has been able to

put “design changes” into commercial encryption that make the security appear intact, yet it is nonetheless open to NSA penetration.<sup>82</sup> As the *Washington Post* explained, the NSA does not infiltrate server databases. Rather it gets “‘data on the fly.’ The NSA and GCHQ [Britain’s Government Communications Headquarters] do not break into user accounts that are stored on Yahoo and Google computers. They intercept the information as it travels over fiber optic cables from one data center to another.” The NSA is also working with its British counterpart, GCHQ to intercept the private clouds of Yahoo and Google, which use private fiber optic highways outside the public Internet, to protect their data.<sup>83</sup>

The NSA has access to more than 80 percent of international telephone calls, for which it pays the U.S. telecom monopolies hundreds of millions of dollars a year. And it has broken into Internet data abroad.<sup>84</sup> By these means it has spied even on the heads of state of its allies.

The government and the corporate media sought to brand Snowden as a traitor. Two leading figures seeking to discredit Snowden in the media circuit are Clark, who invariably fails to disclose his own role in surveillance capitalism (having left Acxiom he is now on the advisory board of the cyber-intelligence corporation Tiversa), and McConnell (who downplays the continuous revolving door that has allowed him to move back and forth between the U.S. intelligence establishment and Booz Allen). Both have claimed that Snowden has compromised the security of the United States, by letting the population of the country and the world know the extent to which their every move is under surveillance.<sup>85</sup>

The Snowden revelations bewildered a U.S. population already struggling with numerous intrusions into their private lives, and ubiquitous surveillance. Dissident hackers associated with Anonymous and Wikileaks, and courageous whistle-blowers, like Snowden and Chelsea (formerly Bradley) Manning—the twenty-five-year-old soldier who released hundreds of thousands of classified documents—have been fighting the secret government-corporate security state.<sup>86</sup> Numerous organizations have been struggling for free speech and privacy rights in the new surveillance capitalism.<sup>87</sup> The population as a whole, however, has yet to perceive the dangers to democracy in an environment already dominated by a political system best characterized as a “dollarocracy,” and now facing a military-financial-digital complex of unbelievable dimensions, data mining every aspect of life—and already using these new technological tools for repression of dissident groups.<sup>88</sup>

So far the Snowden revelations have mainly disturbed the elites, making it clear that monopolistic corporations, and particularly the



intelligence community, are able to penetrate into the deepest secrets at every level of society. Employees in some private corporations working for the NSA have the ability to hack into most corporate data. The most likely result of all of this is a coming together of giant firms with the security apparatus of government, at the expense of the larger population.

Meanwhile the likelihood of cyberwar increases, threatening the entire capitalist system, and the U.S. empire itself. Ironically, the very structure of imperialism has increased security threats. (And, of course, the threat of cyberwar will be used as a justification for reducing individual rights and noncommercial values online ever more.) The global labor arbitrage, by means of which multinational corporations based in the United States and elsewhere take advantage of low wages in other countries, means that most production of computer hardware, including chips, is now done abroad, primarily in Asia.<sup>89</sup> A critical concern of the U.S. Defense Department (which purchases 1 percent of the world's integrated circuit production) has become the hacking of digital malware into the circuits of chips and computer devices themselves, leading to the possibility that critical weapons could be programmed to malfunction at a certain time or for weapons to arm or disarm. Hacked circuits could be used to bring down financial as well as defense systems. DARPA has nine contracts out to private corporations seeking to develop the means for dealing with these vulnerabilities.<sup>90</sup>

Nevertheless, such vulnerabilities are truly inescapable in today's hyper-imperialist system growing out of the contradictions of monopoly-finance capital. Its very economic exploitation of the world population, as well as its own, has left the U.S. imperial system open to attack, producing ever greater attempts at control. These are signs of a dying empire. To prevent total human and planetary disaster it is necessary that the *vox populi* be heard once again and for the empire to go. The digital revolution must be demilitarized and subjected to democratic values and governance, with all that entails. There is no other way.

## Notes

1. Richard B. DuBoff, *Accumulation and Power* (Armonk, NY: M.E. Sharpe, 1989), 91.

2. William H. Branson, "Trends in United States International Trade and Investment Since World War II," in Martin Feldstein, ed., *The American Economy in Transition* (Chicago: University of Chicago Press, 1980), 183.

3. Dean Acheson, quoted in William Appleman Williams, *The Tragedy of American Diplomacy* (New York: Dell, 1962),

235-36.

4. General Dwight D. Eisenhower, "Memorandum for Directors and Chiefs of War Department General and Special Staff Divisions and Bureaus and the Commanding Generals of the Major Commands; Subject: Scientific and Technological Resources as Military Assets," April 1946. Published as Appendix A in Seymour Melman, *Pentagon Capitalism* (New York: McGraw Hill, 1971), 231-34.

5. "'No Such Agency' Spies on the Communications of the World," *Washington Post*, June 6, 2013, <http://washingtonpost.com>.

6. U.S. State Department, *Foreign Relations of the United States, 1950. National Security Affairs; Foreign Economic Policy*, vol. 1, <http://digital.library.wisc.edu>, 258-61, 284-86.

7. S. Nelson Drew, ed., *NSC-68: Forging the Strategy of Containment; With Analy-*

- ses by Paul H. Nitze (Washington, DC: National Defense University, 1994), 117; "The Narcissism of NSC-68," November 12, 2009, <http://econospeak.blogspot.com>.
8. Dean Acheson, *Present at the Creation* (New York: W.W. Norton, 1987), 377; Thomas H. Etzold and John Lewis Gaddis, *Containment: Documents on American Policy and Strategy, 1949-50* (New York: Columbia University Press, 1978), chapter 7; Institute for Economic Democracy, "NSC-68, Master Plan for the Cold War," <http://ied.info>; Fred Block, "Economic Instability and Military Strength: The Paradoxes of the Rearmament Decision," *Politics and Society* 10, no. 35 (1980): 35-58.
9. *Business Week*, April 15, 1950, 15, quoted in Harold G. Vatter, *The U.S. Economy in the 1950s* (New York: W.W. Norton, 1963), 72.
10. Harry Magdoff, *The Age of Imperialism* (New York: Monthly Review Press, 1969), 200-201.
11. Lynn Turgeon, *Bastard Keynesianism: The Evolution of Economic Thinking and Policymaking Since World War II* (Westport, CT: Greenwood Press, 1996), 13; Noam Chomsky, *Necessary Illusions* (Boston: South End Press, 1989), 183.
12. Paul A. Baran and Paul M. Sweezy, *Monopoly Capital* (New York: Monthly Review Press, 1966), 152.
13. Scott Nearing, "World Events," *Monthly Review* 16, no. 2 (June 1964): 122.
14. Quoted in Fred J. Cook, *The Warfare State* (New York: Macmillan, 1962): 165-66.
15. "WPB Aide Urges U.S. to Keep War Set-Up," *New York Times*, January 20, 1944; Charles E. Wilson, "For the Common Defense," *Army Ordnance* 26, no. 143 (March-April 1944): 285-88.
16. Slichter and *U.S. News and World Report*, quoted in Cook, *The Warfare State*, 171.
17. Bureau of Economic Analysis, "National Income and Product Accounts," Table 1.1.5 (Gross Domestic Product), and Table 3.9.5 (Government Consumption Expenditures and Gross Investment), <http://bea.gov>; Baran and Sweezy, *Monopoly Capital*, 161, 207-13; John Bellamy Foster and Robert W. McChesney, "A New Deal under Obama?" *Monthly Review*, 60, no. 9 (February 2009): 1-11; Hannah Holleman, Robert W. McChesney, John Bellamy Foster, and R. Jamil Jonna, "The Penal State in an Age of Crisis," *Monthly Review* 61, no. 2 (June 2009): 1-17.
18. Baran and Sweezy, *Monopoly Capital*, 191, 206, 213-17.
19. For an excellent discussion of this, see Andrew J. Bacevich, *Breach of Trust: How Americans Failed Their Soldiers and Their Country* (New York: Metropolitan Books, 2013), 48-79.
20. Barbara W. Tuchman, *The March of Folly: From Troy to Vietnam* (New York: Random House, 1984), 326.
21. See Paul A. Baran and Paul M. Sweezy, "Some Theoretical Implications," *Monthly Review* 64, no. 3 (July-August 2012): 45-58; John Bellamy Foster, *The Theory of Monopoly Capitalism*, new edition (New York: Monthly Review Press, 2014), xiv-xviii.
22. Thorstein Veblen, *Absentee Ownership and Business Enterprise in Recent Times* (New York: Augustus M. Kelley, 1964), 300.
23. Martin Mayer, *Madison Avenue* (New York: Harper, 1958), 13-14.
24. See Michael Dawson, *The Consumer Trap* (Urbana: University of Illinois Press, 2005).
25. On the concept of the cultural apparatus, see John Bellamy Foster and Robert W. McChesney, "The Cultural Apparatus of Monopoly Capital," *Monthly Review* 65, no. 3 (July-August 2013): 1-33.
26. Baran and Sweezy, *Monopoly Capital*, 118-28.
27. Advertising spending, as noted above, was \$10 billion in 1957, while annual military spending in the Eisenhower administration was \$40-\$50 billion. On the latter figure see Turgeon, *Bastard Keynesianism*, 13.
28. Baran and Sweezy, *Monopoly Capital*, 115-17.
29. Dennis Daye, "Great Moments in Branding: Neil McElroy Memo," June 12, 2009, <http://brandingstrategyinsider.com>; Mayer, *Madison Avenue*, 26; Editors of *Advertising Age*, *The House that Ivory Built* (Lincoln, IL: National Textbook Co., 1988), 20-21, 158; Katie Hafner and Matthew Lyon, *Where Wizards Stay Up Late* (New York: Simon and Schuster, 1996), 14.
30. Herbert I. Schiller, *Mass Communications and American Empire* (Boulder: Westview Press, 1992), 8-9.
31. See the detailed critique of the Federal Communications Commission in this respect in *Monthly Review* in the late 1950s: Leo Huberman and Paul M. Sweezy, "Behind the FCC Scandal," *Monthly Review* 9, no. 12 (April 1958): 401-11.
32. Hafner and Lyon, *Where Wizards Stay Up Late*, 14-21, 255; L. Parker Temple III, *Shades of Gray: National Security and the Evolution of Space Reconnaissance* (Reston, VA: American Institute of Aeronautics and Astronautics, 2005), 132-33, 142, 146, 192-200, 208-18, 233, 242.
33. Helen Bury, *Eisenhower and the Cold War Arms Race* (New York: I.B. Tauris, 2014), 205; William Conrad Gibbons, *The U.S. Government and the Vietnam War: Executive and Legislative Roles and Relationships; Part IV: July 1965-January 1968* (Princeton: Princeton University Press, 1995), 3-4.
34. President Dwight D. Eisenhower, "President Eisenhower's Farewell to the Nation." Published as Appendix B in Melman, *Pentagon Capitalism*, 235-39; Charles E. Nahtanson, "The Militarization of the American Economy," in David Horowitz, ed., *Corporations and the Cold War* (New York: Monthly Review Press, 1969), 209.
35. Christopher H. Pyle, *Military Surveillance of Civilian Politics, 1967-1970* (New York: Garland Publishing, 1986), 69-81, "Military Intelligence Overkill," in Sam J. Ervin, et. al., *Uncle Sam is Watching You: Highlights from the Hearings of the Senate Subcommittee on Constitutional Rights* (Washington, DC: Public Affairs Press, 1971), 74-147; Christopher H. Pyle, "Be Afraid, Be Very Afraid, of Spying by U.S. Army," December 5, 2002, <http://bintjpeil.com>; Seth F. Kreimer, "Watching the Watchers: Surveillance, Transparency, and Political Freedom in the War on Terror," *University of Pennsylvania Journal of Constitutional Law* 133 (September 2004): 138-44; Frank J. Donner, *The Age of Surveillance* (New York: Alfred A. Knopf, 1980), 287-320.
36. "Computers Carried Army Files; MIT Investigation Underway," *The Tech*, April 11, 1975, <http://tech.mit.edu>; Hafner and Lyon, *Where Wizards Stay Up Late*, 231; Gibbons, *The U.S. Government and the Vietnam War*, 854.
37. "Ervin Discusses Privacy," *The Tech*, April 11, 1975, <http://tech.mit.edu>.
38. Arthur R. Miller, "The Surveillance Society," in Ervin, et. al., *Uncle Sam is Watching You*, 25-26.
39. FBI COINTELPRO documents quoted (and displayed) in Noam Chomsky, "Introduction," in Nelson Blackstock, ed., *COINTELPRO: The FBI's Secret War on Political Freedom* (New York: Pathfinder, 1988), 15-16, 25-33.
40. Matthew M. Aid and William Burr, "Secret Cold War Documents Reveal NSA Spied on Senators," *Foreign Policy*, September 25, 2013, <http://foreignpolicy.com>.
41. William Blum, *Rogue State* (Monroe, ME: Common Courage, 2005), 271-74, and "Anti-Empire Report #118," June 26, 2013, <http://williamblum.org>.
42. See John Bellamy Foster and Robert W. McChesney, *The Endless Crisis* (New York: Monthly Review Press, 2012).
43. William Safire, "You Are a Suspect," *New York Times*, November 14, 2002, <http://nytimes.com>; Shane Harris, *The Watchers: The Rise of America's Surveillance State* (New York: Penguin, 2010), 194-235, and "Total Recall," *Foreign Policy*, June 19, 2013, <http://foreignpolicy.com>; "Threats and Responses," *New York Times*, July 29, 2003, <http://nytimes.com>; "Pentagon Prepares a Future Market on Terror Attacks," *New York Times*, July 29, 2003; Whitfield Diffie and Saul Landau, *Privacy on the Line* (Cambridge, MA: The MIT Press, 1998), 66-67; "Chief Takes Over New Agency to Thwart Attacks on U.S.," *New York Times*, February 13, 2002;

- White House, National Security Decision Directive Number 145, "National Policy on Telecommunications and Automated Information Security Systems," September 17, 1984, <http://fas.org>; Chalmers Johnson, *Dismantling the Empire* (New York: Henry Holt, 2010), 104-5.
44. Fred Magdoff and John Bellamy Foster, "Stagnation and Financialization: The Nature of the Contradiction," *Monthly Review* 66, no. 1 (May 2014): 9.
45. Harry Magdoff and Paul M. Sweezy, "Production and Finance," *Monthly Review* 35, no. 1 (May 1983): 1-13; Paul M. Sweezy, "More (or Less) on Globalization," *Monthly Review* 49, no. 4 (September 1997): 1-4.
46. See Nomi Prins, *All the Presidents' Bankers: The Hidden Alliances that Drive American Power* (New York: Nation Books, 2014).
47. See Michael Lewis, *Flash Boys* (New York: WW. Norton, 2014).
48. Christian Parenti, *The Soft Cage: Surveillance in America* (New York: Basic Books, 2003), 91-92, 96.
49. Dawson, *The Consumer Trap*, 51.
50. CBS 60 Minutes, "The Data Brokers: Selling Your Personal Information," March 9, 2014, <http://cbsnews.com>; "Never Heard of Axiom?," *Fortune*, February 23, 2004, <http://money.cnn.com>.
51. CBS 60 Minutes, "The Data Brokers"; "Never Heard of Axiom?"; Lois Beckett, "Everything We Want to Know About What Data Brokers Know About You," *ProPublica*, September 13, 2013, <https://propublica.org>; U.S. Senate, Staff Report for Chairman [Jay] Rockefeller, Office of Oversight and Investigations Majority Staff, Committee on Commerce, Science, and Transportation, "A Review of the Data Broker Industry," December 18, 2013, 29; <http://commerce.senate.gov>; Alice E. Marwick, "How Your Data Are Being Deeply Mined," *New York Review of Books*, January 9, 2014, <http://nybooks.com>.
52. "What Chase and Other Banks Won't Tell You About Selling Your Data," *Forbes*, October 17, 2013, <http://forbes.com>.
53. Harris, *The Watchers*, 322-29.
54. "Financial Terrorism: The War on Terabytes," *Economist*, December 31, 2011, <http://economist.com>.
55. *Ibid*; Mortimer Zuckerman, "How to Fight and Win the Cyberwar," *Wall Street Journal*, December 6, 2010, <http://online.wsj.com>; James Bamford, "The Secret War," *Wired*, June 12, 2013, <http://wired.com>.
56. Haftner and Lyon, *Where Wizards Stay Up Late*, 242-56; Robert W. McChesney, *Digital Disconnect* (New York: New Press, 2013), 102-4.
57. On the Telecommunications Act of 1996, see Robert W. McChesney, *The Problem of the Media* (New York: Monthly Review Press, 2004), 51-56.
58. John Bellamy Foster and Hannah Holleman, "The Financial Power Elite," *Monthly Review* 62, no. 1 (May 2010): 1-19.
59. Bill Gates, *The Road Ahead* (New York: Viking, 1995), 171, 241-42, and "Keynote Address," in O'Reilly Associates, ed., *The Internet and Society* (Cambridge, MA: Harvard University Press, 1997), 32; Michael Dawson and John Bellamy Foster, "Virtual Capitalism," in Robert W. McChesney, Ellen Meiksins Wood, and John Bellamy Foster, eds., *Capitalism and the Information Age* (New York: Monthly Review Press, 1998), 51-67.
60. McChesney, *Digital Disconnect*, 103-37.
61. McChesney, *Digital Disconnect*, 158.
62. Beatrice Edwards, *The Rise of the American Corporate Security State* (San Francisco: Berrett-Koehler, 2014), 41 (reprinted in this issue, 54); Mark Karlin, "Six Reasons to Be Afraid of the Private Sector/Government Security State" (interview with Beatrice Edwards), *Truthout*, May 16, 2014, <http://truth-out.org>.
63. Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Henry Holt, 2014), 114.
64. Luke Harding, *The Snowden Files* (New York: Vintage, 2014), 202.
65. "Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security," *ProPublica*/*New York Times*, September 5, 2013, <http://propublica.org>; "Microsoft Handed the NSA Access to Encrypted Messages," *Guardian*, July 11, 2013, <http://theguardian.com>; Greenwald, *No Place to Hide*, 112-15.
66. "Exclusive: Secret Contract Tied NSA and Security Industry Pioneer," *Reuters*, December 20, 2013, <http://reuters.com>.
67. "C.I.A. Is Said to Pay AT&T for Call Data," *New York Times*, November 7, 2013, <http://nytimes.com>.
68. Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *Guardian*, June 6, 2013, <http://theguardian.com>; "CIA Is Said to Pay AT&T for Call Data," *New York Times*, November 7, 2013, <http://nytimes.com>; Electronic Frontier Foundation, "NSA Spying on Americans," <https://eff.org>.
69. "Microsoft, Facebook, Google, and Yahoo Release US Surveillance Requests," *Guardian*, February 3, 2014, <http://theguardian.com>.
70. Larry Greenemeir, "The Drone Wars," *Scientific American*, September 2, 2011, <http://scientificamerican.com>.
71. "Why Facebook and Google Are Buying Into Drones," *Guardian*, April 20, 2014, <http://theguardian.com>; Denise Young, "The Edge of Possibility: Regina Dugan," *Virginia Tech Magazine* 35, no. 4, Summer 2013, <http://vtmag.vt.edu>; Alan McDuffie, "Darpa Turns Aging Surveillance Drones Into Wi-Fi Hotspots," *Wired*, April 14, 2014, <http://wired.com>.
72. "U.S. Marketing Spending Exceeded \$1 Trillion in 2005," *Metrics* 2.0, June 26, 2006, <http://metrics2.com>; John Bellamy Foster, Hannah Holleman, and Robert W. McChesney, "The U.S. Imperial Triangle and Military Spending," *Monthly Review* 60, no. 5 (October 2008): 1-19; U.S. Bureau of Economic Analysis, *Survey of Current Business*, May 2008, 43, <http://bea.gov>.
73. Max Haiven, "Financialization and the Cultural Politics of Securitization," *Cultural Politics* 9, no. 3 (2013): 239-62.
74. Johnson, *Dismantling the Empire*, 104-5.
75. *Frontline*, "United States of Secrets," May 13, 2014, <http://pbs.org>; Ryan Lizza, "State of Deception," *New Yorker*, December 16, 2013, <http://newyorker.com>; Greenwald, *No Place to Hide*, 95-97; Electronic Frontier Foundation, "How the NSA's Domestic Spying Program Works," <https://eff.org>.
76. "Booz Allen, the World's Most Profitable Spy Organization," *Bloomberg Business Week*, June 20, 2013, <http://businessweek.com>; "Booz Allen Executive Leadership: John M. (Mike) McConnell, Vice Chairman," accessed May 30, 2014, <https://boozallen.com>.
77. Greenwald, *No Place to Hide*, 101; Glenn Greenwald and Ewen MacAskill, "Boundless Informant," *Guardian*, June 11, 2013, <http://theguardian.com>.
78. Greenwald, *No Place to Hide*, 48; "Ex-NSA Chief Details Snowden's Hiring at Agency, Booz Allen," *Wall Street Journal*, February 4, 2014, <http://online.wsj.com>.
79. Greenwald, *No Place to Hide*, 108.
80. Harding, *The Snowden Files*, 197-99.
81. Harding, *The Snowden Files*, 204.
82. Harding, *The Snowden Files*, 208-14.
83. "How We Know the NSA had Access to Internal Google and Yahoo Cloud Data," November 4, 2013, <http://washingtonpost.com>; Electronic Frontier Foundation, "How the NSA's Domestic Spying Program Works."
84. Harding, *The Snowden Files*, 203.
85. James Ridgeway, "Wesley Clark Remains Caged on the Stump," *Village Voice*, January 13, 2004, <http://villagevoice.com>; "Tiversa Advisory Board: General Wesley Clark," accessed May 30, 2014, <http://tiversa.com>; "Ex-NSA Chief Details Snowden's Hiring at Agency, Booz Allen."
86. "Similarities Seen in Leaks by Snowden, Manning," *Baltimore Sun*, June 10, 2013, <http://articles.baltimore-sun.com>.
87. On such groups see Heidi Boghosian, *Spying on Democracy* (San Francisco: City Light Books, 2013), 265-89.
88. John Nichols and Robert W. McChesney, *Dollarocracy* (New York: Nation Books, 2013).
89. On the global labor arbitrage see Foster and McChesney, *The Endless Crisis*, 137-54.
90. Adam Rawnley, "Can Darpa Fix the Cybersecurity Problem from Hell?," *Wired*, August 5, 2011, <http://wired.com>.

# Electronic Communications Surveillance

LAUREN REGAN

*“I think you’re misunderstanding the perceived problem here, Mr. President. No one is saying you broke any laws. We’re just saying it’s a little bit weird that you didn’t have to.”*—JOHN OLIVER on *The Daily Show*<sup>1</sup>

The government is collecting information on millions of citizens. Phone, Internet, and email habits, credit card and bank records—virtually all information that is communicated electronically is subject to the watchful eye of the state. The government is even building a nifty, 1.5 million square foot facility in Utah to house all of this data.<sup>2</sup> With the recent exposure of the NSA’s PRISM program by whistleblower Edward Snowden, many people—especially activists—are wondering: How much privacy do we actually have? Well, as far as electronic privacy, the short answer is: None. None at all. There are a few ways to protect yourself, but ultimately, nothing in electronic communications is absolutely protected.

In the United States, surveillance of electronic communications is governed primarily by the Electronic Communications Privacy Act of 1986 (ECPA), which is an extension of the 1968 Federal Wiretap act (also called “Title III”) and the Foreign Intelligence Surveillance Act (FISA). Other legislation, such as the USA PATRIOT Act and the Communications Assistance for Law Enforcement Act (CALEA), supplement both the ECPA and FISA.

The ECPA is divided into three broad areas: wiretaps and “electronic eavesdropping,” stored messages, and pen registers and trap-and-trace devices. Each degree of surveillance requires a particular burden that the government must meet in order to engage in the surveillance. The highest burden is in regards to wiretaps.

---

**LAUREN REGAN** is the executive director and staff attorney of the Civil Liberties Defense Center in Eugene, Oregon. This information is constantly changing; to keep yourself updated, consider becoming a member of the Civil Liberties Defense Center and receive our weekly action alerts and updates (<http://cldc.org>). The information contained in this article is not intended as legal advice nor does it form an attorney-client relationship. Thanks to Cooper Brinson at the University of Oregon for research assistance on this article.

## Wiretapping and Electronic Eavesdropping

Under ECPA, it is unlawful for any person to intercept or attempt to intercept wire, oral, or electronic communications by means of an electronic, mechanical, or any other device unless such conduct is authorized or not covered.<sup>3</sup> Wiretaps are unique in that they capture the content of communications, i.e., they reveal the purpose and meaning of a particular communication, not just the outlying “metadata.”<sup>4</sup> Interestingly, silent video surveillance is not prohibited under this particular statute.

Prior to the adoption of ECPA or FISA, in 1967 the U.S. Supreme Court in *Katz v. United States*, formed a baseline test to determine whether the monitoring of certain communications violated the Fourth Amendment.<sup>5</sup> The test is centered on whether the individual being monitored can *reasonably expect* the communications at issue to be, in fact, private. In his concurrence, Justice Harlan summarizes the test: “there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable.”<sup>6</sup> This standard is currently the measure in deciding whether a wiretap violates the ECPA.

Some entities and situations are exempt from the prohibition on wiretapping.<sup>7</sup> For instance, businesses conducting wiretapping as a part of their ordinary business practices may be permitted to monitor communications provided that such monitoring is routinely performed and done for a “legitimate business reason.” In many jurisdictions, businesses are required to notify their employees of monitoring. Jails, prisons, and other law enforcement institutions regularly record phone and other electronic communications.<sup>8</sup>

## CALEA, FISA, and Wiretapping

Perhaps the most significant legal development in regards to wiretapping came in 1994 with the passing of the Communications Assistance for Law Enforcement Act (CALEA).<sup>9</sup> Under CALEA, telecommunications providers and manufacturers have a general “duty to cooperate in the interception of communications for Law Enforcement purposes, and for other purposes.”<sup>10</sup> Specifically, however, CALEA requires that telecommunications providers “ensure that...equipment, facilities, or services” are built in such a way as to allow federal agencies the power to monitor communications sent through such equipment, facilities, or services.<sup>11</sup> Currently, CALEA extends to telephone, Internet, and Voice over Internet Protocol (VoIP) communications.<sup>12</sup> Interestingly, telecommunications providers are not responsible for decrypting messages that have been encrypted by customers.<sup>13</sup>

As a result of the exposure of extensive domestic warrantless surveillance, and as a result of the desire of the National Security Apparatus for some form of legislative and judicial approval of the warrantless “foreign intelligence” surveillance they had long conducted, in 1978 Congress passed FISA.<sup>14</sup> The stated intent of FISA was to limit surveillance of U.S. citizens—restricting invasive surveillance techniques to collecting information on “foreign powers” and “agents of foreign powers.” Nevertheless, FISA allows the president to “authorize electronic surveillance without a court order...for periods of up to one year.”<sup>15</sup> In order for the president’s request to be granted, the attorney general must certify, in writing and under oath, that a number of conditions are satisfied. This certification is then submitted to—not reviewed by—the Foreign Intelligence Surveillance Court (FISC) and the Senate Select Committee on Intelligence. In other words, the president may authorize warrantless searches so long as the attorney general swears that the searches comply with FISA. Other federal police agencies must submit a request to FISC. The request is then denied or approved by a panel of three judges. The only catch is that this court is secret—its opinions are not subject to public scrutiny, and documents that are made public are heavily redacted. Between 1979 and 2012, federal police agencies submitted 33,942 FISA surveillance requests. Only eleven requests were denied.<sup>16</sup>

Under the Patriot Act, the powers granted to the executive branch were substantially broadened. One of the most significant changes involves the entire stated purpose of FISA. Prior to the Patriot Act, FISA required that agents seeking authorization to spy declare, “the purpose...of the surveillance is to obtain foreign intelligence information.” After the Patriot Act, the statute now requires that agents only assert, “that a *significant* purpose of the surveillance is to obtain foreign intelligence information” (emphasis added).<sup>17</sup> The change in language significantly broadens the circumstances in which surveillance may be authorized. The domestic U.S. result of this change was to void the limited protection offered by the preexisting rule that once the purpose of the warrantless foreign intelligence surveillance shifted to criminal prosecution, the fruits of ongoing “foreign intelligence” warrantless surveillance could no longer be used in court.<sup>18</sup>

Additionally, the Patriot Act amended 50 U.S.C. § 1805(c)(2)(B), to authorize what is known as a “roving wiretap.”<sup>19</sup> Essentially, a roving wiretap “allows the interception of any communications made to or by an intelligence target without specifying the particular telephone line, computer or other facility to be monitored.”<sup>20</sup> According to EPIC, “prior

law required third parties (such as common carriers and others) ‘specified in court-ordered surveillance’ to provide assistance necessary to accomplish the surveillance—under the new law, that obligation has been extended to unnamed and unspecified third parties.”<sup>21</sup>

A number of challenges have been made to the U.S. government’s domestic spy programs. However, most of the significant challenges have been tossed out on procedural grounds. With the recent revelations surrounding PRISM, what the next round of litigation offers remains to be seen.<sup>22</sup>

### **How Does the Government Actually Spy? Inherent Vulnerabilities in Electronic Communications**

#### **E-mail**

Email is extraordinarily vulnerable. Messages “travel” through a number of different channels before their arrival with the intended recipient. At any one of these channels, an email can be intercepted and its content viewed. If your email is not encrypted, the content of your messages is at its most vulnerable in terms of being viewed by a third party.<sup>23</sup>

Email messages can be intercepted and then reformatted to be sent to the intended recipient or someone else altogether. This kind of interception is called a “man-in-the-middle-attack.”<sup>24</sup> Email addresses can be disguised as another person or organization in a process called masquerading.<sup>25</sup> A more invasive and insidious form of disguise is spoofing, in which email addresses are actually forged.<sup>26</sup> Thus, Suzy may think she is getting an email from her longtime friend, Bill, but in fact, it is from an unknown third party. It’s not just private security firms or government agencies that have access to spoofing—everyday Internet users can disguise themselves with the help of websites like Fogmo.com. Emails can also be disabled through Denial of Service Attacks (DoS) or Distributed Denial of Service Attacks.<sup>27</sup> These attacks can be carried out through a variety of methods, and there is little protection against them.

#### **Mobile Phones**

Cell phones, through either triangulation or multilateration, constantly track your location.<sup>28</sup> However, many of these processes are irrelevant since many smartphones now have built in GPS that is recorded and stored.

Government agencies are typically required to get a court order before monitoring cell phone use (via a pen register and/or trap and trace device) but with the recent exposure of programs like PRISM, it’s clear that this requirement is often ignored.<sup>29</sup> These court orders are

used almost exclusively for the purpose of compelling a communications service provider to turn over records and information needed to track a cell phone user. But, with technology like “triggerfish,” federal police agencies, at least at a technical level, do not have to go through the communications company—that is, the court order would simply be a courteous formality in terms of actually getting the desired information to track a person.<sup>30</sup> Triggerfish is a technology that mimics a cell phone tower, picking up on a cell phone’s signal and essentially, through a man-in-the-middle attack, intercepts calls and reveals numbers dialed and received, locations, and other information that can pinpoint the identity of the cell phone user. In fact, some suspect that triggerfish was used to round-up the RNC [Republican National Convention]-8 in 2008.<sup>31</sup> The technology known as “Stingray” is essentially the same as triggerfish.<sup>32</sup> A similar technology called an IMSI-catcher can also be used to intercept cell phone calls and data, though its utility is limited compared to triggerfish or stingray. Tools are available in order to protect yourself when using a mobile phone.<sup>33</sup> Note, however, that like most forms of electronic communication, there is no absolute protection against surveillance. You can make it extraordinarily difficult for people or technologies to gather your data, but no protection is absolutely impassable.

### **Intelligence Programs and Methods**

Law enforcement agencies are involved in a number of multi-agency operations to spy on individuals and groups, both domestic and foreign. These include:

**Boundless Informant** is a computer system used by the NSA to compile and make sense of data collected in various data mining schemes. The system does not compile FISA data.<sup>34</sup>

**X-KEYSCORE** is a program developed and used by the NSA that provides the “widest-reaching” access to information about individuals’ online activity. The program allows its user to view emails, chats, browsing histories, and “nearly everything a typical user does on the internet.” Analysts using the program can access information with no prior authorization from courts or even a signature from a supervisor. The analyst simply fills out an online form with a brief “justification” and a time-frame for the particular data sought. Screen-shots and the NSA’s presentation illustrate the format of the system. The plug-ins used by analysts operating with X-KEYSCORE are the reason we can say: there is no online privacy. These plug-ins can uncover VPN (Virtual Private Network, used to create a secure session between a user and a



private network) and PGP (Pretty Good Privacy, (a widely used open source data encryption standard for email and files) users. And aside from these tools, I know of nothing that can make a considerable difference with respect to the protection of peoples's electronic privacy.<sup>35</sup>

DCSNet (Digital Connection Systems Network) is a surveillance system used by the FBI to wiretap cell phones (including SMS text messaging) and landlines.<sup>36</sup> The system allows agents to easily access wiretapping posts located throughout the country through a "point-and-click" interface.<sup>37</sup> DCSNet is run on a secure "Peerless IP fiber network" developed and maintained by Sprint.<sup>38</sup> The network is not connected to the public internet. DCSNet was built from the remnants of Carnivore—a spy software tool utilized by the FBI.<sup>39</sup>

NSA Call Database contains the records of "billions" of call records of U.S. citizens. The call records are from AT&T and Verizon. Most of the records collected are from citizens who are not suspected of any crime. The database is apparently the largest of its kind in the world.<sup>40</sup>

**AT&T and the NSA.** According to the Electronic Frontier Foundation (EFF):

AT&T's internet traffic in San Francisco runs through fiber-optic cables at an AT&T facility located at 611 Folsom Street in San Francisco. Using a device called a 'splitter,' a complete copy of the internet traffic that AT&T receives—email, web browsing requests, and other electronic communications sent to or from the customers of AT&T's WorldNet Internet service from people who use another internet service provider—is diverted onto a separate fiber-optic cable which is connected to a room, known as the SG-3 room, which is controlled by the NSA. The other copy of the traffic continues onto the internet to its destination.<sup>41</sup>

The exposure of this program culminated in a lawsuit, *Hepting v. AT&T*, in which EFF sued AT&T and Verizon for "violating privacy law by collaborating with the NSA in the massive, illegal program to wiretap and data-mine American's communications." After surviving the government's motion to dismiss, the case was appealed to the Ninth Circuit and then was dismissed. The court held that AT&T and Verizon have retroactive immunity from suit under amendments made to FISA in the FISA Amendments Act of 2008.<sup>42</sup>

TALON ("Threat and Local Observation Notice") was a U.S. Air Force database that stored information on individuals and groups who allegedly pose threats to the United States.<sup>43</sup> After the database was exposed for having collected mass amounts of information on peace groups and activists, the government announced that it would shut the database down and transfer data to the FBI's Guardian database.

**Guardian** (“Guardian Threat Tracking System”) is, according to the FBI, an “automated system that records, stores, and assigns responsibility for follow-up on counterterrorism threats and suspicious incidents. It also records the outcome of the FBI’s handling of terrorist threats and suspicious incidents.” To give an idea of the breadth of this system, a 2007 internal audit of the system found that between July 2004 and November 2007, 108,000 “potential terrorism-related threats, reports of suspicious incidents, and terrorist watchlist encounters” were recorded. The audit notes that “the overwhelming majority of the threat information documented in Guardian had no nexus to terrorism.”<sup>44</sup>

**ADVISE** (“Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement”) was a massive database/computer system used by Homeland Security that captured and analyzed personal data of U.S. citizens. The project was essentially a data-mining operation.<sup>45</sup>

**Magic Lantern** is a software program developed by the FBI that logs keystrokes, i.e., records what is typed. There are a number of different types of “keyloggers.”<sup>46</sup> Essentially, keystroke software like Magic Lantern bypasses the protection typically offered by encryption. Magic Lantern can be installed through an email with an attachment (a trojan horse) or through other nefarious means.<sup>47</sup> Keyloggers are typically unknown to the user being logged.

### Protecting Yourself

Here is the bottom line: *You don’t really have any privacy when it comes to electronic communication. There are no absolute protections in electronic communication. Your cell phone, email, social media, and any other form of communication are subject to surveillance.* However, in light of PRISM and the extent of NSA surveillance, the *Washington Post* has suggested a few ways to protect yourself against the NSA (note, these are *in no way* absolute protections):<sup>48</sup>

- Browse the Internet with Tor or through a “virtual private network.”<sup>49</sup>
- Use OTR to encrypt chats.<sup>50</sup>
- Use “Silent Circle” or “Redphone” to make phone calls.<sup>51</sup>
- Take out your phone battery.<sup>52</sup>

Additionally, and directly relevant to activists, Riseup has offered a number of services to protect against online surveillance.<sup>53</sup>

### Grey Intelligence and Government Collusion: Attacks upon Dissent

One of the common threats to all movements, activists, and global citizens is the attack upon the rights to privacy, organizing, and dissent


that is being wrought by the government-corporate surveillance state. Anyone who has heard the news lately should be fairly acquainted with the outrageous surveillance conducted by the NSA and several other agencies against every phone call or Facebook post you have ever made. Many might be surprised to hear that the military infiltrated and spied on peace activists in Washington.<sup>54</sup> Or that the FBI has been recruiting young women from college classrooms to spy upon, and entrap young anarchist/environmental activists while pretending to date the male victims.<sup>55</sup> And even more disturbing, the U.S. government has colluded with private corporations and extractive industries to ratchet up their COINTELPRO-esque tactics upon climate justice activists. The few constitutional protections that exist to limit the ability of the feds to spy on political organizations and activities are exploited by their partners in the “grey intelligence” realm of corporate spying.

Some 1,271 government organizations and 1,931 private companies work on programs related to counterterrorism, homeland security, and intelligence in about 10,000 locations across the United States.<sup>56</sup> “By 2007, 70 percent of the U.S. intelligence budget—or about \$38 billion annually—was spent on private contractors.” One defense analyst says that today, overall annual spending on corporate security and intelligence is roughly \$100 billion, double what it was a decade ago.<sup>57</sup>

To give you an example of how this is playing out: a climate justice group—whether fighting fracking, coal, tar sands or pipelines—engages in completely lawful, constitutionally protected First Amendment activity, like holding a banner on a street corner. Big industry creates a side business that includes “private security” and “public relations” components in order to keep their hands clean. The private spies are often former FBI head honchos who leave government service for the lucrative land of corporate paychecks, but remain well-connected to their former employers and coworkers. Private spies infiltrate the group, create problems, steal membership or financial information from the group, and sometimes hack computers and/or attempt to provoke the group to break the law (or escalate tactics without group consent). Then they bring the information back to the PR staff, who grossly and maliciously manipulate facts and create a written publication called a “Terrorist Bulletin,” which is produced and sent to fellow industry organizations, as well as federal and local law enforcement. These terrorist bulletins say things like, “This group is lawful and nonviolent now, but they are getting more militant and may become violent in the near future.” In addition, these grey intelligence organizations come up with strategies to destroy and discredit lawful political groups.<sup>58</sup>

Case in point: the U.S. Chamber of Commerce hired a law firm, who in turn, hired a consortium of private intelligence firms in order to discredit their perceived opponents in U.S. Chamber Watch, which included watchdog organizations and labor unions. As a result of a memo leaked by Anonymous (a hacktivist group), evidence of their defamatory COINTELPRO hijinks were clearly uncovered. In the “Information Operations Recommendation,” the authors state they “need to discredit the organization through the following:” snitch-jacketing the leaders, planting false information and spies within the group, and using mainstream media to embarrass and derogate the organization. They admit, “unlike some groups, members of this organization are politically connected and well established, making the US Chamber Watch vulnerable to information operations that could embarrass the organization and those associated with it” (see below).<sup>59</sup>

In addition, it has become commonplace for corporations like TransCanada to provide PowerPoint presentations to local and federal



Information Operations Recommendation

Subject: US Chamber Watch Information  
Operations Recommendation

Date: November 29, 2010

Summary

US Chamber Watch is one of the most active members of the opposition to the US Chamber of Commerce (CoC). Unlike some groups, members of this organization are politically connected and well established, making the US Chamber Watch vulnerable to information operations that could embarrass the organization and those associated with it.

Details

US Chamber Watch is well connected politically, evidenced by the established relationship between CtW and Andy Stern, and is associated with many powerful DC operatives behind the scenes. The organization typically does not use theatrical performances or overt gestures. The people in this case are less important than the organization. Therefore we need to discredit the organization through the following.

1. Paint US Chamber Watch as an operative of CtW and the unions, while at the same time highlighting the organization of the unions against the chamber. We should show also the flow of members from unions to CtW as well as the closeness of CtW and US Chamber Watch.
2. Craft a message to combat the messaging propaganda of US Chamber Watch. For example, target how the unions are being an inhibitor to progress by advocating for unrealistic individual benefits, while the Chamber continues its focus on job creation through innovation in order to showcase how the US economy prospers in the global economy. Packaged in the right mediums, such an operation can prove to be powerful.
3. Create a false document, perhaps highlighting periodical financial information, and monitor to see if US Chamber Watch acquires it. Afterward, present explicit evidence proving that such transactions never occurred. Also, create a fake insider persona and generate communications with CtW. Afterward, release the actual documents at a specified time and explain the activity as a CtW contrived operation. Both instances will prove that US Chamber Watch cannot be trusted with information and/or tell the truth.
4. Connect US Chamber Watch's radical tactics to Velvet Revolution, explaining that both entities are loosely operating together. Depending on the level of connection established, such an approach may need to be spotlighted as more of a conspiracy rather than a separate, vocal persona.
5. If needed, create two fake insider personas, using one as leverage to discredit the other while confirming the legitimacy of the second. Such work is complicated, but a well-thought out approach will give way to a variety of strategies that can sufficiently aid the formation of vetting questions US Chamber Watch will likely ask.
6. Create a humor piece about the leaders of CtW.

law enforcement, as well as District Attorneys and other prosecutors, where the tar sands industrial giant provides them with information on political organizers and advocates terrorism investigations and prosecutions of nonviolent activists engaged in political campaigns against the irreparable destruction of the planet.<sup>60</sup> I provide legal support to the Tar Sand Blockade, a Texas-based nonviolent frontlines direct action group resisting the southern portion of the TransCanada KXL pipeline.<sup>61</sup> At one lawful protest that I witnessed, local rural residents lined the side of the road holding signs in opposition to the pipeline, while other activists perched in trees that were to be cut to make way for the pipeline route. Local untrained sheriff's deputies began indiscriminately pepper-spraying the crowd of bystanders that included elders and children. After the cop riot was over, I witnessed the TransCanada representative walk up to one of the sheriff's deputies, slap him on the back, thank him for a job well done, and then offer to bring by more pepper spray to replenish the department's supplies. This outrageous collusion is not an isolated incident.

In another case, the director of the Pennsylvania Department of Homeland Security, James Powers, mistakenly sent an email to an anti-drilling activist he believed was sympathetic to the industry, warning her not to post industry terrorist bulletins online. In his email Powers wrote: "We want to continue providing this support to the Marcellus Shale Formation natural gas stakeholders while not feeding those groups fomenting dissent against those same companies."

Despite the attempts by government and corporations to crush the grassroots climate justice movements flourishing around the world, the number of activists and actions against these industries continues to grow on a daily basis. Only by taking control away from these corporations and their beholden government cronies will this egregious surveillance activity be curtailed; and the only way that will happen is by fostering a powerful mass movement capable of reclaiming our civil liberties and the virtuous right to dissent.

## Notes

1. Cited in Mike Masnick, "Daily Show Takes On NSA Surveillance: It's A Little Weird That Feds Didn't Have To Break Any Laws To Spy On Everyone," June 11, 2013, <http://techdirt.com>.

2. Howard Berkes, "Amid Data Controversy, NSA Builds Its Biggest Data Farm," June 10, 2013, <http://npr.org>.

3. The ESCA is 18 U.S.C.2511. According to

18 U.S.C.2510(6), "Person' means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation."

4. "Metadata" includes data about data, i.e., data void of necessarily meaningful content. For example, the kind of data gathered by pen registers (discussed below) that reveals the source and destination of a

communication but not the actual content of a communication is a form of metadata.

5. 389 U.S. 347 (1967), <http://law.cornell.edu/sup>.

6. *Ibid*, 361.

7. There are roughly five categories of exemptions to the prohibition of wiretapping: consent of one or more party; publicly accessible radio communications;

government officials; communication service providers; and situations involving a parent and a minor child or spouses.

8. Telephone conversations between inmates and clergy, however, are not subject to recording/monitoring. *Mockaitis v. Harderodad*, 104 F.3d 1522, 1530 (9th Cir. 1997).

9. Electronic Frontier Foundation, "CALEA: The Perils of Wiretapping the Internet," <https://eff.org/issues/calea>.

10. 141 Cong. Rec. H113-05 (Oct. 25, 1994).

11. 47 U.S.C. § 1002.

12. For example, Skype or Google Talk.

13. "A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication." 47 U.S.C. § 1002(b)(3). Interestingly, the feds (particularly the DEA) are having a very tough time decrypting Apple's built in encryption for text messages between iPhones. Dan Goodin, "Apple's iMessage Crypto Stymies Federal Eavesdropping of Drug Suspect," April 4, 2013, <http://arstechnica.com>.

14. "50 U.S. Code Chapter 36 - Foreign Intelligence Surveillance," <http://law.cornell.edu>.

15. 50 USCA § 1802.

16. "Foreign Intelligence Surveillance Act Court Orders 1979-2014," updated May 1, 2014, <http://epic.org>.

17. 50 USCA § 1804.

18. See *In re: Sealed Case No. 02-001*, 310 F.3d 717 (United States Foreign Intelligence Surveillance Court of Review 2002). The pre-existing rule was set out in *U.S. v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980). It should be noted that the author of an article in this issue of *Monthly Review*, Michael E. Tigar, as well as the issue editor, John Mage, were trial and appellate counsel for Truong.

19. "Let the Sun Set on PATRIOT - Section 206: Roving Surveillance Authority Under the Foreign Intelligence Surveillance Act of 1978," <http://w2.eff.org>.

20. "Foreign Intelligence Surveillance Act (FISA)," <http://epic.org>.

21. *Ibid.*

22. Charlie Savage, "A.C.L.U. Files Lawsuit Seeking to Stop the Collection of Domestic Phone Logs," *New York Times*, June 11, 2013, <http://nytimes.com>.

23. To learn encryption basics, see: "Message Security," <https://riseup.net/en/message-security>.

24. "Man-in-the-middle attack," <http://en.wikipedia.org>, accessed May 30, 2014. If you would like to know how to identify and defeat these kinds of attacks, see Christopher Soghoian and Sid Stamm, "Certified Lies: Detecting and Defeating

Government Interception Attacks Against SSL," paper presented at Financial Cryptography and Data Security '11, Fifteenth International Conference, March 2011, <http://files.cloudprivacy.net/ssl-mitm.pdf>.

25. Symantec, "Configuring Email Aliases and Address Masquerades," August 20, 2012, <http://symantec.com>.

26. "Email Bombing and Spamming," <http://cert.org>.

27. "Denial-of-service attack," <https://en.wikipedia.org>.

28. eHow, "How to Triangulate a Cell Phone," <http://ehow.com>; "Multilateration," <http://en.wikipedia.org>.

29. "Pen register," accessed May 30, 2104, <http://en.wikipedia.org>; "The term 'trap and trace device' means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." 18 U.S.C. §3127, <http://law.cornell.edu>.

30. Jonathan Racicot, "Cyber Espionage: The Triggerfish," November 19, 2008, <http://cyberwarfaremag.wordpress.com>.

31. Tom Burghardt, "Preemptive Policing & the National Security State: Repressing Dissent at the Republican Convention," November 18, 2008, <http://globalresearch.ca>.

32. Kim Zetter, "Feds' Use of Fake Cell Tower: Did it Constitute a Search?," November 3, 2011, <http://wired.com>; Zetter, "Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight," April 9, 2013, <http://wired.com>.

33. OsmocomBB, <http://bb.osmocom.org/trac>.

34. "Boundless Informant: NSA Explainer-Full Document Text," *Guardian*, June 8, 2013, <http://guardian.co.uk>.

35. Glenn Greenwald, "XKeyscore: NSA Tool Collects 'Nearly Everything A User Does On the Internet,'" *Guardian*, July 31, 2013, <http://theguardian.com/>

36. "DCSNet," accessed May 30, 2014, <http://en.wikipedia.org>.

37. "EFF Documents Shed Light on FBI Electronic Surveillance Technology," August 29, 2007, <http://eff.org>.

38. Susan M. Menke, "Army Guard and FBI Sign Up for less IP net," October 23, 2003, <http://gcn.com>.

39. "Carnivore (software)," accessed May 30, 2014, <http://en.wikipedia.org>.

40. Leslie Cauley, "NSA has Has Massive Database of Americans' Phone Calls," *USA TODAY*, May 11, 2006, <http://usatoday30.usatoday.com>.

41. "AT&T's Role in Dragnet Surveillance of Millions of its Customers," <https://eff.org>.

42. *In re Nat'l Sec. Agency Telecomms.*

*Records Litig. (Hepting v. AT&T Corp.)*, 671 F.3d 881, (9th Cir. 2011), <http://www2.bloomberglaw.com>.

43. Associated Press, "Pentagon To Shut Down Controversial Database," August 21, 2007, <http://nbcnews.com>.

44. U.S. Department of Justice, Office of the Inspector General, "The Federal Bureau of Investigation's Terrorist Threat and Suspicious Incident Tracking System, Audit Report 09-02," November 2008, <http://justice.gov>.

45. "Homeland Security Revives Supersnoop," *Washington Times*, March 8, 2007, <http://washingtontimes.com>.

46. Bob Sullivan, "FBI Software cracks Cracks Encryption Wall," November 20, 2001, <http://nbcnews.com>; "Keystroke logging," accessed May 30, 2014, <http://en.wikipedia.org>.

47. "Trojan horse (computing)," accessed May 30, 2014, <http://en.wikipedia.org>.

48. Timothy B. Lee, "Five Ways To Stop the NSA From Spying On You," *Washington Post*, June 10, 2013, <http://washingtonpost.com>.

49. "What is the Tor Browser Bundle?," (with instructions for use), <https://torproject.org>.

50. "Off-the-Record Messaging," <http://cyberpunks.ca/otr>.

51. "Silent Circle, The World's Most Secure Solution in Mobile Privacy," <https://silentcircle.com>; "Red Phone :: Secure Calls," October 21, 2013, <https://play.google.com/store/apps>.

52. "Mobile phone tracking," accessed May 30, 2104, <http://en.wikipedia.org>.

53. "Riseup.net Security Resources," <https://riseup.net/en/resources>.

54. Kevin Gostola, "Lawsuit: Attempted Entrapment of Activists by Military Officer & Further Evidence of Domestic Spying," February 26, 2014, <http://dissenter.fire-doglake.com>.

55. *Support Eric McDavid*, <http://support-eric.org>.

56. Dana Priest and William M. Arkin, "A Hidden World, Growing Beyond Control," *Washington Post*, July 19, 2010, <http://projects.washingtonpost.com>.

57. Adam Federman, "We're Being Watched: How Corporations and Law Enforcement Are Spying on Environmentalists," *Earth Island Journal*, Summer 2013, <http://earthisland.org>.

58. *Ibid.*

59. See Thermis, "Information Operations Recommendation," November 29, 2010, <http://images2.americanprogress.org>.

60. See <http://boldnebraska.org> for more information about the FOIA documents this group unveiled.

61. *Tar Sands Blockade*, <http://tarsands-blockade.org>.

# The New Surveillance Normal

## *NSA and Corporate Surveillance in the Age of Global Capitalism*

DAVID H. PRICE

The National Security Agency (NSA) document cache released by Edward Snowden reveals a need to re-theorize the role of state and corporate surveillance systems in an age of neoliberal global capitalism. While much remains unknowable to us, we now are in a world where private communications are legible in previously inconceivable ways, ideologies of surveillance are undergoing rapid transformations, and the commodification of metadata (and other surveillance intelligence) transforms privacy. In light of this, we need to consider how the NSA and corporate metadata mining converge to support the interests of capital.

This is an age of converging state and corporate surveillance. Like other features of the political economy, these shifts develop with apparent independence of institutional motivations, yet corporate and spy agencies' practices share common appetites for metadata. Snowden's revelations of the NSA's global surveillance programs raises the possibility that the state intelligence apparatus is used for industrial espionage in ways that could unite governmental intelligence and corporate interests—for which there appears to be historical precedent. The convergence of the interests, incentives, and methods of U.S. intelligence agencies, and the corporate powers they serve, raise questions about the ways that the NSA and CIA fulfill their roles, which have been described by former CIA agent Philip Agee as: "the secret police of U.S. capitalism, plugging up leaks in the political dam night and day so that shareholders of U.S. companies operating in poor countries can continue enjoying the rip-off."<sup>1</sup>

There is a long history in the United States of overwhelming public opposition to new forms of electronic surveillance. Police, prosecutors, and spy agencies have recurrently used public crises—ranging from the Lindbergh baby kidnapping, wars, claimed threats of organized crime and terror attacks, to marshal expanded state surveillance powers.<sup>2</sup>

---

DAVID H. PRICE is Professor of Anthropology in the Department of Society and Social Justice at Saint Martin's University. His most recent book is *Weaponizing Anthropology: Social Science in Service of the Militarized State* (CounterPunch Books, 2011).

During the two decades preceding the 9/11 terror attacks, Congress periodically considered developing legislation establishing rights of privacy; but even in the pre-Internet age, corporate interests scoffed at the need for any such protections. Pre-2001 critiques of electronic-surveillance focused on privacy rights and threats to boundaries between individuals, corporations, and the state; what would later be known as metadata collection were then broadly understood as violating shared notions of privacy, and as exposing the scaffolding of a police state or a corporate panopticon inhabited by consumers living in a George Tooker painting.

The rapid shifts in U.S. attitudes favoring expanded domestic intelligence powers following 9/11 were significant. In the summer of 2001, distrust of the FBI and other surveillance agencies had reached one of its highest historical levels. Decades of longitudinal survey data collected by the Justice Department establish longstanding U.S. opposition to wiretaps; disapproval levels fluctuated between 70–80 percent during the thirty years preceding 2001.<sup>3</sup> But a December 2001 *New York Times* poll suddenly found only 44 percent of respondents believed widespread governmental wiretaps “would violate American’s rights.”<sup>4</sup>

Public fears in the post-9/11 period reduced concerns of historical abuses by law enforcement and intelligence agencies; and the rapid adoption of the PATRIOT Act precluded public considerations of why the Pike and Church congressional committee findings had ever established limits on intelligence agencies’ abilities to spy on Americans. Concurrent with post-9/11 surveillance expansions was the growth of the Internet’s ability to track users, collecting metadata in ways that seductively helped socialize all to the normalcy of the loss of privacy.

The depth of this shift in U.S. attitudes away from resisting data collection can be seen in the public’s response in the early 1990s to news stories reporting the Lotus Corporation’s plans to sell a comprehensive CD-ROM database compiled by Equifax, consisting of Americans’ addresses and phone numbers. This news led to broad-based protests by Americans across the country angry about invasions of privacy—protests that lead to the cancellation of the product which produced results less intrusive than a quick Google search would provide today. Similarly, a broad resistance arose in 2003 when Americans learned of the Bush administration’s secretive Total Information Awareness (TIA) program. Under the directorship of Admiral John Poindexter, TIA planned to collect metadata on millions of Americans, tracking movements, emails, and economic transactions for use in predictive modeling software with hopes of anticipating terror attacks, and other



illegal acts, before they occurred. Congress and the public were outraged at the prospect of such invasive surveillance without warrants or meaningful judicial oversight. These concerns led to TIA's termination, though as the Snowden NSA documents clarify, the NSA now routinely engages in the very activities envisioned by TIA.

Four decades ago broad public outrage followed revelations of Pentagon, FBI, and CIA domestic surveillance campaigns, as news of COINTELPRO, CHAOS, and a host of illegal operations were disclosed by investigative journalists and later the Pike and Church Committees. Today, few Americans appear to care about Senator Dianne Feinstein's recent accusations that the CIA hacked her office's computers in order to remove documents her staff was using in investigations of CIA wrongdoing.<sup>5</sup>

Americans now increasingly accept invasive electronic monitoring of their personal lives. Ideologies of surveillance are internalized as shifts in consciousness embedded within political economic formations converge with corporate and state surveillance desires. The rapid expansion of U.S. electronic surveillance programs like Carnivore, NarusInsight, or PRISM is usually understood primarily as an outgrowth of the post-9/11 terror wars. But while post-9/11 security campaigns were a catalyst for these expansions, this growth should also be understood within the context of global capital formations seeking increased legibility of potential consumers, resources, resistance, and competitors.<sup>6</sup>

### **Convergence of State and Corporate Metadata Dreams**

The past two decades brought an accelerated independent growth of corporate and governmental electronic surveillance programs tracking metadata and compiling electronic dossiers. The NSA, FBI, Department of Defense, and CIA's metadata programs developed independently from, and with differing goals from, the consumer surveillance systems that used cookies and consumer discount cards, sniffing Gmail content, compiling consumer profiles, and other means of tracking individual Internet behaviors for marketing purposes. Public acceptance of electronic monitoring and metadata collection transpired incrementally, with increasing acceptance of corporate-based consumer monitoring programs, and reduced resistance to governmental surveillance.

These two surveillance tracks developed with separate motivations, one for security and the other for commerce, but both desire to make individuals and groups legible for reasons of anticipation and control. The collection and use of this metadata finds a synchronic convergence of intrusions, as consumer capitalism and a U.S. national security state

leaves Americans vulnerable, and a world open to the probing and control by agents of commerce and security. As Bruce Schneier recently observed, “surveillance is still the business model of the Internet, and every one of those companies wants to access your communications and your metadata.”<sup>7</sup>

But this convergence carries its own contradictions. Public trust in (and the economic value of) cloud servers, telecommunications providers, email, and search engine services suffered following revelations that the public statements of Verizon, Google, and others had been less than forthright in declaring their claims of not knowing about the NSA monitoring their customers. A March 2014 *USA Today* survey found 38 percent of respondents believed the NSA violates their privacy, with distrust of Facebook (26 percent) surpassing even the IRS (18 percent) or Google (12 percent)—the significance of these results is that the Snowden NSA revelations damaged the reputations and financial standing of a broad range of technology-based industries.<sup>8</sup> With the assistance of private ISPs, various corporations, and the NSA, our metadata is accessed under a shell game of four distinct sets of legal authorizations. These allow spokespersons from corporate ISPs and the NSA to make misleading statements to the press about not conducting surveillance operations under a particular program such as FISA, when one of the other authorizations is being used.<sup>9</sup>

Snowden’s revelations reveal a world where the NSA is dependent on private corporate services for the outsourced collection of data, and where the NSA is increasingly reliant on corporate owned data farms where the storage and analysis of the data occurs. In the neoliberal United States, Amazon and other private firms lease massive cloud server space to the CIA, under an arrangement where it becomes a share cropper on these scattered data farms. These arrangements present nebulous security relationships raising questions of role confusion in shifting patron–client relationships; and whatever resistance corporations like Amazon might have had to assisting NSA, CIA, or intelligence agencies is further compromised by relations of commerce. This creates relationships of culpability, as Norman Solomon suggests, with Amazon’s \$600 million CIA data farm contract: “if Obama orders the CIA to kill a U.S. Citizen, Amazon will be a partner in assassination.”<sup>10</sup> Such arrangements diffuse complicity in ways seldom considered by consumers focused on Amazon Prime’s ability to speedily deliver a My Little Pony play set for a bronny nephew’s birthday party, not on the company’s links to drone attacks on Pakistani wedding parties.

The Internet developed first as a military-communication system; only later did it evolve the commercial and recreational uses distant from the initial intent of its Pentagon landlords. Snowden's revelations reveal how the Internet's architecture, a compromised judiciary, and duplexed desires of capitalism and the national security state are today converging to track our purchases, queries, movements, associations, allegiances, and desires. The rise of e-commerce, and the soft addictive allure of social media, rapidly transforms U.S. economic and social formations. Shifts in the base are followed by shifts in the superstructure, and new generations of e-consumers are socialized to accept phones that track movements, and game systems that bring cameras into the formerly private refuges of our homes, as part of a "new surveillance normal."<sup>11</sup>

We need to develop critical frameworks considering how NSA and CIA surveillance programs articulate not only with the United States' domestic and international security apparatus, but with current international capitalist formations. While secrecy shrouds our understanding of these relationships, CIA history provides examples of some ways that intelligence operations have supported and informed past U.S. economic ventures. When these historical patterns are combined with details from Snowden's disclosures we find continuities of means, motive, and opportunity for neoliberal abuses of state intelligence for private gains.

### **The NSA and the Promise of Industrial Espionage**

Following Snowden's NSA revelations, several foreign leaders expressed outrage and displeasure upon learning that the NSA had spied on their governments and corporations, yet there has been little consideration of the meaning of the NSA's industrial spying.

The NSA is not the only government-based international hacking unit spying on global competitors. In China, the Shanghai Chinese People's Liberation Army's Unit 61398 purportedly targets U.S. corporate and government computers, with hacking campaigns supposedly seeking data providing economic or strategic advantage to the Chinese government or private businesses. Israel's Cyber Intelligence Unit (known as ISNU, or Unit 8200) has been linked to several political and economic hacking operations, including the Stuxnet worm and a recent attack on the Élysée Palace. While many Western analysts take for granted that such economic espionage networks exist elsewhere, there is little analysis of the possibility that the NSA's surveillance will be used by rogue individuals or agencies seeking economic advantages. Yet the leveraging of such information is a fundamental feature of market capitalism.

Last January, Snowden told the German ARD television network that there is “no question that the U.S. is engaged in economic spying.” He explained that, for example, “if there is information at Siemens that they think would be beneficial to the national interests, not the national security, of the United States, they will go after that information and they’ll take it.”<sup>12</sup> Snowden did not elaborate on what is done with such economic intelligence.

Snowden has released documents establishing that the NSA targeted French “politicians, business people and members of the administration under a programme codenamed US-985D” with French political and financial interests being “targeted on a daily basis.”<sup>13</sup> Other NSA documents show the agency spying on Mexican and Brazilian politicians, and the White House authorized an NSA list of surveillance priorities including “international trade relations” designated as a higher priority than counterespionage investigations.<sup>14</sup> Leaked NSA documents include materials from a May 2012 top secret presentation “used by the NSA to train new agents step-by-step how to access and spy upon private computer networks—the internal networks of companies, governments, financial institutions—networks designed precisely to protect information.”<sup>15</sup> One leaked NSA PowerPoint slide mentions the US\$120 billion a year giant Brazilian petroleum company Petrobras with a caption that “many targets use private networks,” and as the Brazilian press analysis pointed out “Petrobras computers contain information ranging from details on upcoming commercial bidding operations—which if infiltrated would give a definite advantage to anyone backing a rival bidder—to datasets with details on technological developments, exploration information.”<sup>16</sup>

In response to Snowden’s disclosures, Director of National Intelligence James Clapper admitted the NSA collects financial intelligence, but claimed it was limited to searches for terrorist financial networks and “early warning of international financial crises which could negatively impact the global economy.”<sup>17</sup> In March 2013 Clapper lied to Congress, claiming that the NSA was not collecting “data on millions or hundreds of millions of Americans.”<sup>18</sup> He has more recently claimed the NSA does not “use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of—or give intelligence we collect to—US companies to enhance their international competitiveness or increase their bottom line.”<sup>19</sup>

Over the course of several years, the NSA’s Operation Shotgiant hacked into the servers of Chinese telecommunications giant Huawei. Shotgiant

initially sought to learn about the People's Liberation Army's ability to monitor Huawei's client's communications, but the NSA later installed hidden "back doors" in Huawei's routers and digital switches—the exact activities that the U.S. government had long warned U.S. businesses that Huawei had done.<sup>20</sup> Such operations raise the possibility of the NSA gaining knowledge to be used for economic gain by the CIA, NSA employees, or U.S. corporations. When pressed on these issues, a White House spokesperson claimed "we do not give intelligence we collect to U.S. companies to enhance their international competitiveness or increase their bottom line. Many countries cannot say the same." After this NSA operation was revealed, Huawei senior executive William Plummer noted that "the irony is that exactly what they are doing to us is what they have always charged that the Chinese are doing through us."<sup>21</sup>

There are many historical examples of intelligence personnel using information acquired through the course of their work for personal gain, such as selling intelligence information to another power. But what we need to focus upon is a qualitatively different phenomenon: the use of such information for corporate profit or market speculation.

In 1972, while investigating Nixon's presidential campaign finance irregularities, the Senate Foreign Relations subcommittee discovered documents indicating that Northrop had made a \$450,000 bribe to Saudi Arabian air force generals to help secure a \$700 million Northrop F-E5 jet contract. Retired CIA agent Kim Roosevelt (then running a multinational consulting firm operating in Saudi Arabia) denied any involvement in these bribes, but the investigation uncovered documents establishing that Roosevelt used his CIA connections for financial gain. The Senate subcommittee examined correspondence from Kim Roosevelt and Northrop officials, finding "repeated references to 'my friends in the CIA' who were keeping him posted about the moves of commercial rivals."<sup>22</sup> After the subcommittee focused its attentions on other more significant instances of CIA illegal activities, Roosevelt faced no legal consequences for these activities.

The most rigorous study to date documenting intelligence data being used for economic gains in stock market trading was recently published by economists Arindrajit Dube, Ethan Kaplan, and Suresh Naidu. The authors developed empirical measures to determine whether classified knowledge of impending CIA operations has historically been used to generate profits in this manner.<sup>23</sup>

Dube, Kaplan, and Naidu recognized that most regimes historically overthrown by CIA coups had nationalized industries that were once

privately held by international corporations; post-coup these industries returned to the previous corporate owners. Therefore, foreknowledge of upcoming coups had a significant financial value in the stock market. The authors developed a series of measures to detect whether, during past CIA coups, there were detectible patterns of stock trading taking advantage of classified intelligence directives, which were known only to the CIA and President.

Their study selected only CIA coups with now declassified planning documents, which attempted to install new regimes, and in which the targeted pre-coup governments had nationalized once-private multinational industries. They sampled five of twenty-four identified covert CIA coups meeting these three criteria: Iran (1953), Guatemala (1954), Congo (1960–1961), Cuba (failed Bay of Pigs coup, 1961), and Chile (1973). Daily stock returns of companies that had been nationalized by the governments targeted by CIA coups were used to compare financial returns before presidential coup authorizations and after the coups. Dube, Kaplan, and Naidu found that four days after the authorization of coups their sample of stocks rapidly rose (before public awareness of these coming secret coups): for Congo there was a 16.7 percent increase on the day of the authorization, and a 22.7 percent return from the baseline four days later. The Guatemala stocks showed a 4.9 percent increase upon coup authorization, a 16.1 percent increase four days later, and 20.5 percent seven days later; the Iranian stocks rose 7.4 percent four days after authorization, 10.3 percent seven days later, and 20.2 percent sixteen days later. They found evidence of significant economic gains occurring in the stock market, with “the relative percentage benefit of the coup attributable to ex ante authorization events, which amount to 55.0% in Chile, 66.1% in Guatemala, 72.4% in Congo, and 86.9% in Iran.”<sup>24</sup>

Dube, Kaplan, and Naidu concluded that “private information regarding coup authorizations and planning increased the stock prices of expropriated multinationals that stood to benefit from regime change. The presence of these abnormal returns suggests that there were leaks of classified information to asset traders.”<sup>25</sup> By focusing on trading occurring at the point of the top secret presidential authorizations, they found that gains made from stock buys at the time of authorizations “were three times larger in magnitude than price changes from the coups themselves.”<sup>26</sup> It remains unknown whether those profiting were lone individuals (either CIA employees or their proxies), or whether these investments were conducted by the CIA to generate funds for its black ops.

We do not know how such past measures of intelligence-insider profiteering do or do not relate to the NSA's present global surveillance operations. While Snowden released documents (and stated that more will be forthcoming) indicating NSA surveillance of corporations around the world, we do not understand how the NSA puts to use the intelligence they collect. Even with these leaks the NSA largely remains a black box, and our knowledge of its specific activities are limited. Yet, the ease with which a middle-level functionary like Snowden accessed a wealth of valuable intelligence data necessarily raises questions about how the NSA's massive data collections may be used for self-serving economic interests. Dube, Kaplan, and Naidu establish past insider exploitations of intelligence data, and with the growth of insider-cheater capitalism of the type documented in Michael Lewis's *Flash Boys*, and expensive private inside-the-beltway newsletters, there are tangible markets for the industrial espionage collected and analyzed by the NSA and CIA under these programs. Snowden, after all, was just one of tens of thousands of people with access to the sort of data with extraordinary value on floor of global capitalism's casinos.

### **Theorizing Capitalism's Pervasive Surveillance Culture**

Notions of privacy and surveillance are always culturally constructed and are embedded within economic and social formations of the larger society. Some centralized state-socialist systems, such as the USSR or East Germany, developed intrusive surveillance systems, an incessant and effective theme of anti-Soviet propaganda. The democratic-socialist formations, such as those of contemporary northern Europe, have laws that significantly limit the forms of electronic surveillance and the collection of metadata, compared to Anglo-U.S. practice. Despite the significant limitations hindering analysis of the intentionally secret activities of intelligence agencies operating outside of public accountability and systems of legal accountability, the documents made available by whistleblowers like Snowden and WikiLeaks, and knowledge of past intelligence agencies' activities, provide information that can help us develop a useful framework for considering the uses to which these new invasive electronic surveillance technologies can be put.

We need a theory of surveillance that incorporates the political economy of the U.S. national security state and the corporate interests which it serves and protects. Such analysis needs an economic foundation and a view that looks beyond cultural categories separating commerce and state security systems designed to protect capital. The metadata,

valuable private corporate data, and fruits of industrial espionage gathered under PRISM and other NSA programs all produce information of such a high value that it seems likely some of it will be used in a context of global capital. It matters little what legal restrictions are in place; in a global, high-tech, capitalist economy such information is invariably commodified. It is likely to be used to: facilitate industrial or corporate sabotage operations of the sort inflicted by the Stuxnet worm; steal either corporate secrets for NSA use, or foreign corporate secrets for U.S. corporate use; make investments by intelligence agencies financing their own operations; or secure personal financial gain by individuals working in the intelligence sector.

The rise of new invasive technologies coincides with the decline of ideological resistance to surveillance and the compilation of metadata. The speed of Americans' adoption of ideologies embracing previously unthinkable levels of corporate and state surveillance suggests a continued public acceptance of a new surveillance normal will continue to develop with little resistance. In a world where the CIA can hack the computers of Senator Feinstein—a leader of the one of the three branches of government—with impunity or lack of public outcry, it is difficult to anticipate a deceleration in the pace at which NSA and CIA expand their surveillance reach. To live a well-adjusted life in contemporary U.S. society requires the development of rapid memory adjustments and shifting acceptance of corporate and state intrusions into what were once protective spheres of private life. Like all things in our society, we can expect these intrusions will themselves be increasingly stratified, as electronic privacy, or illegibility, will increasingly become a commodity available only to elites. Today, expensive technologies like GeeksPhone's Blackphone with enhanced PGP encryption, or Boeing's self-destructing Black Phone, afford special levels of privacy for those who can pay.

While the United States' current state of surveillance acceptance offers little immediate hope of a social movement limiting corporate or government spying, there are enough historical instances of post-crises limits being imposed on government surveillance to offer some hope. Following the Second World War, many European nations reconfigured long-distance billing systems to not record specific numbers called, instead only recording billing zones—because the Nazis used phone billing records as metadata useful for identifying members of resistance movements. Following the Arab Spring, Tunisia now reconfigures its Internet with a new info-packet system known as mesh networks that hinder



governmental monitoring—though USAID support for this project naturally undermines trust in this system.<sup>27</sup> Following the Church and Pike committees' congressional investigations of CIA and FBI wrongdoing in the 1970s, the Hughes-Ryan Act brought significant oversight and limits on these groups, limits which decayed over time and whose remaining restraints were undone with the USA PATRIOT Act. Some future crisis may well provide similar opportunities to regain now lost contours of privacies.

Yet hope for immediate change remains limited. It will be difficult for social reform movements striving to protect individual privacy to limit state and corporate surveillance. Today's surveillance complex aligned with an economic base enthralled with the prospects of meta-data appears too strong for meaningful reforms without significant shifts in larger economic formations. Whatever inherent contradictions exist within the present surveillance system, and regardless of the objections of privacy advocates of the liberal left and libertarian right, meaningful restrictions appear presently unlikely with surveillance formations so closely tied to the current iteration of global capitalism.

## Notes

1. Philip Agee, *Inside the Company: CIA Diary* (New York: Farrar, Straus & Giroux, 1975), 575.
2. David Price, "Memory's Half-Life: A Social History of Wiretaps," *CounterPunch*, August 9-13, 2013, <http://counterpunch.org>.
3. U.S. Department of Justice, *Sourcebook of Criminal Justice Statistics* (Washington, DC: U.S. Dept. of Justice, Bureau of Justice Statistics, 1994).
4. Robin Toner and Janet Elder, "Public Is Wary But Supportive On Rights Curbs," *New York Times*, December 12, 2001, <http://nytimes.com>.
5. Mark Mazzetti and Jonathan Weisman, "Conflict Erupts in Public Rebuke on CIA," *New York Times*, March 11, 2014, <http://nytimes.com>.
6. For more on state legibility, see James Scott, *Seeing Like a State* (New Haven: Yale University Press, 1998).
7. Bruce Schneier, "Don't Listen to Google and Facebook: The Public-Private Surveillance Partnership Is Still Going Strong," *Atlantic*, March 25, 2014, <http://theatlantic.com>.
8. Jon Swartz, "Consumers Are Souring on Web, Post-NSA, Survey Says," *USA Today*, April 3, 2014, <http://usatoday.com>.
9. Bruce Schneier, "Don't Listen to Google and Facebook." The four authorizations are the 1978 FISA Act, EO 12333 of 1981, 2004, & 2008, PATRIOT Act of 2001, section 215, and Section 702 of the 2008 FISA Amendment Act.
10. Norman Solomon, "If Obama Orders the CIA to Kill a U.S. citizen, Amazon Will Be a Partner in Assassination," *AlterNet*, February 12, 2014, <http://alternet.org>.
11. The phrase "new surveillance normal" is adapted from Catherine Lutz's "the military normal," in the Network of Concerned Anthropologists, eds., *Counter-Counterinsurgency Manual* (Chicago: Prickly Paradigm Press, 2009), 23-37.
12. Sam Jones, "US Spies Engaged In Industrial Espionage Will Be Jailed, Says Lawmaker," *Financial Times*, January 31, 2014, <http://ft.com>.
13. Angelique Chrisafis and Sam Jones, "Snowden Leaks: France Summons US Envoy Over NSA Surveillance Claims," *Guardian*, October 21, 2013, <http://theguardian.com>.
14. Jens Glüsing, et al., "Fresh Leak on US spying: NSA Accessed Mexican President's Email," *Spiegel*, October 20, 2013, <http://spiegel.de>.
15. "NSA Documents Show United States Spied Brazilian Oil Giant," *Da Globo*, September 9, 2013, <http://g1.globo.com>.
16. Ibid.
17. Jonathan Watts, "NSA Accused of Spying on Brazilian Oil Company Petrobras," *Guardian*, September 9, 2013, <http://theguardian.com>.
18. Brian Fung, "Darrell Issa: James Clapper Lied to Congress About NSA and Should Be Fired," *Washington Post* blog, January 27, 2014. <http://washingtonpost.com/blogs>.
19. Jonathan Watts, "NSA Accused of Spying on Brazilian Oil Company Petrobras."
20. David E. Sanger and Nicole Perloth, "NSA Breached Chinese Servers Seen as Security Threat," *New York Times*, March 22, 2014, <http://nytimes.com>.
21. Ibid.
22. Benjamin Wells, "Serving Oil, Arabs, and the CIA," *New Republic*, July 25, 1975, 10.
23. Arindrajit Dube, Ethan Kaplan, and Suresh Naidu, "Coups, Corporations, and Classified Information," *Quarterly Journal of Economics* 126, no.3 (2011): 1375-1409.
24. Ibid, 1406.
25. Ibid, 1407.
26. Ibid, 1376.
27. Carlotta Gall and James Glanz, "U.S. Promotes Network to Foil Digital Spying," *New York Times*, April 20, 2014, <http://nytimes.com>.

# The Zombie Bill

## *The Corporate Security Campaign That Would Not Die*

**BEATRICE EDWARDS**

The government-corporate surveillance complex is consolidating. What has been a confidential but informal collaboration now seeks to legalize its special status.

July 9, 2012, was a scorcher in Washington, DC, with afternoon temperatures over 100 degrees, when an audience of about fifty think-tankers convened in a third-floor briefing room of the Senate's Russell Office Building on Capitol Hill. Then-Senator John Kyl sponsored the show, although he did not appear in person. He had invited the American Center for Democracy (ACD) and the Economic Warfare Institute (EWI) to explore the topic of "Economic Warfare Subversions: Anticipating the Threat."

At the front of the room, under a swag of the heavy red draperies and the U.S. flag, sat the panel. The lineup was peculiar. The speakers, waiting for the audience to settle in, included a number of very big names from the intelligence community, including General Michael Hayden, by this time the former director of both the CIA and the NSA; James Woolsey, former CIA director; and Michael Mukasey, former Attorney General for George W. Bush.

And then there were the others. First among them was the facilitator and director of the EWI herself. Dr. Rachel Ehrenfeld was a relative unknown who, throughout the long afternoon, would aggressively use her academic title at every opportunity, an unusual practice in this company. According to the available brochure, one of the other panelists would argue that jihadists were setting the wildfires ravaging Colorado that summer. Another, who had worked with the International Monetary Fund, would present a memorable anecdote involving complex terror scenarios not even Hollywood had ever produced.

---

**BEATRICE EDWARDS** is the Executive Director and International Program Director at the Government Accountability Project in Washington, D.C., the nation's leading whistleblower protection and advocacy organization. She has more than thirty years of experience working on labor issues, anti-corruption measures, and public-service reforms both in the United States and abroad.

This article is adapted, with permission, from chapter 4 of her *The Rise of the American Corporate Security State: Six Reasons to Be Afraid*, © 2014 Berrett-Koehler Publishers.

In total, the panel included Doctor Ehrenfeld and eight white American men. At precisely 2:00 PM, Ehrenfeld approached the podium. She opened her remarks with the announcement that the United States was target-rich for economic jihad, apparently a new concept for only a few of us in the audience. We, the uninitiated, exchanged nervous glances as she went on to explain the “cutting edge threats” that kept her up at night. She pointed out that both September 11, 2001 and September 15, 2008 were potentially devastating to the United States. One attack was the work of Al-Qaeda, a foreign enemy, and the other was self-inflicted by the management of our own financial institutions. However, Ehrenfeld said, we could not rule out the possibility that economic terrorists were: (a) responsible for, or (b) learning from the economic collapse that precipitated the Great Recession. She also referenced the “flash crash” of May 6, 2010, when the Dow lost more than one thousand points in a few minutes, only to regain six hundred of them minutes later. Ehrenfeld reminded us:

Still, two years later, the joint report by the SEC [Securities and Exchange Commission] and the Commodity Futures Trading Committee did not rule out “terrorism” as a possible cause for the May 2010 “flash crash,” and the entire financial industry still has no uniform explanation of why or how this event occurred....

EWI is of the strong opinion that threats to the U.S. economy are the next great field of battle. Indeed, we are already at economic war with such state actors as China and Iran and such nonstate actors as Al-Qaeda and its affiliates. The future battlefield is vast: it not only includes the realms of cyber and space but also of banking and finance, market and currency manipulation, energy, and drug trafficking. The list could go on and on.<sup>1</sup>

Wait! We’re at economic war with China? Most of us did not know that. Apparently the Chinese don’t know it either because their government holds a large load of U.S. debt. After the European Union, the United States is China’s largest trading partner. And after Canada, China is the United States’ largest trading partner.<sup>2</sup>

And what about an economic war with Al-Qaeda? Aren’t we winning that one? We have Wall Street and the NSA. They have bitcoins and Waziristan.

The afternoon becomes increasingly fantastic. The EWI believes, Ehrenfeld informs us, that the United States faces mass terror-induced electronic/economic calamity. The fact that this has not yet occurred, Dr. Ehrenfeld cautions us, does not mean it isn’t going to.

When she finishes, she turns the microphone over to General Michael Hayden, now a principal at the Chertoff Group, a well-connected security

consulting firm run by Bush's former secretary of Homeland Security, Michael Chertoff. General Hayden stands to speak about "the most dangerous weapons in the most dangerous hands—how much should we fear hacktivists achieving state-like capabilities?" The answer to this rhetorical question is "Quite a lot." Speaking as the former director of the NSA, he tells us that we want the government to go to the cyber-domain to defend us. In that domain, practically every advantage goes to the attacker because the environment is both insecure and indispensable. In other words, he says, he can't defend us without the proper weapons.<sup>3</sup>

Like Ehrenfeld, Hayden is frightening, but unfortunately, he does not tell us that afternoon what the proper weapons are. Nonetheless, as many in the room knew, the battle to acquire them is at that very moment heating up in the U.S. Senate.

Between the two of them, Ehrenfeld and Hayden establish a scenario in which the United States is unprotected from flash crashing at the hands of terrorist hacktivists waging economic jihad, and the next speaker is no relief. Daniel Heath, the former U.S. alternate director at the International Monetary Fund and currently a managing director at Maxwell Stamp, opens his remarks by inviting the audience to imagine this scenario:

In mid-2014 Chinese creditors announce the exchange of \$2 trillion in U.S. Treasury and agency debt for exclusive food production rights in California and mineral rights in Alaska for 100 years. As the implications settle in, a significant capital outflow trend from the U.S. takes hold. Later that year, in the holiday week between Christmas and New Year's Day, a massive storm hits the East Coast. Electricity is gone, as recently in Washington. Minor but incapacitating sabotage occurs on subway systems and on other limping transport infrastructure. Most government and commercial activity ceases. Then, odd killings occur, appearing to be random, like the 2001 sniper attack in Washington's suburbs. But some are clearly assassinations of high-value targets, including the heads of two large Wall Street firms, prominent traders, and officials of the New York Fed. While security forces scramble in a state of emergency, minor biochemical attacks on East coast water supplies occur. Like the 2001 anthrax attack in Washington, direct physical damage is minimal but trust in city services is shattered. Emergency ad hoc work arrangements are found to deliver incomplete information for markets, and the financial system "browns out" then freezes. Panic spreads beyond the East coast as employers across the United States ration cash.

Heath just keeps on going. Shadowy parties might manipulate the price of oil and a real economic crisis would occur—like the one of September 15, 2008. He suggests, then, that September 2008 was actually a jihadist plot. Probably.

What if terrorists aim to engineer a renewed financial meltdown? Is it possible? How would the financial system handle a massive attack on New York City? Is enough being done to buttress financial resilience—to limit the contagion of cascading failures throughout the economy? In what ways could different kinds of terrorist attacks succeed in destabilizing our financial sector and impair the real economy?<sup>4</sup>

All of these people are creative and emotional. Just imagine what they could do if they were talking about a real pending catastrophe like climate change.

David Aufhauser, former general counsel and chief legal officer of the Treasury Department, takes the floor. He announces the title of his talk, “Transnational Crime; Unholy Allies to Disorder, Terror, and Proliferation,” and pauses to survey the room. Gauging the impact of that, he clears his throat and proceeds. Aufhauser speculates about an alliance between Iran, the Revolutionary Armed Forces of Colombia, and then-president of Venezuela Hugo Chavez. Among them, he suggests, they are about to create nuclear weapons for Venezuela. Terror, psychocrime, drug-fueled guerrilla warfare, and jihad would come together for the politically purposeful annihilation of U.S.-based banks. We must identify nodes in the corruption network and break the circuitry, Mr. Aufhauser urges everyone.<sup>5</sup>

After a few more presentations, Michael Mukasey wraps up as the final speaker. He is the hard closer, talking about legal perspectives on economic terror and the need for comprehensive electronic surveillance inside the United States. Essentially, he says, the law—whether national or international—is unequal to the task of controlling the contemporary technology of war.<sup>6</sup> The law needs to stay out of the way, he tells us. The rules won’t work and the current regime is inadequate. Criminal law punishes after the act, but in warfare, we must often take action before the bad guys act. And the only way we can do that is to monitor them, so that we can intervene before they execute their plan for us. In addition, because we don’t know exactly who the bad guys are, we’re going to have to monitor everyone, and our “too big to fail” banks must help. The NSA, the CIA, Bank of America, and Citigroup will work together to protect all of us—and our data.

Why isn’t this a comforting prospect? Perhaps because in 2012, when Dr. Ehrenfeld’s conference took place, we were still recovering from the loss of our livelihoods that occurred as a consequence of the banks’ last exercise in risk management during the run-up to the financial crisis of 2008. This reality, however, did not deter the EWI from

concluding: "In dealing with new economic threats and circumstances, the law has a strong tendency to get in the way. This is not to disparage the law but, rather, to recognize that new circumstances beg some jettisoning of old principles and the creation of new ones."<sup>7</sup>

Yes, in a democracy, the law does get in the way. Of course, the logical next question is: get in the way of what, exactly? Even without an answer to the question, this statement from a roster of former U.S. law enforcement and intelligence officials, many of whom took an oath to uphold the Constitution and the law of the United States, is unnerving.

This is the way a would-be dictator thinks. Angered by criticism of him that appears in a newspaper, the prospective autocrat wants to order the offending journalist arrested. But the law gets in the way. Frustrated by political opposition to a program he's promoting, the head of state imagines closing down the legislature. The law gets in the way. In the face of this aggravation, what is a clever tyrant to do?

Simple. Change the law.

The Cyber Intelligence Sharing and Protection Act (CISPA) is the new law that will supersede the obsolete statutes and principles now in place. In April 2012, three months before Michael Mukasey and his cronies spoke at the Economic Warfare Conference, the House of Representatives passed CISPA: legislation that would allow the keepers of the country's finances and infrastructure to share and protect the voluminous data they collect about their customers with U.S. military intelligence agencies and the Department of Homeland Security. And vice versa. The exchange could occur without warrants and beyond the reach of the Freedom of Information Act. That summer, Senator Kyl was doing his damndest to keep CISPA alive in the upper chamber, where it lacked sufficient support. The usual suspects opposed it: the ACLU, the Center for Constitutional Rights, the Electronic Privacy Information Center, the Government Accountability Project, the Electronic Frontier Foundation, and many others. For many months, those interested in the bill kept a campaign building, and Kyl's conference on that July afternoon was to alert the think-tankers to the urgent need for CISPA.

Ultimately, CISPA failed in the Senate that year, but in February 2013, Michigan Republican Congressman Mike Rogers reintroduced it in the House of Representatives, just after the president signed his executive order on cybersecurity.<sup>8</sup> As the timing of CISPA's reintroduction made clear, the executive order was regarded by the EWI and its friends as inadequate and flabby. In fact, they're right; it is a lengthy list of bureaucratic provisions that inspires neither committed support

nor opposition—the kind of thing that gives government a bad name for creating metric tons of paper work for little gain. In brief, the order calls for a cyber-security framework, together with recommendations, reports, consultations, and inconceivably complex policy coordination. The drafters, however, did learn from the objections to CISPA: the executive order did not explicitly weaken existing privacy laws or require specific collection of data. Nor did it put an intelligence agency in the lead for the development of a cyber-security framework.

In the meantime, CISPA was making its way through the Congress, and on April 19, 2013, the bill once again passed the House with a few half-baked privacy protection amendments tacked on. It then headed for the Senate, where it had considerable support. Opponents called it “zombie legislation” because it refused to stay dead after it was defeated in 2012, even for six months.

There is a determination—a tenacity and relentlessness—about the campaign for CISPA that seems unusual, even now. The forces lined up behind it are impressive: General Dynamics, Lockheed Martin, General Electric, Northrop Grumman, SAIC, Google, Yahoo, the U.S. Chamber of Commerce, IBM, Boeing, the Business Roundtable, Time Warner Cable, American Petroleum Institute, among many others. Bank of America and Citigroup support CISPA behind the veil of the American Bankers Association and the Financial Services Roundtable. Google, Yahoo, and Microsoft also signed on through a proxy: an industry association called TechNet. It’s fairly safe to say that when you’re on the other side of the issue from this league, you’re at a distinct disadvantage.

For the U.S. public, the stakes in the CISPA battle are high, which explains the resolve behind the corporate campaign for it. A tip sheet called “Tech Talker” explains what’s in play here for the average citizen: “We’re talking about the government legally reading your emails, Facebook messages, your Dropbox files, and pretty much anything else you had stored online, in the cloud.”<sup>9</sup>

That sums it up.

On February 14, the Business Roundtable released a page of points explaining the position of its membership in support of CISPA:

- “From our perspective, the missing piece of effective cyber-security is robust, two-way information sharing, with appropriate legal and privacy protection, between business and government.
- The current information sharing environment is not supported by strong legal protections to safeguard companies that share and receive cyber-security information from civil or criminal action.

- Furthermore, there are not nearly enough security clearances. In many cases, only one or two employees are cleared even within very large global enterprises, which create difficulties in communicating problems and acting quickly across global operations.”<sup>10</sup>

The fight for CISPACT continued through 2013.

In June, however, the CISPACT campaign hits a snag: the Snowden disclosures. Edward Snowden began releasing documents that expose the United States as the major cyber-attacker in the world. It's not the Russians, Chinese, or Iranians. Nor do Somali and Yemeni jihadists pose serious cyber-threats to U.S. banking systems and electronic communications. The Snowden revelations are extremely inconvenient for the government-corporate surveillance complex because the hefty expenditures for the next round of cyber-battles depend on a persuasive and (at the very least) semi-hysterical cyber-terror narrative. Billions are at stake, and even if we already know the truth, the Business Roundtable and the NSA aren't going down without a struggle.

It is 8:00 AM on October 30, 2013. Washington is socked in for a dreary, drizzling day, as the cyber-security crowd gathers once again at the Ronald Reagan Trade Center, three blocks from the White House. They will hear from a lineup of cyber-experts on the threats to critical infrastructure posed by “those who would do us harm.” This clumsy reference to our putative antagonists will be used throughout the morning. As the experts talk about the calamitous consequences of a cyber-attack on Wall Street or our electric power grid, they never actually specify who is going to do this. Or why. In fact, the whole threat rests on the juvenile assumption that someone or some government—maybe Russia or a hacktivist group—will cause a disaster just because they can. Well, maybe they can.

Around noon, Keith Alexander, director of the NSA, sits down for an onstage interview. It's about fifteen minutes in, and he's behaving badly. He's trying to be flip and coy with his very pretty interviewer, Trish Regan of Bloomberg, but he's not coming off well. He's too old and geeky to be at all amusing in this way. Regan asks him a question about NSA capabilities, and Alexander answers, “I don't know. What do you think?”

She looks slightly perplexed. “But I asked you.”

“And I asked you,” says Alexander. He seems to be having a good time, but there's a certain amount of embarrassed coughing and seat shifting in the audience.

Silent moments pass, and Alexander begins to fluster; it seems that Regan is distracted by someone talking to her through her earpiece.



“General,” she finally says, “this is just coming across the wire now, and we have no confirmation, but the *Washington Post* is breaking a story that the NSA has backdoor access to data from Google and Yahoo. Is that true?”

A hush falls on the anxious audience. Instantly, Alexander is a different person altogether. Gone is the flirty goofball who wants the pretty lady to like him. In his place is the cagey politician with an awkward yes/no question on his hands.

He looks earnest and deeply concerned as he replies. “This is not the NSA breaking into any databases. It would be illegal for us to do that. So I don’t know what the report is, but I can tell you factually: we do not have access to Google servers, Yahoo servers, dot-dot-dot. We go through a court order.”

Later, it turns out that the keywords in this answer are server and database. The *Post* report did not say that the NSA broke into databases and servers. Rather the newspaper reported that the agency taps into the cables that transmit data between servers. So with a barely perceptible sidestep, Keith Alexander gives a truthful answer to a question that wasn’t asked and deftly misleads everyone listening to him.

It’s impressive really. Alexander did this without batting an eye. Unless he knew that the story was about to break, he denied the truth extemporaneously without actually lying.

Regan retreats to safer questions: “Are we catching the bad guys?” she asks.

Alexander pauses again. This time, however, it is probably because it’s not clear, even to him, who the bad guys are.

Except for one bad guy. Everyone knows who he is. Without saying so this morning, it is obvious that the only identified adversary for this group is Edward Snowden. His name comes up again and again. Around 10:30 AM, one speaker becomes visibly agitated at the idea that Snowden’s disclosures have undermined the case for closer collaboration between intelligence agencies and private corporations about cyber-threats—have quite possibly shot down CISPA for good and all. Larry Clinton, CEO at Internet Security Alliance, bursts out with his opinion that surveillance and cyber-sharing are completely distinct. Real-time, network-speed, machine-to-machine information exchange on cyber-threats has nothing to do with privacy, he asserts with exasperation. His head has turned red and he’s looking at us as if we’re stupid. “It’s a completely different process,” he winds up.

Then there comes a question from the floor: “So why do you need legal immunities?”

This is the question Bill Binney—the former NSA official turned whistleblower, represented by the Government Accountability Project (GAP)—keeps asking. And the discussion at the Bloomberg event this morning shows that these people want legal immunities. The executive order is not good enough. The just-published cyber-security framework coming out of the White House isn’t sufficient, either. There has to be legislation providing immunity. Threatened infrastructure—80 percent plus of which is privately owned and controlled—is not exchanging cyber-info without protection from the courts. This morning, after all is said and done, that much is very, very obvious.

The reintroduction of CISPA in the House of Representatives provoked an angry outcry from the civil liberties people. In the United States, when we focus, we tend to have a horror of intrusive government. This comes from the old days when the British quartered their horses in our parlors without asking permission, which would almost certainly have been refused. We pay taxes grudgingly; we suspect social programs of widespread fraud; we fear that a repressive police force will confiscate our shotguns someday soon. The only way to convince Americans to go along with the CISPA initiative is to crank up the terror machine again. This explains the quasi-psychotic tone of the briefing by the EWI in July 2012, as well as the nebulous catalog of cyber-debacles alluded to at the Bloomberg conference.

Our history—the Red Scare of the 1920s, the internment of the Japanese during the Second World War, and the witch-hunts of McCarthy era—shows that however free and proud and fierce we consider ourselves, we willingly surrender our civil rights when we believe we’re in danger. Each of these groups came under attack by a government that portrayed them as treacherous: the Reds of the 1920s were swarthy, low-class brutes; the Japanese were clannish Asians who were too smart for their own good and wore tiny little glasses; and Communists were hirsute, ugly men in cheap brown suits and therefore untrustworthy for that reason alone.

After 9/11, all the old scare tactics came to life. Arab men, of course, became the objects of extreme suspicion. In the rapidly evolving national imagination, it was impossible to reason with them as representatives of other countries because they’re fanatical and insane. They blow themselves up believing that they’re going to paradise where they will debauch seventy-two virgins. In the meantime, they bugger young

boys and one another. They have menacing headgear, and their women, whom they treat badly, wear sinister masks. To protect ourselves from these evil people, we allow surveillance, torture, kidnapping, imprisonment, and execution, which are—some of us admit—also evil.

John Kiriakou, the CIA agent who revealed the United States' official torture regime, reported his shock when he encountered the actual enemy in Pakistan in 2002: teenage boys who, when captured, cried and shivered and wanted to go home. He said he found himself asking: This is it? These are kids who can't even devise plausible cover stories for themselves. This is the mortal enemy the United States mobilized to hunt down and kill?

Now, admittedly, they aren't all kids, and they aren't all inept and untrained. The attacks of September 11, 2001, were highly coordinated, but then every propaganda campaign has a kernel of truth at its center. Effective official lies are always based on some credible fact. It's the extrapolation that reaches the realm of the fantastic. Let's think about it.

After the Cold War ended suddenly in 1989–1990, the United States was at a loss. The first President Bush was reluctant to declare the hostilities over for fear of economic disruption in the United States and Europe and lack of political direction afterward. Declassified memos of the last meeting between then-president Ronald Reagan, Soviet leader Mikhail Gorbachev, and president-elect George H.W. Bush in 1988 reveal that Reagan and Bush were stunned by the Soviet offer to disarm unilaterally. A report prepared by the National Security Archives, which obtained the memos, concluded that Bush was unwilling “to meet Gorbachev even halfway.”<sup>11</sup> Nonetheless, of course, the Cold War ended without Bush's consent. The United States then struggled through the early 1990s with economic dislocation, later floating its prosperity on an ephemeral dot-com bubble and keeping such defense appropriations as were credible based on the feeble posturing of a dilapidated North Korea. Scanning the world for a believable enemy, the miserable Pyongyang was the best the Pentagon and the intelligence agencies could produce.

The United States had a brief skirmish with Saddam in early 1991, but then President Bush realized that this was playing with fire and got out quickly. The resounding defeat of the Iraqi military brought Bush only short-lived glory, and with a faltering economy, he failed to win reelection a year later.

And then came September 11, 2001. Tom Drake, the NSA whistleblower and another GAP client, reported that one senior official at the NSA called the attack “a gift,” suggesting that 9/11 revived the agency's argument for budget increases by showing the U.S. public that real

enemies continued to plot effectively against us. Although the attacks showed the utter uselessness of our alleged defense industries and intelligence services, both raked in huge budget bonuses afterward.

As the post-9/11 years passed, though, the terrorist threat wore thin. In March 2013, the tenth anniversary of the Iraq invasion came and went as barely a blip on the daily news cycle. Paul Wolfowitz appeared on CNN and made a pathetic effort to justify his role in the fiasco, but few remarked about his reappearance. George W. Bush, who presided over the eight years of terror warfare, never surfaced at all; it was as if he no longer existed. Nor did Dick Cheney return for interviews. In 2014, the official hostilities in Afghanistan will end, and it will all be over.

Socially and economically, the United States needs such a respite. Too much of the national wealth has been squandered on the unproductive expenses of war. In 2011, the last year for which we have comprehensive statistics, the U.S. government spent more than \$700 billion for defense and international security, more than the thirteen next-highest-defense-spending countries combined.<sup>12</sup> If that kind of outlay is going to continue, with all the competing domestic deficits we have, we're going to need an imminent danger again very soon.

Beginning about eighteen months after the financial meltdown of September 2008, certain political forces began mobilizing about "the debt." U.S. budget shortfalls would soon be crippling, they warned, and the House of Representatives began to obstruct all financial efforts to operate the government. The Republican caucus in the House refused to raise the debt ceiling without concessions from the White House. Those who rode into Washington with Tea Party support wanted cuts to Medicare and Social Security, programs the corporate elite have long referred derogatorily as "entitlements." They threatened to shut down the government and refused to pass a real budget. The machinations became more and more creative. In August 2011, the Congress passed the Budget Control Act as a condition for raising the debt ceiling and avoiding national default. The act established the "sequester": across-the-board budget cuts so draconian and disabling that even the House of Representatives, in the hands of the so-called fiscal conservatives, could never allow them. The Pentagon would take a virtually unprecedented fiscal hit.

But it happened. After four months of noise about the cataclysmic consequences of the sequester, the House refused to agree on a deficit reduction program, and the cuts went into effect on March 1, 2013. The Congress let them occur. In the fall of 2013, Tea Party renegades did

shut down the government. If the defense industry was paying attention—which of course it was—fear and hate were flagging.

In Washington, though, a few prescient thinkers were getting ready and preparing a new menace: a truly frightening one. At the Government Accountability Project, where I am the executive director, we represent whistleblowers from the NSA, the CIA, and the major U.S. banks. We've learned that none of these institutions can be allowed to operate with the secrecy, privileged information, and latitude they already have. Using their current powers, intelligence agencies are already conducting wholesale surveillance of U.S. citizens while wasting billions in taxpayers' money on boondoggle projects, which, if they worked, would be unconstitutional. For their part, private banks have been leveraging loans to a point where their solvency becomes an issue, while the individual compensation for senior managers bloats into breathtaking mountains of loot.

Despite this record of repression and recklessness, both the intelligence community and the finance sector are lobbying hard for CISPA. The last time this coalition of forces tried to pass the bill (in the fall of 2012), the legislation died. Its demise was lost in the uproar over the 2012 election that occupied everyone's attention after August. And then, in February 2013, the CISPA zombie came back from the dead.

After the Snowden disclosures stopped CISPA in the summer of 2013, we gained time to think about why it is that an official exchange of public and private data beyond the reach of citizens is such a bad idea. It's alarming because it forms the backbone of an alliance between two forces that already have great power, but which do not necessarily operate in the public interest. To be sure, at their best, they do: a democratic government acts according to the dictates of the majority while respecting the rights of the minority, and a private corporation strives to produce and sell the best possible services and goods in a competitive market.

Suppose, however, they're not at their best. Suppose government is captured by finance, and finance is monopolistic and systemically fraudulent. Then suppose that a tenacious law enforcement official with a nasty secret in his personal life is investigating Corporation X. Should the secret come to light, the official could be neutralized, and the problems he or she poses for Corporation X would fade away.

*Client No. 9, aka George Fox, called the Emperor's Club from time to time to request the service of prostitutes, for which he paid handsomely. On February 13, 2008, at around 9:30 PM, a call girl named Ashley Dupré arrived at room 871 in the Mayflower Hotel in Washington, DC, to meet Client No. 9. Forty-five minutes later, George Fox arrived—by midnight, he was gone.*

*Dupré called the club then with an after-action report. This call from the Mayflower Hotel to the Emperor Club desk was recorded by the FBI.*<sup>13</sup>

George Fox was Eliot Spitzer, the former attorney general of New York. Over the course of his investigations into the fast and loose Wall Street trading in the early aughts, Spitzer had made serious enemies. One of them was Ken Langone, chairman of the compensation committee at the New York Stock Exchange. Another was Hank Greenberg, the former CEO of AIG, which in September 2008 was identified as the firm at the heart of the Wall Street collapse. Spitzer had pressured Greenberg to resign and Greenberg viscerally hated him.<sup>14</sup> Langone, too, openly detested Spitzer after the attorney general exposed him as one of the masterminds behind the spectacular \$139 million pay package given NYSE boss Richard Grasso for two years work at the not-for-profit, taxpayer-subsidized institution.

As Client No. 9, Spitzer attempted to hide his payments to the Emperor's Club. He often paid through a shell company and a small bank called North Fork, where he had also caused trouble. On one occasion, North Fork sent an unusually long and detailed Suspicious Activity Report (SAR) to the Financial Crimes Enforcement Network (FINCen), a branch of the U.S. Treasury Department. Another bank, HSBC—also a Spitzer target—generated a SAR about the shell company, and somehow, the two came together.

We know that these SARs entered the databases of the NSA for datamining purposes.<sup>15</sup> We also know that the FBI recorded Dupré's phone call about Spitzer in February 2008 and that was the end of Eliot Spitzer's political climb. The *New York Times* posted the headline "Spitzer is linked to prostitution ring" at 1:58 PM on March 10, 2008. In his book about the investigation, Peter Elkind reported that there was audible jubilation on the floor of the New York Stock Exchange and at Greenberg's Park Avenue office. According to Elkind, Greenberg received a stream of celebratory calls that afternoon, one of them from Langone, who knew details about the investigation of Spitzer that were not public.<sup>16</sup>

This is the kind of J. Edgar Hoover-esque nightmare that civil liberties groups cite when they envision the government/corporate cooperative surveillance to which we are subjected. Although Eliot Spitzer was not behaving admirably on that night in 2008, he was doing admirably good work for the public during the day. He was one of the very few public officials to challenge the reckless, value-free activities of the financial district in New York before 2008. Because of his personal misconduct, however, he is no longer working for New York state, and the damage to the public interest may go well beyond that. A fall from

grace like his serves as a warning to public interest advocates who might otherwise take on the Greenbergs and Langones of this world. If your personal life is not presentable for one reason or another, you do not want to get yourself crossways with a corporate figure who may have access to the U.S. government's database about citizens. In other words, if you're thinking about exposing waste, fraud, or abuse at a powerful corporation, think first about how the most embarrassing thing you've ever done will look on CNN.

Then there is Wikileaks, the anti-secrecy organization that released the video "Collateral Murder" on April 5, 2010. The video, filmed on the morning of July 12, 2007, showed a street in Baghdad from above—from the viewpoint of the U.S. Army Apache helicopter crew members as they shot the civilians scrambling for cover beneath them. One of the dead was a Reuters cameraman, and two of the wounded were children.

When questioned shortly after the incident, a military spokesman concealed the truth about how the Reuters cameraman died and said the army did not know how the children were injured. Through the Freedom of Information Act, Reuters tried unsuccessfully to obtain the video for years, but the recording saw the light of day only through Wikileaks. In October 2010, financial reprisal against the site began. Moneybookers, an online payment firm in the United Kingdom that processed donations to Wikileaks, suspended the website's account.<sup>17</sup>

In December 2010, PayPal, Visa, Mastercard, Western Union, and Bank of America stopped processing donations to Wikileaks, and by January, 95 percent of Wikileaks's revenue had evaporated due to the banking blockade.<sup>18</sup>

Nonetheless, the website continued to publish the secrets of the U.S. government. On November 13, 2013, Wikileaks posted the draft text of the intellectual property chapter of the Trans Pacific Partnership, a trade agreement being negotiated among the countries of the Pacific Rim. The chapter, negotiated in secret in the name of the U.S. public, contained provisions favorable to the U.S. private sector that could not pass the Congress.<sup>19</sup> If Wikileaks had not obtained and released the draft text, the public would not have known what the U.S. government was negotiating in its name. Official harassment of Wikileaks continues.

Spitzer's history and Wikileaks's difficulties are cautionary tales about a capability and cooperation that can be used to target and punish political or corporate enemies, whomever they may be. There are also forms of government/corporate surveillance cooperation that target you. On December 11, 2013, the *Washington Post* revealed that the NSA piggybacks

on Internet cookies to track users from website to website, compile their browsing history, and target them for hacking.<sup>20</sup> An Internet company such as Google has almost certainly had occasion to attach its cookies to virtually everyone who uses the Internet with any regularity at all. In brief, the *Post*'s story showed the connection between the tracking done by commercial websites in order to target commercial messages to the consumers most likely to buy from them and NSA surveillance.

The story also revealed that the NSA uses cookies to track Internet users whose messages and activities are encrypted when they switch to unencrypted browsing.<sup>21</sup> In other words, Internet users trying to protect their privacy are singled out for surveillance by the NSA through Google. This collaboration is already occurring, and as the target population we lack the tools to stop it. Finally, consider the government/corporate electronic intrusions that may be coming soon. In theory and in practice, a database built on citizens' credit card history, banking information, email, Internet browsing record, and telephony metadata, held in common by intelligence agencies and private corporations, poses a genuine threat to privacy and dissent.

For example, Peter Van Buren, a whistleblower at the U.S. State Department, asks that you think about what a telecom might do to you if you either got in its way or a surveillance partner such as the NSA requested a favor. Consider how you would live if nothing you ever did, said, or wrote appeared anywhere electronic ever. This is the scenario Van Buren imagines as potential reprisal to be visited upon you by Internet service providers if you should become a problem for them or their allies.<sup>22</sup> You are simply deleted and blocked from email, social media, and search engines. Without your knowledge or consent, online access to your public records is restricted. You are deleted from Facebook, Twitter, LinkedIn, Gmail, and the rest. In the near future—if it is not the case already—you will have problems communicating with friends, finding a job, renting an apartment, buying a house, voting, getting a credit card, and as time passes, doing just about anything. You will be the last person on earth with a book of stamps and a box of stationery. With CISPA in place, you will have no legal remedy to digital exile. No matter what the damages, no one will be liable.

The danger of cyber-cooperation between the public and private sectors is deeper than a simple privacy concern. We're not talking about conspiracy theories here. We're not imagining the fantastic scenario of the government snooping on you just because. We're not talking about private companies using your personal Internet habits to target you



for sales. Although these facts of life are not ideal, that's not really the point. We're talking about the collaboration between profit-making corporations and public agencies, such as the FBI and the NSA, which are empowered to target citizens for investigation and potential punishment. This threat is the real one. Secret collaboration between the power of force and the pursuit of profit is the point.

## Notes

1. Quotes from the presentation are taken from Rachel Ehrenfeld and Kenneth M. Jensen, eds., *Economic Warfare Subversions: Anticipating the Threats. A Capitol Hill Briefing* (New York: Economic Warfare Institute, July 9, 2012), <http://acdemocracy.org>, 10.
2. U.S. Census Bureau, "Top Trading Partners—December 2012," <http://census.gov>.
3. Ehrenfeld and Jensen, eds., *Economic Warfare Subversions*, 19.
4. *Ibid.*, 27, 29.
5. *Ibid.*, 46.
6. *Ibid.*, 52.
7. *Ibid.*, 8.
8. "Presidential Policy Directive--Critical Infrastructure Security and Resilience," PPD-21, February 12, 2013. <http://whitehouse.gov>.
9. Eric Escobar, "What is CISPAA?," <http://quickanddirtytips.com>.
10. John Engler, "Statement Submitted for the Record, U.S. House of Representatives Permanent Select Committee on Intelligence," February 14, 2013 hearing on "Advanced Cyber Threats Facing Our Nation," <http://intelligence.house.gov>.
11. "Declassified Documents from Reagan, Gorbachev and Bush's Meeting at Governor's Island. National Security Archives," December 8, 2008, <http://cf.gov>.
12. Brad Lumer, "America's Staggering Defense Budget, In Charts," *Washington Post*, January 7, 2013, <http://washingtonpost.com>.
13. See Peter Elkind, *Rough Justice: The Rise and Fall of Eliot Spitzer* (New York: Penguin, 2010).
14. Maurice R. Greenberg and Lawrence A. Cunningham, *The AIG Story* (New York: Wiley, 2013).
15. Michael Isikoff, "The Whistleblower Who Exposed Warrantless Wiretaps," *Newsweek*, December 12, 2008, <http://newsweek.com>.
16. Peter Elkind, "Eliot Spitzer's Flameout," April 13, 2010, <http://money.cnn.com>.
17. David Leigh and Rob Evans, "WikiLeaks Says Funding Has Been Blocked After Government Blacklisting," *Guardian*, October 14, 2010, <http://theguardian.com>.
18. "Banking Blockade," June 28, 2011, <http://wikileaks.org>.
19. "Leaked Treaty: Worse than SOPA and ACTA," November 14, 2013, *Washington's Blog*, <http://washingtonsblog.com>.
20. Ashkan Soltani, Andrea Peterson, and Barton Gellman, "NSA Uses Google Cookies to Pinpoint Targets for Hacking," *Washington Post* blogs, December 10, 2013, <http://washingtonpost.com>.
21. *Ibid.*
22. Kevin Van Buren, "Welcome to the Memory Hole," in "Tomgram: Peter Van Buren, 1984 Was an Instruction Manual," December 3, 2013, <http://tomdispatch.com>.

## MONTHLY REVIEW

## Fifty Years Ago

We have received a letter signed by W.H. Ferry, A.J. Muste, and I.F. Stone which we unfortunately lack the space to print in full. But at least we can record, and associate ourselves with, their appeal for "moral, intellectual, and financial support" of the new organization called Students for a Democratic Society, which is concentrating its energies on "creating interracial movements in key Northern and border-state communities around such issues as jobs, housing, and schools."

—LEO HUBERMAN AND PAUL SWEETZ, "Notes From the Editors,"  
*Monthly Review*, July–August 1964.

# Surveillance and Scandal

## *Weapons in an Emerging Array for U.S. Global Power*

ALFRED W. McCOY

During six riveting months in 2013–2014, Edward Snowden’s revelations about the National Security Agency (NSA) poured out from the *Washington Post*, the *New York Times*, the *Guardian*, Germany’s *Der Spiegel*, and Brazil’s *O Globo*, revealing nothing less than the architecture of the U.S. global surveillance apparatus. Despite heavy media coverage and commentary, no one has pointed out the combination of factors that made the NSA’s expanding programs to monitor the world seem like such an alluring development for Washington’s power elite. The answer is remarkably simple: for an imperial power losing its economic grip on the planet and heading into more austere times, the NSA’s latest technological breakthroughs look like a seductive bargain when it comes to projecting power and keeping subordinate allies in line. Even when revelations about spying on close allies roiled diplomatic relations with them, the NSA’s surveillance programs have come with such a discounted price tag that no Washington leader was going to reject them.

For well over a century, from the pacification of the Philippines in 1898 to trade negotiations with the European Union today, surveillance and its kissing cousins, scandal and scurrilous information, have been key weapons in Washington’s search for global dominion. Not surprisingly, in a post-9/11 bipartisan exercise of executive power, George W. Bush and Barack Obama have presided over building the NSA step by secret step into a digital panopticon designed to monitor the communications of every American and foreign leader worldwide.

What exactly was the aim of such an unprecedented program of massive domestic and planetary spying, which clearly carried the risk of controversy at home and abroad? Here, an awareness of the more than century-long history of U.S. surveillance can guide us through the billions of bytes swept up by the NSA to the strategic significance of such a program for the planet’s last superpower.<sup>1</sup> What the past reveals is a long-term relationship between

---

ALFRED W. McCOY is the J.R.W. Smail Professor of History at the University of Wisconsin-Madison. He is the author of *Policing America’s Empire: The United States, the Philippines, and the Rise of the Surveillance State* (2009), winner of the Kahin Prize from the Association for Asian Studies. An earlier version of this article appeared on TomDispatch.com on January 19, 2014.

American state surveillance and political scandal that helps illuminate the unacknowledged reason why the NSA monitors America's closest allies.

Not only does such surveillance help gain intelligence advantageous to U.S. diplomacy, trade relations, and war-making, but it also scoops up intimate information for leverage—akin to blackmail—in sensitive global dealings and negotiations of every sort. The NSA's global panopticon thus fulfills an ancient dream of empire. With a few computer key strokes, the agency has solved the problem that has bedeviled world powers since at least the time of Caesar Augustus: how to control unruly local leaders, who are the foundation for imperial rule, by ferreting out crucial, often scurrilous, information to make them more malleable.

### **The Cost of Cost-Savings**

At the turn of the twentieth century, such surveillance was both expensive and labor intensive. Today, however, unlike the U.S. Army's shoe-leather surveillance during the First World War or the FBI's break-ins and phone bugs in the Cold War years, the NSA can monitor the entire world and its leaders with only one hundred-plus probes into the Internet's fiber optic cables.<sup>2</sup>

This new technology is both omniscient and omnipresent beyond anything those lacking top-secret clearance could have imagined before the Edward Snowden revelations began.<sup>3</sup> Not only is it unimaginably pervasive, but NSA surveillance is also a particularly cost-effective strategy compared to just about any other form of global power projection. And better yet, it fulfills the greatest imperial dream of all: to be omniscient not just for a few islands, as in the Philippines a century ago, or a couple of countries during the Cold War, but now on a truly global scale.

In a time of increasing imperial austerity and exceptional technological capability, everything about the NSA's surveillance told Washington to just "go for it." This cut-rate mechanism for both projecting force and preserving U.S. global power surely looked like a must-have bargain for any American president in the twenty-first century—before new NSA documents started hitting front pages weekly, thanks to Snowden, and the whole world began returning the favor by placing Washington's leaders beneath an incessant media gaze.<sup>4</sup>

As the gap has grown between Washington's global reach and its shrinking mailed fist, as it struggles to maintain 40 percent of world armaments (as of 2012) with only 23 percent of global gross output, the United States will need to find new ways to exercise its power much more economically.<sup>5</sup> When the Cold War started, a heavy-metal U.S. military—with 500

foreign bases worldwide circa 1950—was sustainable because the country controlled some 50 percent of the global gross product.<sup>6</sup>

But as America's share of world output falls—to an estimated 17 percent by 2016—and its social-welfare costs climb relentlessly from 4 percent of gross domestic product in 2010 to a projected 18 percent by 2050, cost-cutting becomes imperative if Washington is to survive as anything like the planet's "sole superpower."<sup>7</sup> Compared to the \$3 trillion cost of the U.S. invasion and occupation of Iraq, the NSA's 2012 budget of just \$11 billion for worldwide surveillance and cyberwarfare looks like cost saving the Pentagon can ill-afford to forego.<sup>8</sup>

Yet this seeming "bargain" comes at what turns out to be an almost incalculable cost. The sheer scale of such surveillance leaves it open to countless points of penetration, whether by a handful of anti-war activists breaking into an FBI field office in Media, Pennsylvania, back in 1971 or Edward Snowden downloading NSA documents at a Hawaiian outpost in 2012.<sup>9</sup> Once these secret programs are exposed, it turns out nobody really likes being under surveillance. Proud national leaders refuse to tolerate foreign powers observing them like rats in a maze. Ordinary citizens recoil at the idea of Big Brother watching their private lives like so many microbes on a slide.<sup>10</sup>

### **Cycles of Surveillance**

Over the past century, the tension between state expansion and citizen-driven contraction has pushed U.S. surveillance through a recurring cycle. First comes the rapid development of stunning counterintelligence techniques under the pressures of fighting foreign wars; next, the unchecked, usually illegal, application of those surveillance technologies back home behind a veil of secrecy; and finally, belated, grudging reforms as press and public discover the outrageous excesses of the FBI, the CIA, or now, the NSA. In this hundred-year span—as modern communications advanced from the mail to the telephone to the Internet—state surveillance has leapt forward in technology's ten-league boots, while civil liberties have crawled along behind at the snail's pace of law and legislation.

The first and, until recently, most spectacular round of surveillance came during the First World War and its aftermath. Fearing subversion by German-Americans after the declaration of war on Germany in 1917, the FBI and Military Intelligence swelled from bureaucratic nonentities into all-powerful agencies charged with extirpating any flicker of disloyalty anywhere in America, whether by word or deed. Since only 9 percent of the country's population then had telephones, monitoring the loyalties

of some 10 million German-Americans proved incredibly labor-intensive, requiring legions of postal workers to physically examine some 30 million first-class letters and 350,000 badge-carrying vigilantes to perform shoe-leather snooping on immigrants, unions, and socialists of every sort. During the 1920s, Republican conservatives, appalled by this threat to privacy, slowly began to curtail Washington's security apparatus. This change culminated in Secretary of State Henry Stimson's abolition, in 1929, of the government's cryptography unit—the "black chamber" famous for cracking delegates' codes at the Washington Naval Conference—with his memorable admonition, "Gentlemen do not read each other's mail."<sup>11</sup>

In the next round of mass surveillance during the Second World War, the FBI discovered that the wiretapping of telephones produced an unanticipated by-product with extraordinary potential for garnering political power: scandal. To block enemy espionage, President Franklin Roosevelt gave the FBI control over all U.S. counterintelligence and, in May 1940, authorized its director, J. Edgar Hoover, to engage in wiretapping.

What made Hoover a Washington powerhouse was the telephone. With 20 percent of the country and the entire political elite by now owning phones, FBI wiretaps at local switchboards could readily monitor conversations by both suspected subversives and the president's domestic enemies, particularly leaders of the isolationist movement such as aviator Charles Lindbergh and Senator Burton Wheeler.

Even with these centralized communications, however, the Bureau still needed massive manpower for its wartime counterintelligence. Its staff soared from just 650 in 1924 to 13,000 by 1943. Upon taking office on Roosevelt's death in early 1945, Harry Truman soon learned the extraordinary extent of FBI surveillance. "We want no Gestapo or Secret Police," Truman wrote in his diary that May. "FBI is tending in that direction. They are dabbling in sex-life scandals and plain blackmail."<sup>12</sup>

After a quarter of a century of warrantless wiretaps, Hoover built up a veritable archive of sexual preferences among America's powerful and used it to shape the direction of U.S. politics. He distributed a dossier on Democratic presidential candidate Adlai Stevenson's alleged homosexuality to assure his defeat in the 1952 presidential elections, circulated audio tapes of Martin Luther King, Jr.'s philandering, and monitored President Kennedy's affair with mafia mistress Judith Exner.<sup>13</sup> And these are just a small sampling of Hoover's uses of scandal to keep the Washington power elite under his influence.

"The moment [Hoover] would get something on a senator," recalled William Sullivan, the FBI's chief of domestic intelligence during the

1960s, “he’d send one of the errand boys up and advise the senator that ‘we’re in the course of an investigation, and we by chance happened to come up with this data on your daughter...’ From that time on, the senator’s right in his pocket.” After his death, an official tally found Hoover had 883 such files on senators and 722 more on congressmen.<sup>14</sup>

Armed with such sensitive information, Hoover gained the unchecked power to dictate the country’s direction and launch programs of his choosing, including the FBI’s notorious Counterintelligence Program (COINTELPRO) that illegally harassed the civil rights and anti-Vietnam War movements with black propaganda, break-ins, and agent provocateur-style violence.<sup>15</sup> At the end of the Vietnam War, Senator Frank Church headed a committee that investigated these excesses. “The intent of COINTELPRO,” recalled one aide to the Church investigation, “was to destroy lives and ruin reputations.”<sup>16</sup> These findings prompted the formation, under the Foreign Intelligence Surveillance Act of 1978, of “FISA courts” to approve in advance requests for future national security wiretaps.<sup>17</sup>

### **Surveillance in the Age of the Internet**

Looking for new weapons to fight terrorism after 9/11, Washington turned to electronic surveillance, which has since become integral to its strategy for exercising global power. In October 2001, not satisfied with the sweeping and extraordinary powers of the newly passed PATRIOT Act, President Bush ordered the NSA to commence covert monitoring of private communications through the nation’s telephone companies without requisite FISA warrants.<sup>18</sup> Somewhat later, the agency began sweeping the Internet for emails, financial data, and voice messaging on the tenuous theory that such “metadata” was “not constitutionally protected.”<sup>19</sup> In effect, by penetrating the Internet for text and the parallel Public Switched Telephone Network (PSTN) for voice, the NSA had gained access to much of the world’s telecommunications. By the end of Bush’s term in 2008, Congress had enacted laws that not only retroactively legalized these illegal programs, but also prepared the way for NSA surveillance to grow unchecked.<sup>20</sup>

Rather than restrain the agency, President Obama oversaw the expansion of its operations in ways remarkable for both the sheer scale of the billions of messages collected globally and for the selective monitoring of world leaders.

What made the NSA so powerful was, of course, the Internet—that global grid of fiber optic cables that now connects 40 percent of

all humanity.<sup>21</sup> By the time Obama took office, the agency had finally harnessed the power of modern telecommunications for near-perfect surveillance. It was capable of both blanketing the globe and targeting specific individuals. For this secret mission, it had assembled the requisite technological tool-kit—specifically, cable access points to collect data, computer codes to break encryption, data farms to store its massive digital harvest, and supercomputers for nanosecond processing of what it was engorging itself on.<sup>22</sup>

By 2012, the centralization via digitization of all voice, video, textual, and financial communications into a worldwide network of fiber optic cables allowed the NSA to monitor the globe by penetrating just 190 data hubs—an extraordinary economy of force for both political surveillance and cyberwarfare.<sup>23</sup> With a few hundred cable probes and computerized decryption, the NSA can now capture the kind of gritty details of private life that J. Edgar Hoover so treasured and provide the sort of comprehensive coverage of populations once epitomized by secret police like East Germany's Stasi. And yet, such comparisons only go so far.

After all, once FBI agents had tapped thousands of phones, stenographers had typed up countless transcripts, and clerks had stored this salacious paper harvest in floor-to-ceiling filing cabinets, Hoover still only knew about the inner-workings of the elite in one city: Washington, D.C. By contrast, the marriage of the NSA's technology to the Internet's data hubs now allows the agency's 37,000 employees a similarly close coverage of the entire globe with just one operative for every 200,000 people on the planet.<sup>24</sup>

### **A Dream as Old as Ancient Rome**

In the Obama years, the first signs have appeared that NSA surveillance will use the information gathered to traffic in scandal, much like Hoover's FBI once did. In September 2013, the *New York Times* reported that the NSA has, since 2010, applied sophisticated software to create “social network diagrams... unlock as many secrets about individuals as possible... and pick up sensitive information like regular calls to a psychiatrist's office [or] late-night messages to an extramarital partner.”<sup>25</sup>

Through the expenditure of \$250 million annually under its Sigint Enabling Project, the NSA has stealthily penetrated all encryption designed to protect privacy. “In the future, superpowers will be made or broken based on the strength of their cryptanalytic programs,” reads a 2007 NSA document. “It is the price of admission for the U.S. to maintain unrestricted access to and use of cyberspace.”<sup>26</sup>

Imperial proconsuls, from ancient Rome to modern America, have gained both the intelligence and aura of authority necessary for dominion over alien societies by collecting knowledge—routine, intimate, or scandalous—about foreign leaders. The importance, and challenge, for hegemonies to control obstreperous local elites cannot be overstated. During its pacification of the Philippines after 1898, for instance, the U.S. colonial regime subdued the contentious Filipino leaders via pervasive policing that swept up both political intelligence and personal scandal.<sup>27</sup> And that, of course, was just what J. Edgar Hoover was doing in Washington during the 1950s and '60s.

Indeed, the mighty British Empire, like all empires, was a global tapestry woven out of political ties to local leaders or “subordinate elites”—from Malay sultans and Indian maharajas to Gulf sheiks and West African tribal chiefs. As historian Ronald Robinson once observed, the British Empire spread around the globe for two centuries through the collaboration of these local leaders and then unraveled, in just two decades, when that collaboration turned to “non-cooperation.”<sup>28</sup> After rapid decolonization during the 1960s transformed half-a-dozen European empires into one hundred new nations, their national leaders soon found themselves the subordinate elites of a spreading American global imperium. Washington suddenly needed the sort of private information that could keep such figures in line.

Surveillance of foreign leaders provides world powers—Britain then, America now—with critical information for the exercise of global hegemony. Such spying gave special penetrating power to the imperial gaze, to that sense of superiority necessary for dominion over others. It also provided operational information on dissidents who might need to be countered with covert action or military force; political and economic intelligence so useful for getting the jump on allies in negotiations; and, perhaps most important of all, scurrilous information about the derelictions of leaders useful in coercing their compliance.

In late 2013, the *New York Times* reported that, when it came to spying on global elites, there were “more than 1,000 targets of American and British surveillance in recent years,” reaching down to mid-level political actors in the international arena.<sup>29</sup> Revelations from Edward Snowden’s cache of leaked documents indicate that the NSA has monitored leaders in some thirty-five nations worldwide—including Brazilian president Dilma Rousseff, Mexican presidents Felipe Calderón and Enrique Peña Nieto, German Chancellor Angela Merkel, and Indonesia’s president Susilo Bambang Yudhoyono. Count in as well, among so many other



operations, the monitoring of “French diplomatic interests” during the June 2010 UN vote on Iran sanctions and “widespread surveillance” of world leaders during the G-20 summit meeting at Ottawa in June 2010.<sup>30</sup> Apparently, only members of the historic “Five Eyes” signals-intelligence alliance (Australia, Canada, New Zealand, and the United Kingdom) remain exempt—at least theoretically—from NSA surveillance.<sup>31</sup>

Such secret intelligence about allies can obviously give Washington a significant diplomatic advantage. During UN wrangling over the U.S. invasion of Iraq in 2002–2003, for example, the NSA intercepted Secretary-General Kofi Anan’s conversations and monitored the “Middle Six”—third world nations on the Security Council—offering what were, in essence, well-timed bribes to win votes.<sup>32</sup> The NSA’s deputy chief for regional targets sent a memo to the agency’s Five Eyes allies asking “for insights as to how membership is reacting to on-going debate regarding Iraq, plans to vote on any related resolutions” and “the whole gamut of information that could give U.S. policymakers an edge in obtaining results favorable to U.S. goals.”<sup>33</sup>

In 2010, Susan Rice, U.S. ambassador to the United Nations, asked the NSA for assistance in monitoring the Security Council debate over sanctions against Iran’s nuclear program. Through NSA monitoring of the missions of four permanent and four transient members—Bosnia, Gabon, Nigeria, and Uganda—the NSA, said Rice, “gave us an upper hand in negotiations...and provided information about various countries’ red lines,” winning approval of the U.S. position by twelve of the fifteen delegations. Apart from such special assignments, the NSA has routinely penetrated, according to Snowden’s documents, the missions or embassies of at least seventeen nations.<sup>34</sup>

Indicating Washington’s need for incriminating information in bilateral negotiations, the State Department pressed its Bahrain embassy in 2009 for details, damaging in an Islamic society, on the crown princes, asking: “Is there any derogatory information on either prince? Does either prince drink alcohol? Does either one use drugs?”<sup>35</sup>

Indeed, in October 2012 an NSA official identified as “DIRNSA,” or Director General Keith Alexander, proposed the following for countering Muslim radicals: “[Their] vulnerabilities, if exposed, would likely call into question a radicalizer’s devotion to the jihadist cause, leading to the degradation or loss of his authority.” The agency suggested such vulnerabilities could include “viewing sexually explicit material online” or “using a portion of the donations they are receiving...to defray personal expenses.” The NSA document identified

one potential target as a “respected academic” whose “vulnerabilities” are “online promiscuity.”<sup>36</sup>

Just as the Internet has centralized communications, so it has moved most commercial sex into cyberspace. With an estimated 25 million salacious sites worldwide and a combined 10.6 billion page views *per month* in 2013 at the five top sex sites, online pornography has become a global business; by 2006, in fact, it generated \$97 billion in revenue.<sup>37</sup> With countless Internet viewers visiting porn sites and almost nobody admitting it, the NSA has easy access to the embarrassing habits of targets worldwide, whether Muslim militants or European leaders. According to James Bamford, author of several authoritative books on the agency, “The NSA’s operation is eerily similar to the FBI’s operations under J. Edgar Hoover in the 1960s where the bureau used wiretapping to discover vulnerabilities, such as sexual activity, to ‘neutralize’ their targets.”<sup>38</sup>

The ACLU’s Jameel Jaffer has warned that a president might “ask the NSA to use the fruits of surveillance to discredit a political opponent, journalist, or human rights activist. The NSA has used its power that way in the past and it would be naïve to think it couldn’t use its power that way in the future.”<sup>39</sup> Even President Obama’s recently convened executive review of the NSA admitted: “in light of the lessons of our own history...at some point in the future, high-level government officials will decide that this massive database of extraordinarily sensitive private information is there for the plucking.”<sup>40</sup>

Indeed, whistleblower Edward Snowden has accused the NSA of actually conducting such surveillance. In a December 2013 letter to the Brazilian people, he wrote, “They even keep track of who is having an affair or looking at pornography, in case they need to damage their target’s reputation.”<sup>41</sup> If Snowden is right, then one key goal of NSA surveillance of world leaders is not U.S. national security, but political blackmail—as it has been since 1898.

Such digital surveillance has tremendous potential for scandal, as anyone who remembers New York Governor Elliot Spitzer’s forced resignation in 2008 after routine phone taps revealed his use of escort services; or, to take another obvious example, the ouster of France’s budget minister Jérôme Cahuzac in 2013 following wire taps that exposed his secret Swiss bank account.<sup>42</sup> As always, the source of political scandal remains sex or money, both of which the NSA can track with remarkable ease.

Given the acute sensitivity of executive communications, world leaders have reacted sharply to reports of NSA surveillance—with Chancellor Merkel demanding Five-Eyes-exempt status for Germany,

the European Parliament voting to curtail sharing of bank data with Washington, and Brazil's President Rousseff canceling a U.S. state visit and contracting a \$560 million satellite communications system to free her country from the U.S.-controlled version of the Internet.<sup>43</sup>

### **The Future of U.S. Global Power**

By starting a swelling river of NSA documents flowing into public view, Edward Snowden has given us a glimpse of the changing architecture of U.S. global power. At the broadest level, Obama's digital "pivot" complements his overall defense strategy, announced in 2012, of reducing conventional forces while expanding into the new, cost-effective domains of space and cyberspace.<sup>44</sup>

While cutting back modestly on costly armaments and the size of the military, President Obama has invested billions in the building of a new architecture for global information control. If we add the \$791 billion expended to build the Department of Homeland Security bureaucracy to the \$500 billion spent on an increasingly paramilitarized version of global intelligence in the dozen years since 9/11, then Washington has made a \$1.2 trillion investment in a new apparatus for world power.<sup>45</sup>

Just as the Philippine Insurrection of 1898 and the Vietnam War sparked rapid advances in the U.S. capacity to control subject populations, so the occupation of Iraq and Afghanistan have, since 2001, served as the catalyst for fusing aerospace, cyberspace, and biometrics into a robotic information regime of extraordinary power. After a decade of ground warfare in Afghanistan and Iraq, the Obama administration announced, in 2012, a leaner defense strategy with a 14 percent cut in infantry compensated by an increased emphasis on space and cyberspace, particularly investments to "enhance the resiliency and effectiveness of critical space-based capabilities." While this policy paper emphasized defense against the ability of state and non-state actors "to conduct cyber espionage and, potentially, cyber attacks on the United States" and the defense of "an increasingly congested and contested space environment," the administration's determination to dominate these critical areas is clear.<sup>46</sup> By 2020, this new defense architecture should be able to integrate space, cyberspace, and terrestrial combat through robotics for seamless information and lethal action.

So formidable is this security bureaucracy that Obama's recent executive review recommended regularization, not reform, of current NSA practices, allowing the agency to continue collecting American phone calls and monitoring foreign leaders into the foreseeable future.<sup>47</sup> Cyberspace offers Washington an austerity-linked arena for the exercise

of global power, albeit at the cost of trust by its closest allies—a contradiction that will bedevil America's global leadership for years to come.

To update Henry Stimson: in the age of the Internet, gentlemen don't just read each other's mail, they watch each other's porn. Even if we think we have nothing to hide, all of us, whether world leaders or ordinary citizens, have good reason to be concerned.

## Notes

1. Alfred McCoy, "Obama's Expanding Surveillance Universe," July 14, 2013, <http://tomdispatch.com>.
2. Floor Boon, Steven Derix, and Huib Modderkolk, "NSA Infected 50,000 Computer Networks with Malicious Software," November 23, 2013, <http://nrc.nl>.
3. "The NSA Files," *Guardian*, <http://the-guardian.com>.
4. James Risen and Eric Lichtblau, "How the U.S. Uses Technology to Mine More Data More Quickly," *New York Times*, June 8, 2013, <http://nytimes.com>.
5. Sam Perlo-Freeman, Elisabeth Sköns, Carina Solmirano, and Hélén Wilandh, *Trends in World Military Expenditure, 2012*, <http://books.sipri.org>; Asa Johansson, et al., "Looking to 2060: Long-Term Global Growth Prospects: A Going for Growth Report," OECD Economic Policy Papers, no. 3, <http://oecd.org>, Figure 10, 23.
6. "U.S. Has 300 Bases on Foreign Soil," *Chicago Daily Tribune*, September 11, 1954, 10; Walter Trohan, "U.S. Strategy Tied to World Air Superiority," *Chicago Daily Tribune*, February 14, 1955, 6; James R. Blaker, *United States Overseas Basing: An Anatomy of the Dilemma* (New York: Praeger, 1990), table 2; Julian Go, *Patterns of Empire: The British and American Empires, 1688 to Present* (New York: Cambridge University Press, 2011), 170.
7. International Monetary Fund, "World Economic Outlook Database," April 2011 edition, <http://imf.org>; Mark Weisbrot, "2016: When China Overtakes the US," *Guardian*, April 27, 2011, <http://guardian.co.uk>; Michael Mandelbaum, *The Frugal Superpower: America's Global Leadership in a Cash-Strapped Era* (New York: PublicAffairs, 2010), 20, 46-52, 185.
8. Laura J. Blimes and Joseph E. Stiglitz, "The Iraq War Will Cost Us \$3 Trillion, and Much More," *Washington Post*, March 9, 2008, <http://washingtonpost.com>; Scott Shane, "New Leaked Document Outlines U.S. Spending on Intelligence Agencies," *New York Times*, August 29, 2013, <http://nytimes.com>.
9. Mark Mazzetti, "Burglars Who Took On F.B.I. Abandon Shadows," *New York Times*, January 7, 2014, <http://nytimes.com>.
10. Peter Van Buren, "1984 Was an Instructive Manual," December 3, 2013, <http://tomdispatch.com>.
11. Joan Jensen, *The Price of Vigilance* (Chicago: Rand McNally, 1968), 287-89; Harold M. Hyman, *To Try Men's Souls: Loyalty Tests in American History* (Berkeley: University of California Press, 1959), 323-24; Charles H. McCormick, *Seeing Reds: Federal Surveillance of Radicals in the Pittsburgh Mill District, 1917-1921* (Pittsburgh: University of Pittsburgh Press, 1997) 202; Theodore Kornweibel, Jr., "Seeing Red": *Federal Campaigns against Black Militancy, 1919-1925* (Bloomington: Indiana University Press, 1998), 174-75; David Kahn, *The Reader of Gentlemen's Mail: Herbert O. Yardley and the Birth of American Codebreaking* (New Haven: Yale University Press, 2004), 94-103; Roy Talbert, Jr., *Negative Intelligence: The Army and the American Left, 1917-1941* (Jackson, MS: University of Mississippi Press, 1991), 208-11; Ralph Van Deman, December 15, 1928, Office of Chief of Staff, Cross Reference Card, Microform 1194, RG 350, National Archives and Records Administration; U.S. Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 94th Congress, 2d Session, *Supplementary Reports on Intelligence Activities, Book 6* (Washington, DC: U.S. Government Printing Office, 1976), 105-6; Reginald Schmidt, *Red Scare: FBI and the Origins of Anticommunism in the United States, 1919-1943* (Copenhagen: Museum Tusulanum Press, University of Copenhagen, 2000), 324-28, 368; James Bamford, "Building America's Secret Surveillance State," *Reuters*, June 10, 2013, <http://blogs.reuters.com>.
12. Federal Bureau of Investigation, "A Brief History of the FBI," <http://fbi.gov>; Tim Weiner, *Enemies: A History of the FBI* (New York: Random House, 2012), 77, 86-90, 134-35; Anthony Summers, "The Secret Life of J. Edgar Hoover," *Guardian*, December 31, 2011, <http://theguardian.com>.
13. Weiner, *Enemies*, 178, 249-50; Michael O'Brien, "The Exner File—Judith Campbell Exner, John F. Kennedy's Mistress," *Washington Monthly*, December 1999, 36-41, <http://unz.org>; Kitty Kelly, "The Dark Side of Camelot," *People Magazine* 29, no. 8, January 29, 1988, <http://archive.people.com>. See also, Dudley Clendinning, "J. Edgar Hoover, 'Sex Deviates' and My Godfather," *New York Times*, November 25, 2011, <http://nytimes.com>; National Public Radio, "The History of the FBI's Secret 'Enemies' List," *Fresh Air*, February 14, 2012, <http://npr.org>.
14. Ronald Kessler, *The Secrets of the FBI* (New York, 2011), 37-41. See also Ronald Kessler, "Hoover's Secret Files," *Daily Beast*, August 2, 2011, <http://thedailybeast.com>; Summers, "The Secret Life of J. Edgar Hoover."
15. Todd Gitlin, "Are 'Intelligence' and Instigation Running Riot?," June 27, 2013, <http://tomdispatch.com>.
16. Mazzetti, "Burglars Who Took On F.B.I. Cast Off Shadows."
17. Seymour M. Hersh, "Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years," *New York Times*, December 22, 1974, 1; Nicholas M. Horrock, "Tightened Controls Over Agency Urged," *New York Times*, June 11, 1975, 1; Nicholas M. Horrock, "Report on Spying Released by C.I.A.," *New York Times*, July 9, 1975, 1; Nicholas M. Horrock, "Ford Bill Opposes Taps on Citizens," *New York Times*, March 17, 1976, 1; Tom Wicker, "Is Oversight Enough?," *New York Times*, May 14, 1976, 21; Linda Charlton, "Senate Gets Carter Bill to Curb Foreign Intelligence Wiretapping," *New York Times*, May 19, 1977, 1; David Burnham, "Congress Studies Bill to Require Judicial Scrutiny of Some Spying," *New York Times*, January 25, 1978, 19; David Binder, "Carter Signs Order to Reorganize Intelligence and Curb Surveillance," *New York Times*, January 15, 1978; Nicholas M. Horrock, "Senate Passes Bill to Bar Bugging in U.S. Without Court Order," *New York Times*, April 21, 1979, 17.
18. Risen and Lichtblau, "How the U.S. Uses Technology to Mine More Data More Quickly."
19. National Security Agency, Office of Inspector General, "Working Draft," March 24, 2009, 7-13, <http://apps.washingtonpost.com>. 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.
20. Barton Gellman and Laura Poitras,

- "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program," *Washington Post*, June 6, 2013, <http://articles.washingtonpost.com>.
21. Xan Rice, "Internet: Last Piece of Fibre-optic Jigsaw Falls into Place as Cable Links East Africa to Grid," *Guardian*, August 17, 2008, <http://theguardian.com>; "ITU Releases Latest Tech Figures and Global Rankings," ITU, October 7, 2013, <http://itu.int>.
22. Steven Rich and Barton Gellman, "NSA Seeks to Build Quantum Computer that could Crack Most Types of Encryption," *Washington Post*, January 2, 2014, <http://washingtonpost.com>; Domestic Surveillance Directorate, "Utah Data Center," <http://nsa.gov.1.info>; James Bamford, "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)," *Wired*, March 15, 2012, <http://wired.com>.
23. National Security Agency, "Driver 1: Worldwide SIGINT/Defense Cryptologic Platform" (2012), in Boon, Derix and Modderkolk, "NSA Infected 50,000 Computer Networks with Malicious Software."
24. Camille Tuutti, "Introverted? Then NSA Wants You," *FCW: The Business of Federal Technology*, April 16, 2012, <http://fcw.com>.
25. Risen and Poitras, "N.S.A. Examines Social Networks of U.S. Citizens."
26. Nicole Perloff, Jeff Larson, and Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," *New York Times*, September 5, 2013.
27. McCoy, "Obama's Expanding Surveillance Universe."
28. Ronald Robinson, "Non-European Foundations of European Imperialism: Sketch for a Theory of Collaboration," in Roger Owen and Bob Sutcliffe, eds., *Studies in the Theory of Imperialism* (London: Longman, 1972), 132-33, 138-39.
29. James Glanz and Andrew W. Lehren, "N.S.A. Spied on Allies, Aid Groups and Businesses," *New York Times*, December 20, 2013, <http://nytimes.com>; James Glanz and Andrew W. Lehren, "U.S. and Britain Extended Spying to 1,000 Targets," *New York Times*, December 21, 2013, <http://nytimes.com>. See also James Ball and Nick Hopkins, "GCHQ and NSA Targeted Charities, German, Israeli PM and EU Chief," *Guardian*, December 20, 2013, <http://theguardian.com>.
30. Simon Romero and Randal C. Archibald, "Brazil Angered Over Report N.S.A. Spied on President," *New York Times*, September 3, 2013, <http://nytimes.com>; Alissa J. Rubin, "French Condemn Surveillance by N.S.A.," *New York Times*, October 21, 2013, <http://nytimes.com>; Alison Smale, "Anger Growing Among Allies On U.S. Spying," *New York Times*, October 23, 2013, <http://nytimes.com>; David E. Sanger and Mark Mazzetti, "Allegation of U.S. Spying on German Leader Puts Obama at Crossroads," *New York Times*, October 25, 2013, <http://nytimes.com>; Alison Smale, "Data Suggests U.S. Spying on Merkel Dates to '02," *New York Times*, October 27, 2013, <http://nytimes.com>; Editorial, "More Damage from N.S.A. Snooping," *New York Times*, October 25, 2013, <http://nytimes.com>; Mark Mazzetti and David E. Sanger, "Tap on Merkel Provides Peek at Vast Spy Net," *New York Times*, October 31, 2013, <http://nytimes.com>; Joe Cochrane, "N.S.A. Spying Scandal Hurts Close Ties Between Australia and Indonesia," *New York Times*, November 19, 2013, <http://nytimes.com>; Ian Austen, "Ire in Canada Over Report N.S.A. Spied From Ottawa," *New York Times*, November 28, 2013, <http://nytimes.com>. See also James Ball, "NSA Monitored Calls of 35 World Leaders after US Official Handed over Contacts," *Guardian*, October 24, 2013, <http://theguardian.com>.
31. Stephen Castle and Eric Schmitt, "Europeans Voice Anger Over Reports of Spying by U.S. on Allies," *New York Times*, July 1, 2013, <http://nytimes.com>; Even MacAskill and Julian Borger, "New NSA Leaks Show How US is Bugging its European Allies," *Guardian*, June 30, 2013, <http://guardian.co.uk>; Laura Poitras, et al., "How the NSA Targets Germany and Europe," *Spiegel*, July 1, 2013, <http://spiegel.de>
32. Brian Cloughley, "Hi-Tech Fun and Games with the NSA," *CounterPunch*, October 28, 2013, <http://counterpunch.org>.
33. James Bamford, *The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America* (New York: Doubleday, 2008), 141-42. See also, "US Plan to Bug Security Council: The Text," *Guardian*, March 2, 2003, <http://theguardian.com>.
34. Charlie Savage, "Book Reveals Wider Net of U.S. Spying on Envoys," *New York Times*, May 12, 2014, <http://nytimes.com>.
35. "(S/NF) Bahrain: Emergent Princes Nasir and Khalid," *Telegraph*, February 17, 2011, <http://telegraph.co.uk>.
36. Glenn Greenwald, Ryan Gallagher, and Ryan Grim, "Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers,'" *Huffington Post*, November 26, 2013, <http://huffingtonpost.com>.
37. David Rosen, "Is Success Killing the Porn Industry?," May 27, 2013, <http://altnet.org>; "Press Releases," March 12, 2007, <http://toptenreviews.com>.
38. Greenwald, Gallagher, and Grim, "Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers.'" 39. *Ibid.*
40. President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World (Washington, DC: White House, December 12, 2013), 114, <http://whitehouse.gov>.
41. Edward Snowden, "An Open Letter to the People of Brazil," *Folha de S. Paulo*, December 16, 2013, <http://folha.uol.com.br>.
42. Alan Feuer, "Four Charged with Running Online Prostitution Ring," *New York Times*, March 7, 2008, <http://nytimes.com>; Nico Pitney, "Spitzer As Client 9: Read Text Messages From Spitzer To Prostitute," March 28, 2008, <http://huffingtonpost.com>; Angeliqwe Chrisafis, "French Budget Minister Accused of Hiding Swiss Bank Account," *Guardian*, December 27, 2012, <http://theguardian.com>; Angeliqwe Chrisafis, "France's Former Budget Minister Admits Lying about Secret Offshore Account," *Guardian*, April 2, 2013, <http://theguardian.com>.
43. Alison Smale, "Surveillance Revelations Shake U.S.-German Ties," *New York Times*, August 25, 2013, <http://nytimes.com>; Smale, "Anger Growing Among Allies On U.S. Spying"; "Arrival and doorstep EP President (Schulz)," October 24, 2013, *TV Newsroom-European Council of the EU*, <http://tvnewsroom.consilium.europa.eu>; "Brazil Will Have Its Own National-made Secure Communications Satellite by 2016," *Mercopress* (Montevideo), November 29, 2013, <http://en.mercopress.com>.
44. Julian E. Barnes and Nathan Hodge, "Military Faces Historic Shift," *Wall Street Journal*, January 6, 2012, <http://online.wsj.com>; U.S. Department of Defense, Sustaining U.S. Global Leadership: Priorities for 21st Century Defense (Washington, DC: U.S. Department of Defense, January 2012), 2-5, <http://defense.gov>.
45. Chris Hellman and Mattea Kramer, "The Washington Creation That Ate Your Lunch," February 28, 2013, <http://tomdispatch.com>; Shane, "New Leaked Document Outlines U.S. Spending on Intelligence Agencies."
46. Department of Defense, *Sustaining U.S. Global Leadership*, 3-5; Craig Whitlock and Greg Jaffe, "Obama Announces New, Leaner Military Approach," *Washington Post*, January 5, 2012, <http://washingtonpost.com>; Lance M. Bacon, "Chief, Congress and DoD Hammer Out Army Manning Levels," *Army Times*, October 7, 2013, <http://armytimes.com>.
47. David E. Sanger, "Obama Panel Said to Urge N.S.A. Curbs," *New York Times*, December 13, 2013, <http://nytimes.com>.

# “We’re Profiteers”

## *How Military Contractors Reap Billions from U.S. Military Bases Overseas*

DAVID VINE

“You whore it out to a contractor,” Major Tim Elliott said bluntly. It was April 2012, and I was at a swank hotel in downtown London attending “Forward Operating Bases 2012,” a conference for contractors building, supplying, and maintaining military bases around the world. IPQC, the private company running the conference, promised the conference would “bring together buyers and suppliers in one location” and “be an excellent platform to initiate new business relationships” through “face-to-face contact that overcrowded trade shows cannot deliver.”<sup>1</sup> Companies sending representatives included major contractors like General Dynamics and the food services company Supreme Group, which has won billions in Afghan war contracts, as well as smaller companies like QinetiQ, which produces acoustic sensors and other monitoring devices used on bases. “We’re profiteers,” one contractor representative said to the audience in passing, with only a touch of irony.

Other than the corporate representatives and a couple of journalists, a few officers from NATO member militaries were on hand to speak. Major Elliott of the Royal Scots Brigades had offered his stark assessment while explaining how to build a military base that allows a base commander to “forget the base itself”—that is, the work of running the base—and instead maximize his effectiveness outside the base.<sup>2</sup>

Of course, Elliott said, in wartime you won’t get contractors to run a base without “a shitload of money.” At times, he said, this has meant vast amounts of “time, effort, and resources” are going “just to keep a base running.” In Afghanistan, Elliott said he saw situations so bad that on one base there were private security guards protecting privately contracted cooks who were cooking for the same private security guards...who were protecting the privately contracted cooks...who

---

DAVID VINE is associate professor of anthropology at American University in Washington, D.C. He is the author of the forthcoming *Base Nation: How American Military Bases Abroad Are Damaging National Security and Hurting Us All* (Metropolitan Books, 2015), and *Island of Shame: The Secret History of the U.S. Military Base on Diego Garcia* (Princeton University Press, 2009).

were cooking for the private security guards... who were protecting the privately contracted cooks, and on it went.

By the end of 2014 in Afghanistan, the U.S. military will have closed, deconstructed, or vacated most of what were once around 800 military installations, ranging from small checkpoints to larger combat outposts to city-sized bases.<sup>3</sup> Previously, the military vacated 505 bases it built or occupied in Iraq.<sup>4</sup>

Despite the closure of these 1,000-plus installations, the U.S. military will still occupy around 800 military bases outside the fifty states and Washington, D.C.<sup>5</sup> In addition to more than 4,000 domestic bases, this collection of extraterritorial bases is undoubtedly the largest in world history.<sup>6</sup>

As the *Monthly Review* editors and others have pointed out, U.S. bases overseas have become a major mechanism of U.S. global power in the post-Second World War era. Alongside postwar economic and political tools like the International Monetary Fund, the World Bank, and the United Nations, the collection of extraterritorial bases—like colonies for the European empires before it—became a major mechanism for “maintaining [U.S.] political and economic hegemony,” advancing corporate economic and political interests, protecting trade routes, and allowing control and influence over territory vastly disproportionate to the land bases actually occupy.<sup>7</sup> Without a collection of colonies, the United States has used its bases, as well as periodic displays of military might, to keep wayward nations within the rules of an economic and political system favorable to itself.<sup>8</sup>

Building and maintaining this global base presence has cost U.S. taxpayers billions of dollars. While the military once built and maintained its forts, bases, and naval stations, since the U.S. war in Vietnam, private military contractors have increasingly constructed and run this global collection of bases, foreshadowing and helping to fuel broader government privatization efforts. During this unprecedented period, major corporations—U.S. and foreign—have increasingly benefitted from the taxpayer dollars that have gone to base contracting.

After an extensive examination of government spending data and contracts (as part of a larger five-year investigation of U.S. bases abroad), my calculations show the Pentagon has dispersed around \$385 billion in taxpayer-funded contracts to private companies for work outside the United States, mainly on bases, between the onset of the war in Afghanistan in late 2001 and 2013 alone. The total is nearly double the entire State Department budget over the same period (and, of course, these overseas

contracts represent only a portion of the total Pentagon budget, which totaled trillions over this period). While some of the contract moneys are for things like weapons procurement and training, rather than for bases and troop support, the thousands of contracts believed to be omitted from these tallies thanks to government accounting errors make the numbers a reasonable reflection of the everyday moneys flowing to private contractors to support the country's global base collection. Because of the secrecy surrounding military budgets as well as the Pentagon's poor accounting practices, the true total may be significantly higher.

Almost a third of the total—more than \$115 billion—was concentrated among the top ten corporate recipients alone. Many of the names scoring the biggest profits are familiar: former Halliburton subsidiary Kellogg Brown & Root, private security company DynCorp, BP. Others are less well known: Agility, Fluor, Bahrain Petroleum Company. The complete list includes major transnational construction firms, large food service providers, the world's biggest oil companies, and thousands upon thousands of smaller companies receiving government contracts.

Others have also benefitted—financially, politically, and professionally—from the huge collection of bases overseas. High-ranking officials in the military and the Pentagon bureaucracy, members of Congress (especially members of the armed services and appropriations committees), lobbyists, and local and national-level politicians in countries accommodating bases have all reaped rewards.

My investigation into base contracting abroad also reveals that base spending has been marked by spiraling expenditures, the growing use of uncompetitive contracts (and contracts lacking incentives to control costs), and outright fraud—in addition to the repeated awarding of non-competitive contracts to companies with histories of fraud and abuse. Financial irregularities have been so common that any attempt to document the misappropriation of taxpayer funds at bases globally would be a mammoth effort. In the Afghanistan and Iraq wars alone, the Commission on Wartime Contracting (which Congress established to investigate waste and abuse) has estimated that there has been \$31–\$60 billion in contracting fraud during the wars, with most of it involving bases in and around Afghanistan and Iraq.<sup>9</sup> In Singapore, at least four Navy officials have recently been charged with receiving bribes in the form of cash, gifts, and sexual services in exchange for providing a contractor with inside information and helping to inflate the company's billing. Globally, billions of dollars are likely wasted or misused every year.



Proponents of outsourcing the work of building, running, and supplying bases overseas argue that contractors save government and taxpayer money while allowing the military, as Major Elliott suggested, to focus on its combat duties. Research suggests that this is often not the case. Contractors tend to provide base (and other) services at higher costs than the military itself.<sup>10</sup> While contracting overseas has helped build and maintain a global network of bases that has supported the U.S. government's geopolitical and geoeconomic aims—and U.S. corporate interests—worldwide, foreign bases have become an important source of profit-making in their own right that have diverted hundreds of billions of taxpayer dollars from pressing domestic needs.

### The Base World

Although some of the bases in the base world, like the naval station at Guantánamo Bay, Cuba, date to the late nineteenth century, most were built or occupied during the Second World War. (It is important to remember, however, that most of today's domestic bases, from the continental United States to Hawai'i and Alaska, occupy land that was once "abroad.") President Franklin D. Roosevelt acquired many of today's overseas bases in his "destroyers for bases" deal with Britain. Acquisitions accelerated and continued through the end of the war. By 1945, the United States occupied more than 30,000 installations at more than 2,000 base sites globally.<sup>11</sup>

While the number of U.S. bases overseas fluctuated during the Cold War and declined by around 60 percent after the Cold War's end, seventy years after the Second World War and more than sixty years after the Korean War, there are still 179 U.S. base sites in Germany, 109 in Japan, and 83 in South Korea—among scores more dotting the planet in places like Aruba and Australia, Bahrain and Bulgaria, Colombia, Kenya, Qatar, and Yemen, just to name a few.<sup>12</sup> The bases range in size from small radar installations to massive air bases. While the Pentagon considers most of its overseas base sites "small installations or locations," it defines "small" as having a reported value of up to \$800 million.<sup>13</sup> At the height of the wars in Iraq and Afghanistan, the total number of bases outside the fifty states and Washington, D.C. probably numbered around 2,000. Today, the total remains around 800 (although the Pentagon does not even have an accurate count).

And the U.S. military presence abroad is actually even larger. There are the Navy's eleven aircraft carriers—a kind of floating base, or as the Navy tellingly refers to them, "four and a half acres of sovereign

U.S. territory.”<sup>14</sup> There is also a significant, and growing, military presence in space, with space bases and weapons in development featuring names like “Rods from God.”

Globally, the Pentagon occupies more than 28 million acres (97 percent domestically), which is about the size the State of New York and bigger than all of North Korea. The military’s buildings alone cover 2.2 billion square feet of space—almost three times that of Wal-Mart. McDonald’s, too, pales in comparison with some 35,000 stores compared to the Pentagon’s 291,000 buildings.<sup>15</sup> A more apt comparison is the total number of U.S. embassies and consulates abroad. As a physical manifestation of the country’s diplomatic tools, the 278 embassies and consulates worldwide represent about one-third the total number of bases and occupy far less territory. By my very conservative calculations, total expenditures to maintain bases and troops overseas probably reached \$175 billion in fiscal year 2012.<sup>16</sup>

### **Peeling the Potatoes and Bringing Home the Bacon**

Once upon a time, the military, not contractors, built and ran U.S. bases. Soldiers, sailors, marines, airmen, and airwomen built the barracks, cleaned the clothes, and peeled the potatoes. This started changing during the Vietnam War, when Brown & Root began building major military installations in South Vietnam as part of a contractor consortium.<sup>17</sup> The company, which later became known as KBR, enjoyed deep ties with President Lyndon Johnson dating to the 1930s, leading to well-founded suspicions that Johnson steered contracts to Brown & Root.<sup>18</sup>

The use of contractors grew as the war in Vietnam continued. Amid nationwide resistance to the draft, contractors were one way to solve a labor problem that became permanent with the end of conscription in 1973. Militaries always need bodies to have a fighting force. In the era of the “all-volunteer force,” hiring contractors reduced the need to recruit new service members. In practice, the government passed the labor problem to contractors, who have generally searched the globe for the cheapest possible workers. Frequently, they have been Filipinos and other often formerly colonized non-U.S. citizens willing to work for much less than uniformed troops. Additionally, the government and contractors often avoid paying for the health care, retirement, and other benefits provided to U.S. troops.

A broader rise in the privatization of formerly government services only accelerated the trend in the military. Without forced conscription, the military was also under pressure to retain troops once they joined.

Keeping troops and their families happy with an increasingly diverse array of comforts played an important part in retaining the military's labor force. Especially at bases abroad, military leaders sought to mitigate the challenges of overseas tours with a generally cushier lifestyle than troops could afford at home. With time, troops, families, and, importantly, politicians came to expect elevated and ever-rising living standards not just at peacetime bases, but in warzones as well. To deliver this lifestyle, the military would pay contractors with increasing generosity.

By the first Gulf War in 1991, one out of every hundred deployed personnel was a contractor. During military operations later in the 1990s in Somalia, Rwanda, Haiti, Saudi Arabia, Kuwait, and especially the Balkans, Brown & Root received more than \$2 billion in base-support and logistics contracts for construction and maintenance, food services, waste removal, water production, transportation services, and much more.<sup>19</sup> In the Balkans alone, Brown & Root built thirty-four bases. The largest, Camp Bondsteel in Kosovo, covered 955 acres and included two gyms and other sports facilities, extensive dining and entertainment facilities, two movie theaters, coffee bars, and a post exchange ("PX") for shopping. Describing off-duty soldiers, a U.S. Army representative told *USA Today*, "We need to get these guys pumping iron and licking ice cream cones, whatever they want to do." By contrast, military personnel from other NATO countries lived in existing apartments and factories.<sup>20</sup>

By the second Gulf War, contractors represented roughly half of all deployed personnel in Iraq. The company now known as KBR employed more than 50,000 people in the warzone. That is the equivalent of five divisions or one hundred army battalions.<sup>21</sup> City-sized bases became known for their Burger Kings, Starbucks, and car dealerships, their air conditioning, ice cream, and steak.<sup>22</sup> Although recent fiscal constraints have meant some increase in periodic kitchen ("KP") duty, for most in the military, the days of peeling potatoes are long gone.

### **Contracts, Contracts, Contracts**

Figuring out who has been winning all the contracts for the increasingly comfortable military lifestyle was not easy. Between the secrecy surrounding military contracting and the profoundly unreliable nature of Pentagon accounting, it is difficult to determine who has been benefiting from the growth in base contracting. Because the government does not compile many aggregated lists of contract winners, I had to pick through hundreds of thousands of government contracts from publicly available data and research scores of companies worldwide.

I used the same methodology for tracking funds as the Commission on Wartime Contracting, which Congress established to investigate waste and abuse in Afghanistan and Iraq.<sup>23</sup> This allowed me to compile a list of every Pentagon contract with a “place of performance”—that is, the country where most of a contract’s work is performed—outside the United States between the start of the Afghan war in October 2001 (fiscal year 2002) and May 2013.

There were 1.7 million contracts.

Scrolling through 1.7 million spreadsheet rows (more than can fit into a single Microsoft Excel file) offered a dizzying feel for the immensity of the Pentagon’s activities and the money spent globally. Generally, the companies winning the largest contracts have been providing one (or more) of five things: Construction, Operations and Maintenance, Food, Fuel, and Security.

But among the 1.7 million contracts, the breadth was remarkable. There was one for \$43 for sand in South Korea and another for a \$1.7 million fitness center in Honduras. There was the \$23,000 for sports drinks in Kuwait, \$53 million in base support services in Afghanistan, and everything from \$73 in pens to \$301 million for army industrial supplies in Iraq.

Cheek by jowl, I found the most basic services, the most banal purchases, and the most ominous acquisitions, including concrete sidewalks, a traffic light system, diesel fuel, insect fogger, shower heads, black toner, a 59” desk, unskilled laborers, chaplain supplies, linen for “distinguished visitor” rooms, easy chairs, gym equipment, flamenco dancers, the rental of six sedans, phone cards, a 50” plasma screen, billiards cues, X-Box 360 games and accessories, Slushie machine parts, a hot dog roller, scallops, shrimp, strawberries, asparagus, and toaster pastries, as well as hazardous waste services, a burn pit, ammo and clips, bomb disposal services, blackout goggles for detainees, and confinement buildings.

Not surprisingly, given the recent wars and the huge number of bases that have enabled and supported the wars and occupations, contractors have won the most taxpayer dollars in Afghanistan and Iraq. With more than 1,300 installations between the two countries, corporations received around \$160 billion in contracts between 2001 and 2013. In Kuwait, where hundreds of thousands of troops deployed to Iraq, corporations enjoyed \$37.2 billion in contracts. The next four countries where military contractors have received the largest contracts are those that have generally hosted the largest number of bases and the largest number of troops since the Second World War: Germany (\$27.8 billion in contracts), South Korea (\$18.2 billion), Japan (\$15.2 billion), and Britain (\$14.7 billion).

### Top Ten Countries by Pentagon Spending, Funds Fiscal Year 2002-April 2013

Country	Total (billions)
1. Iraq	89.1
2. Afghanistan	69.8
3. Kuwait	37.2
4. Germany	27.8
5. South Korea	18.2
6. Japan	15.2
7. United Kingdom	14.7
8. United Arab Emirates	10.1
9. Bahrain	6.9
10. Italy	5.8

Source: <http://usaspending.gov>.

Note: Canada and Saudi Arabia would have also made the top ten; however, those contracts are for the most part unrelated to the limited U.S. military presence in each country, and thus are excluded from this list.

The \$385 billion total is at best a rough estimate because Pentagon and government accounting practices are so poor; the federal data system has even been called “dysfunctional.”<sup>24</sup> The real totals are almost surely higher, especially considering the secretive nature of Pentagon budgets. Black budgets and CIA contracts for paramilitary activities alone could add tens of billions of dollars in overseas base spending.<sup>25</sup>

The unreliable and opaque nature of the data becomes clear given that the top recipient of Pentagon contracts abroad is not a company at all, but “miscellaneous foreign contractors.”<sup>26</sup> That is, almost 250,000 contracts totaling nearly \$50 billion, or 12 percent of the total, have gone to recipients that the Pentagon has not identified publicly. As the Commission on Wartime Contracting explains, “miscellaneous foreign contractors” is a catchall “often used for the purpose of obscuring the identification of the actual contractor[s].”<sup>27</sup>

The reliability of the data worsens when we consider the Pentagon’s inability to track its own money. Pentagon accounting has been called “frequently fictional,” ledgers are sometimes still handwritten, and \$1 billion can be a rounding error.<sup>28</sup> The Department of Defense remains the only federal agency unable to pass a financial audit.<sup>29</sup> Identifying the value of contracts received by specific companies is more difficult still because of complicated subcontracting arrangements, the use of foreign subsidiaries, frequent corporate name changes, and the general lack of corporate transparency.

### Top Twenty-Five Recipients of Pentagon Contracts Abroad

Contract Awardee	Total (billions)
1. Miscellaneous Foreign Contractors	47.1
2. KBR, Inc.	44.4
3. Supreme Group	9.3
4. Agility Logistics (PWC)	9.0
5. DynCorp International	8.6
6. Fluor Intercontinental	8.6
7. ITT/Exelis, Inc.	7.4
8. BP, P.L.C.	5.6
9. Bahrain Petroleum Company	5.1
10. Abu Dhabi Petroleum Company	4.5
11. SK Corporation	3.8
12. Red Star Enterprises (Mina Corporation)	3.8
13. World Fuel Services Corporation	3.8
14. Motor Oil (Hellas), Corinth Refineries S.A.	3.7
15. Combat Support Associates Ltd.	3.8
16. Refinery Associates Texas, Inc.	3.3
17. Lockheed Martin Corporation	3.2
18. Raytheon Company	3.1
19. S-Oil Corporation (Ssangyong)	3.0
20. International Oil Trading Co./Trigeant Ltd.	2.7
21. FedEx Corporation	2.2
22. Contrack International, Inc.	2.0
23. GS/LG-Caltex (Chevron Corporation)	1.9
24. Washington Group/URS Corporation	1.6
25. Tutor Perini Corporation (Perini)	1.5
<b>SUBTOTAL</b>	<b>\$201.8</b>
<b>All Other Contractors</b>	<b>\$183.4</b>
<b>TOTAL</b>	<b>\$385.2</b>

Source: <http://usaspending.gov>.

Beyond the sheer volume of dollars, a troubling pattern emerges: the majority of benefits have gone to a relatively small group of private contractors. Almost a third of the \$385 billion has gone to just ten contractors. They include scandal-prone companies like KBR, the former subsidiary of former Vice President Richard Cheney's old company Halliburton, and oil giant BP. With these and other contractors, large and small, Pentagon spending in the base world has been marked by spiraling spending expenditures, the growing use of contracts lacking

incentives to control costs, sometimes criminal behavior, and the repeated awarding of non-competitive sweetheart contracts to companies with histories of fraud and abuse.

Putting aside the unknown “miscellaneous foreign contractors” topping the recipients’ list, it is helpful to examine the top three named recipients in some detail.

**1. KBR:** Among the companies bringing home billions, the name Kellogg, Brown & Root dominates. It has almost five times the contracts of the next company on the list and is emblematic of broader problems in the contracting system.

KBR is the latest incarnation of Brown & Root, the company that started paving roads in Texas in 1919 and grew into the largest engineering and construction firm in the United States. In 1962, Halliburton, an international oil services company, bought Brown & Root. In 1995, Richard Cheney became Halliburton’s president and CEO after helping jumpstart the Pentagon’s ever-greater reliance on private contractors when he was President George H.W. Bush’s secretary of defense. During the five years when Cheney ran the company, KBR won \$2.3 billion in U.S. military contracts (compared to \$1.2 billion in the previous five years).<sup>30</sup>

Later, when Cheney was vice president, Halliburton and its KBR subsidiary (formed after acquiring Kellogg Industries) won by far the largest wartime contracts in Iraq and Afghanistan. It is difficult to overstate KBR’s role in the two conflicts. Without its work, there might have been no wars. In 2005, Paul Cerjan, a former Halliburton vice president, explained that KBR was supporting more than 200,000 coalition forces in Iraq, providing “anything they need to conduct the war.” That meant “base support services, which includes all the billeting, the feeding, water supplies, sewage—anything it would take to run a city.” It also meant Army “logistics functions, which include transportation, movement of POL [petroleum, oil, and lubricants] supplies, gas... spare parts, ammunition.”<sup>31</sup>

Most of KBR’s contracts to support bases and troops overseas have come under the multi-billion-dollar Logistics Civilian Augmentation Program (LOGCAP). In 2001, KBR won a one-year LOGCAP contract to provide an undefined quantity and an undefined value of “selected services in wartime.” The company subsequently enjoyed nearly eight years of work without facing a competitor’s bid, thanks to a series of one-year contract extensions. By July 2011, KBR had received more than \$37 billion in LOGCAP funds. KBR reflected the near tripling of Pentagon contracts issued without competitive bidding between 2001

and 2010. “It’s like a gigantic monopoly,” a representative from the watchdog group Taxpayers for Common Sense said of LOGCAP.

The work KBR performed under LOGCAP also reflected the Pentagon’s frequent use of “cost-plus” contracts. These reimburse a company for its expenses and then add a fee that is usually fixed contractually or determined by a performance evaluation board. The Congressional Research Service explains that because “increased costs mean increased fees to the contractor,” there is “no incentive for the contractor to limit the government’s costs.”<sup>32</sup> As one Halliburton official told a congressional committee bluntly, the company’s unofficial mantra in Iraq became, “Don’t worry about price. It’s ‘cost-plus.’”<sup>33</sup>

In 2009, the Pentagon’s top auditor testified that KBR accounted for “the vast majority” of wartime fraud.<sup>34</sup> The company has faced accusations of overcharging for everything from delivering food and fuel to providing housing for troops and base security services.<sup>35</sup> For its work at Camp Bondsteel in Kosovo, Halliburton/KBR paid \$8 million to the government in 2006 to settle lawsuits charging double billing, inflating prices, and other fraud.<sup>36</sup>

After years of bad publicity, in 2007, Halliburton spun KBR off as an independent company and moved its headquarters from Houston to Dubai. Despite KBR’s track record and a 2009 guilty plea for bribing Nigerian government officials to win gas contracts (for which its former CEO received prison time), the company has continued to receive massive government contracts. Its latest LOGCAP contract, awarded in 2008, could be worth up to \$50 billion through 2018. In early 2014, the Justice Department sued KBR and two subcontractors for exchanging kickbacks and filing false reimbursement claims for costs “that allegedly were inflated, excessive or for goods and services that were grossly deficient or not provided.” The suit also charged KBR with transporting ice for troops’ consumption in unsanitized trailers previously used as temporary morgues.<sup>37</sup>

**2. Supreme Group:** Next on the list is the company that has been described as the “KBR for the Afghan War.” Supreme Group has won more than \$9 billion in contracts for transporting and serving meals to troops in Afghanistan and at other bases worldwide. Another nearly \$1.4 billion in fuel transportation contracts takes Supreme’s total over \$10 billion. The company’s growth perfectly symbolizes the soldiers-to-contractors shift in who peels the potatoes.<sup>38</sup>

Supreme was founded in 1957 by an Army veteran, Alfred Ornstein, who saw an opportunity to provide food for the hundreds of growing U.S. bases in Germany. After expanding over several decades into



the Middle East, Africa, and the Balkans, the company won multi-billion-dollar “sole source contracts” that gave it a virtual monopoly over wartime food services in Afghanistan. In the decade since the start of the war in 2001, the company’s revenues grew more than fifty-fold to \$5.5 billion. Its profit margins between 2008 and 2011 ranged between 18 and 23 percent. Wartime contracts account for 90 percent of revenues for the company, now based in Dubai (like KBR). They have made its majority owner, the founder’s son Stephen Ornstein, a billionaire.

Supreme’s chief commercial officer, former Lieutenant General Robert Dail, provides a prime example of the revolving door between the Pentagon and its contractors. From August 2006 to November 2008, Dail headed the Pentagon’s Defense Logistics Agency. The DLA awards the Pentagon’s food contracts. In 2007, Dail presented Supreme with DLA’s “New Contractor of the Year Award.” Four months after leaving the Pentagon, he became the president of Supreme Group USA.

The Pentagon now says Supreme overbilled the military by \$757 million. Others have started to scrutinize how the company won competition-free contracts and charged service fees as high as 75 percent of costs. Supreme denies overcharging and claims the government owes it \$1.8 billion. In 2013, Supreme unsuccessfully sued the Pentagon for awarding a new \$10 billion Afghanistan food contract to a competitor that underbid Supreme’s offer by \$1.4 billion.<sup>39</sup>

**3. Agility Logistics:** After Supreme is Agility Logistics, a Kuwaiti company (formerly known as Public Warehousing Company KSC and PWC Logistics). It won multi-billion-dollar contracts to transport food to troops in Iraq. When the Pentagon decided against awarding similar contracts in Afghanistan to a single firm, Agility partnered with Supreme in exchange for a 3.5 percent fee on revenues. Like Supreme, Agility hired a former high-ranking DLA official, Major General Dan Mongeon, as President of Defense & Government Services, U.S.<sup>40</sup> Mongeon joined the company just months after it won its second multi-billion dollar contract from DLA.

In 2009 and 2010, grand juries criminally indicted Agility for \$6 billion in false claims and price manipulation.<sup>41</sup> In 2011, a grand jury subpoenaed Mongeon as part of investigations into new charges against Agility.<sup>42</sup> With the litigation ongoing, the Pentagon suspended the company and 125 related companies from receiving new contracts. Agility has filed a \$225 million suit against the DLA for breach of contract. Strangely, the Army and the DLA have continued to do business with Agility, extending contracts with more than seven separate “compelling reason” determinations.<sup>43</sup>

### The Rest of the Top Ten: A Pattern of Misconduct

Things do not get much better farther down the list. Next come DynCorp International and Fluor Intercontinental. The two, along with KBR, won the latest LOGCAP contracts. Awarding that contract to three companies rather than one was intended to increase competition. In practice, according to the Commission on Wartime Contracting, each corporation has enjoyed a “mini-monopoly” over logistics services in Afghanistan and other locations. DynCorp, which has also won large wartime private security contracts, has a history littered with charges of overbilling, shoddy construction, smuggling laborers onto bases, as well as sexual harassment and sex trafficking.

Although a Fluor employee pled guilty in 2012 to conspiring to steal and sell military equipment in Iraq, it is the only defense firm in the world to receive an “A” on Transparency International’s anti-corruption index that rates companies’ efforts to fight corruption. On the other hand, number seven on the list, ITT (now Exelis), received a “C” (along with KBR and DynCorp).<sup>44</sup>

The last three in the top ten are BP (which tops the Project on Government Oversight’s federal contractor misconduct list) and the petroleum companies of Bahrain and the United Arab Emirates.<sup>45</sup> The military and its bases run on oil. The military consumed five billion gallons in fiscal year 2011 alone—more than all of Sweden.<sup>46</sup> In total, ten of the top twenty-five firms are oil companies, with contracts for delivering oil overseas totaling around \$40 billion.

The Pentagon and the government generally justify the use of so many contractors based on their supposed efficiency and saving taxpayer money. On average, this appears not to be the case. Research shows that contractors cost two to three times as much as a Pentagon civilian doing the same work. More than half of Army contracts go to administrative overhead rather than contract services.<sup>47</sup> Military comptrollers acknowledge that when it comes to the use of contractors, “growth has been unchallenged.”

“The savings are here,” the comptrollers conclude.<sup>48</sup>

### “Ice Cream”

At the Forward Operating Bases 2012 conference in London, the speakers included members of several NATO militaries. They were a reminder that while U.S. companies working on U.S. bases dominate the industry, private contractors increasingly build, run, and supply bases for the militaries of many nations, as well as for international peacekeepers and oil companies whose extraction facilities often look like military bases.

Among the speakers was U.S. Marine Corps Major Patrick Reynolds. With the help of a Marine Corps video, Reynolds talked about “EXFOB,” the Marines’ experimental, energy-saving forward operating base (according to the video, EXFOB aims to help “change the way we think about energy to maintain our lethality”). Referring to his audience, he said it is great that the “beltway bandits” are on board with this new emphasis on energy efficiency.

Reynolds ended his presentation by alerting the contractors to a list of upcoming contract opportunities. “RFP to be posted on FEDBIZOPPS soon!” read one of his powerpoint slides (referring to the website advertising government procurement opportunities). Suddenly there was a noticeable surge in energy in the room. People sat up in their chairs, and for the first time during his presentation, many in the audience began taking notes on mostly blank notepads. “I know you guys from the industry pay a lot to be here,” Reynolds said, so he thought it right to offer “food for thought [to] give you something to walk away with.”

Just as tellingly as what appeared to be advance notice on government-contract solicitations, Reynolds explained to the group how bases tend to expand exponentially over time. “You start out small” with an outpost, he said, “thinking you’ll only be there for a week.... And then it’s two weeks. And then it’s a month. And then it’s two months.” In the process, bases add facilities, food, and recreational amenities, like steak and lobster, flat screen TVs, and Internet connections. The major said he and others in the military refer to these comforts collectively as “ice cream.”

“There’s no ‘ice cream’ out here” at a small outpost, he told the audience. “But eventually you’ll get to the point where it’s out here” at a patrol base and not just as it is now at headquarters and FOBs. “It’s a building block process.”

The process Major Reynolds described is precisely what happened on bases in and around Afghanistan and Iraq. According to a Congressional Research Service report, the Pentagon “built up a far more extensive infrastructure than anticipated to support troops and equipment.” Funds for the operation and maintenance of bases (including food and amenities) grew three times as fast as the number of deployed troops would suggest.<sup>49</sup>

During a Q&A session, a Supreme Group representative asked Reynolds if the Marines were thinking about reducing the “ice cream,” the TVs, and the other amenities.

I’d love to do that, the major replied. Is it going to happen? “Sort of, kind of, not really.”

“Do we need ice cream? Do we need cable TVs? Do we need high speed internet and all the crap? No,” said Reynolds. “But we have” Senators and Congressmen coming out and “visiting their constituents and they want to help.”

And then he paused before continuing, “That’s probably all I’ll say on that.”

Major Reynolds politely pointed to some of the political players shaping the base world. They are just some of those who, in addition to the contractors, have benefitted from the collection of bases abroad. For example, in Afghanistan and Iraq, Congress members have used base amenities as a public way to demonstrate their patriotism and support for the troops.

One former soldier told me his reaction to arriving at Iraq’s Camp Liberty was, “This is awesome!” Like thousands of others, he found comfortable rooms, beds, and amenities that eventually included unrestricted Internet access (thanks to a favor from a KBR contractor). “It was really plush,” he said. “It was dope.”

Later, he admitted, “I felt ashamed it wasn’t harder.”

The perks of overseas base life are far greater for the generals and the admirals who often enjoy personal assistants and chefs, private planes and vehicles, and other benefits. Beyond the authorized perks, there are cases like former Africa Command commander General William “Kip” Ward. Pentagon investigators found Ward “engaged in multiple forms of misconduct” including billing the government for hundreds of thousands of dollars of personal travel and misusing government funds on luxury hotels, five-car motorcades, and spa and shopping trips for his wife.<sup>50</sup> He also accepted free meals and tickets to a Broadway musical from an unnamed “construction management, engineering, technology and energy services company” with millions in Pentagon contracts.<sup>51</sup>

### **Election Donations**

In addition to illegal efforts to influence base contracting, contractors have made millions in campaign contributions to Congress members. According to the Center for Responsive Politics, individuals and PACs linked to military contractors gave more than \$27 million in election donations in 2012 alone and have donated almost \$200 million since 1990.<sup>52</sup>

Most of these have gone to members of the armed services and appropriations committees in the Senate and House of Representatives. These committees have most of the authority over awarding military dollars. For the 2012 elections, for example, Virginia-based DynCorp’s political action committee donated \$10,000 to both the chair and ranking member of the

House Armed Services Committee, and made additional donations to thirty-three other members of the House and Senate armed services committees and sixteen members of the two appropriations committees.<sup>53</sup>

Contractors also pay lobbyists millions more to sway military budgeteers and policymakers. In 2001 alone, ten leading military contractors spent more than \$32 million on lobbying.<sup>54</sup> KBR and Halliburton spent nearly \$5.5 million on lobbying between 2002 and 2012.<sup>55</sup> This included \$420,000 in 2008 when KBR won the latest LOGCAP contract and \$620,000 the following year when it protested being barred from bidding on contracts in Kuwait.<sup>56</sup> Supreme spent \$660,000 on lobbying in 2012 alone.<sup>57</sup> Agility spent \$200,000 in 2011, after its second indictment on fraud charges.<sup>58</sup> Fluor racked up nearly \$9.5 million in lobbying fees from 2002 to 2012.<sup>59</sup>

Even the German state of Rheinland-Pfalz lobbies the U.S. government to keep bases in its state. Rheinland-Pfalz (also called Rhineland-Palatinate) has been home to more U.S. troops and bases than any other. Since 2007, the state made 258 documented contacts with U.S. government officials. Many of the contacts were with staffers, but others were with powerful Congress members with influence over bases and military policy, including Senators John Warner, Lindsey Graham, James Inhofe, and Representative Solomon Ortiz. Other meetings were with high-ranking Pentagon officials and an assistant secretary of the Army. During this period, Rheinland-Pfalz paid the high-profile Washington, D.C. lobbying firm DLA Piper at least \$772,000 to lobby on its behalf.<sup>60</sup> In neighboring Baden-Württemberg, the German city of Heidelberg enlisted another prominent lobbyist, Patton Boggs, to help keep the Army in its city.<sup>61</sup> One sees how politicians in many countries, along with contractors, trade associations, lobbyists, Pentagon officials, military personnel, veterans, and others are deeply invested in maintaining the base status quo.

### **Avoiding Taxes**

While contractors have enjoyed billions in taxpayer funds, many have sought to minimize U.S. taxes paid on those profits by both legal and illegal means. Across the entire aerospace and military industry, the effective tax rate was 10.6 percent as of 2010 (compared to the top federal statutory corporate tax rate of 35 percent and an average effective tax rate for large profitable U.S. companies of 12.6 percent).<sup>62</sup> In 2004, the Government Accountability Office found that 27,100 Pentagon contractors (about one in nine) were illegally evading taxes while still receiving money from government contracts. Privacy rules prevented the government from naming

names, but in one case a contractor providing base services owed almost \$10 million in taxes while still receiving \$3.5 million from the Pentagon. The government estimated the total taxes owed at \$3 billion.<sup>63</sup>

In recent years, major military contractors have also increasingly created foreign-chartered subsidiaries to lower their taxes legally. At bases overseas, foreign companies frequently receive a significant proportion of base contracts, meaning these contractors pay little if any U.S. taxes at all. Some U.S. companies have taken advantage of this situation by creating foreign subsidiaries to do much of the work on base contracts abroad. KBR, for example, has avoided paying taxes on contracts in Iraq by using shell companies in the Cayman Islands that exist only as a name in a computer file. The company technically hired more than 21,000 of its employees with two Cayman subsidiaries, allowing it to avoid paying Social Security, Medicare, and Texas unemployment taxes. KBR officials claimed the practice saved the military money. While the practice allows the Pentagon to save money, a *Boston Globe* investigation found the loophole “results in a significantly greater loss in revenue to the government as a whole” while giving KBR a competitive advantage over competitor companies not using the loophole. In effect, the loophole lowered KBR’s contributions to the Social Security and Medicare trust funds and meant that employees could not receive unemployment benefits if they lost their jobs because they were technically employed by a foreign corporation. Robert McIntyre, the director of the advocacy group Citizens for Tax Justice, told the *Globe*, “The argument that by not paying taxes they are saving the government money is just absurd.”<sup>64</sup>

Similarly, while KBR’s former parent Halliburton was spinning off KBR as a separate company in 2007, Halliburton announced it would move its corporate headquarters to the no-tax jurisdiction of Dubai in the United Arab Emirates (UAE) where there is no corporate income tax and no tax on employee income (Halliburton already had seventeen foreign subsidiaries in tax-haven countries). Although the company has remained legally incorporated in the United States, moving top executives to Dubai likely allowed the executives to avoid income taxes and Halliburton to avoid employee payroll taxes and reduce its corporate taxes by arguing that a portion of its global profits are attributable to work performed in Dubai, not the United States.<sup>65</sup>

Generally under U.S. tax law, a U.S. firm with overseas operations can indefinitely postpone paying domestic corporate tax on its foreign income by conducting its foreign operations through a foreign-chartered subsidiary. As long as the company’s foreign earnings remain

under the control of the subsidiary and are reinvested abroad, U.S. corporate income taxes are “deferred.” The firm pays U.S. taxes on the overseas earnings of the subsidiary only when the parent company “repatriates” the earnings from the foreign subsidiary as intra-firm dividends or other income.<sup>66</sup> According to a 2012 J.P. Morgan study, U.S. multinational firms have over \$1.7 trillion in foreign earnings “parked” overseas and thus shielded from U.S. taxes.<sup>67</sup>

During a Government Accountability Office investigation, major military contractors admitted, “the use of offshore subsidiaries in foreign jurisdictions helps them lower their U.S. taxes. For example, one defense contractor’s offshore subsidiary structure decreased its effective U.S. tax rate by approximately 1 percent, equaling millions of dollars in tax savings.” (Foreign subsidiaries also protect companies from some legal liabilities and potential lawsuits.)<sup>68</sup>

Because U.S. corporations are taxed only when they repatriate such earnings, the current tax system encourages companies to earn and then keep their income overseas.<sup>69</sup> This Congressionally enacted structural incentive applies to all industries; however, its significance extends far beyond lost tax revenues in the case of contractors doing work on U.S. bases overseas. Given equivalent contracts to provide construction or maintenance services on a base in Texas and a base in the United Arab Emirates, for example, the base in the UAE offers more options for indefinitely reducing U.S. taxes. In short, the U.S. tax code encourages contractors to support the stationing of bases and troops abroad.

### **A Self-licking Ice Cream Cone**

As the FOB2012 conference neared its end, I asked another conference attendee (who asked that I not use his name) if during his wartime deployments in Iraq he had seen the problem Major Elliott had described of a base with private security guards protecting privately contracted cooks, who were cooking for the same private security guards, who were protecting the privately contracted cooks.

“A lot,” he replied. It’s the “self-licking ice cream cone”—by which he meant a self-perpetuating system with no purpose or function except to keep itself going.

“I sat with my ice cream and my prime rib on Sundays” in Iraq, he continued. It’s been this way since 2001 and maybe even Kosovo. There’s been lots of waste and inefficiency. Maybe, he said of the “loggies”—the logisticians who coordinate all the “ice cream”—it would be better “to fire the lot and start over.”

In one of the conference's final conversations, contractor and military representatives discussed fears about the military market drying up as U.S. and European governments cut military budgets. Contractors, many agreed, would increasingly move to build, supply, and maintain bases for UN and other international peacekeepers, as well as for oil and mining companies.

Peter Eberle, a representative from General Dynamics (which just missed making the top twenty-five overseas contract recipients), asked, "What if we have peace break out" after the U.S. withdrawal from Afghanistan?

"God forbid!" replied Major Elliott.

## Notes

1. IQPC, "Forward Operating Bases 2012" and "Sponsorship Opportunities," <http://iqpc.com>.

2. Parts of this article stem from my article, "Where Has All the Money Gone? How Contractors Raked in \$385 Billion to Build and Support Bases Abroad since 2001," *Tom Dispatch*, May 14, 2013, <http://tomdispatch.com>, and my forthcoming book *Base Nation: How American Military Bases Abroad Are Damaging National Security and Hurting Us All* (New York: Metropolitan Books, 2015). Thanks to Michael Tigar, John Mage and the other editors of *MR*, Tom Engelhardt, Clifford Rosky, Laura Jung, all those who generously offered their time and insights during interviews, and many, many others for their help with the work leading to this article.

3. David de Jong, email to author, February 4, 2014, quoting a press officer for the Secretary of Defense: "Using October 2011 as a benchmark we had about 800 facilities—ranging from very small checkpoints that have maybe a squad or platoon of ISAF forces on it to bases that have several hundred to as many as a thousand ISAF members on them."

4. Nick Turse, "Afghanistan's Base Bonanza," September 4, 2012, <http://tomdispatch.com>.

5. By the Pentagon's last reported count, as of September 2012, the military occupies 695 "base sites" outside the fifty states and Washington, D.C. See U.S. Department of Defense, "Base Structure Report Fiscal Year 2013 Baseline (A Summary of DoD's Real Property Inventory)," report, Washington, DC, 2013, <http://acq.osd.mil>. However, this total excludes numerous well-known bases, like those in Kuwait and Afghanistan; secret bases, like those reported in Israel; and a growing number of small "cooperative security locations" or "lily pad" bases in Africa, Asia, and Latin American. My estimate of 800 thus is an adjustment to the Pentagon's enumeration.

6. James R. Blaker, *United States Overseas Basing: An Anatomy of the Dilemma* (New York: Praeger, 1990), 9; Tom Engelhardt, "Advice to a Young Builder in Tough Times: Imperial Opportunities Abound," November 4, 2007, <http://tomdispatch.com>.

7. John Bellamy Foster, Harry Magdoff, and Robert W. McChesney, "U.S. Military Bases and Empire," *Monthly Review* 53, no. 10 (March 2002): 13. See also Chalmers Johnson, *The Sorrows of Empire: Militarism, Secrecy, and the End of the Republic* (New York: Metropolitan Books, 2004); Sydney Lens, *Permanent War: The Militarization of America* (New York: Schocken Books, 1987); Michael S. Sherry, *In the Shadows of War: The United States since the 1930s* (New Haven, CT: Yale University Press, 1995); Tom Engelhardt, "Twenty-first Century Gunboat Diplomacy," March 30, 2004, <http://tomdispatch.com>.

8. See David Vine, *Island of Shame: The Secret History of the U.S. Military Base on Diego Garcia* (Princeton: Princeton University Press, 2009).

9. Commission on Wartime Contracting in Iraq and Afghanistan, "Transforming Wartime Contracting: Controlling Costs, Reducing Risks," final report to Congress, August 2011, <http://cybercemetery.unt.edu>.

10. David Cay Johnston, "The U.S. Government Is Paying Through the Nose for Private Contractors," *Newsweek*, December 12, 2012, <http://newsweek.com>.

11. Blaker, *United States Overseas Basing*, 9.

12. U.S. Department of Defense, "Base Structure Report."

13. What constitutes a "base" is a complicated question. Definitions and terminology (base, post, station, fort, installation, etc.) vary considerably. The Pentagon's annual "Base Structure Report," which provides an annual accounting of its facilities and from which I derive the estimate of 800, refers to "base sites" (see note 5).

In some cases, this means that an installation generally referred to as a single base (like Aviano Air Base in Italy) actually consists of multiple distinct base sites—in Aviano's case, at least eight. For counting purposes, however, it makes sense to follow the Pentagon's lead, given that base sites with the same name can often be in geographically disparate locations. Generally too, each site represents a distinct Congressional appropriation of taxpayer funds. To avoid the linguistic debates, however, and because it's the simplest and most widely recognized name, I use "base"—taken to mean any structure, facility, or place regularly used for military purposes of any kind (see Blaker, *United States Overseas Basing*, 4).

14. Catherine Lutz, in Catherine Lutz, ed., "Introduction: Bases, Empire, and Global Response," *The Bases of Empire: The Global Struggle against U.S. Military Posts* (New York: NYU Press, 2009), 4.

15. U.S. Department of Defense, "Base Structure Report," 2-8; Dan Burrows, "Planet Walmart: Five Big Facts About the World's Largest Company," October 13, 2010, <http://dailyfinance.com/>; McDonald's Corporation, "Getting to Know Us," <http://aboutmcdonalds.com>; U.S. Department of State, accessed January 15, 2014, <http://usembassy.gov>.

16. See David Vine, "Picking Up a \$170 Billion Tab: How U.S. Taxpayers Are Paying the Pentagon to Occupy the Planet," December 11, 2012, <http://tomdispatch.com>.

17. Pratap Chatterjee, *Halliburton's Army: How a Well-Connected Texas Oil Company Revolutionized the Way America Makes War* (New York: Nation Books, 2009), 24-27.

18. *Ibid.*, 18-20.

19. P.W. Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (Ithaca: Cornell University Press, 2003), 80.

20. Chatterjee, *Halliburton's Army*, 61-62.



21. *Ibid.*, 214.
22. Guy Raz, "U.S. Builds Air Base in Iraq for Long Haul," *All Things Considered*, October 12, 2007, <http://npr.org>; Engelhardt, "Advice to a Young Builder."
23. Commission on Wartime Contracting in Iraq and Afghanistan, "Transforming Wartime Contracting," 208-210.
24. Linda Bilmes, "Who Profited from the Iraq War," *EPS Quarterly* 24, no. 1 (March 2012): 6, <http://epsusa.org>. The Federal Procurement Data System that's supposed to track government contracts "often contains inaccurate data," according to the Government Accountability Office, "Federal Contracting: Observations on the Government's Contracting Data Systems," report, GAO-09-1032T, September 29, 2009, <http://gao.gov>. For example, my research showed hundreds of thousands of contracts with no "place of performance" listed. On the other hand, there were 116,527 contracts listing the place of performance as Switzerland, even though the vast majority of the contracts are for delivering food to troops in Afghanistan and at bases worldwide (one of the major companies providing food, an arm of Supreme Group, is based in Switzerland).
25. See e.g., Wilson Andrews and Todd Lindeman, "The Black Budget," *Washington Post*, August 29, 2013, <http://washingtonpost.com>.
26. Or various iterations of the same term.
27. Commission on Wartime Contracting in Iraq and Afghanistan, "Transforming Wartime Contracting," 209.
28. R. Jeffrey Smith, "Pentagon's Accounting Shambles May Cost an Additional \$1 Billion," *Center for Public Integrity*, October 13, 2011 (updated, March 23, 2012), <http://publicintegrity.org>.
29. Asif A. Khan, "DOD Financial Management: Weaknesses in Controls over the Use of Public Funds and Related Improper Payments," United States Government Accountability Office testimony, Panel on Defense Financial Management and Auditability Reform, Committee on Armed Services, House of Representatives, September 22, 2011, <http://gao.gov>.
30. Chatterjee, *Halliburton's Army*, 49.
31. *Ibid.*, 9.
32. Valerie B. Grosso, "Defense Contracting in Iraq: Issues and Options for Congress," Congressional Research Service, Washington, DC, June 18, 2008, <http://fpc.state.gov>.
33. United States House of Representatives Committee on Oversight and Government Reform, "It's Your Money: Iraq Reconstruction," <http://oversight-archive.waxman.house.gov>.
34. Ellen Nakashima, "KBR Connected to Alleged Fraud, Pentagon Auditor Says," *Washington Post*, May 5, 2009, <http://washingtonpost.com>.
35. Dana Hedgpeth, "Audit of KBR Iraq Contract Faults Records For Fuel, Food," *Washington Post*, June 25, 2007, <http://washingtonpost.com>; U.S. Department of Justice, Office of Public Affairs, "United States Sues Houston-based KBR and Kuwaiti Subcontractor for False Claims on Contracts to House American Troops in Iraq," press release, November 19, 2012, <http://justice.gov/opa/pr>; Walter Pincus, "U.S. Files Civil Suit Against Defense Contractor KBR," April 2, 2010, *Washington Post*, <http://washingtonpost.com>.
36. Chatterjee, *Halliburton's Army*, 63-64.
37. U.S. Department of Justice, Office of Public Affairs, "United States Government Sues Kellogg, Brown & Root Services Inc. and Two Foreign Companies for Kickbacks and False Claims Relating to Iraq Support Services Contract," press release, January 23, 2014, <http://justice.gov/opa/pr>.
38. The best source for this section is David de Jong, "Supreme Owner Made a Billionaire Feeding U.S. War Machine," *Bloomberg*, October 7, 2013, <http://bloomberg.com>.
39. Andrew Zajac, "Supreme Foodservice Sues Over U.S., Afghan Food Contract," *Bloomberg News*, April 8, 2013, <http://bloomberg.com>. See also Supreme Foodservice, GmbH v. United States, No. 13-245 C (September 18, 2013).
40. Walter Pincus, "Agency Extends Afghan Food-Supply Contract for Firm that Hired Former Director," *Washington Post*, January 4, 2011, <http://washingtonpost.com>.
41. Neil Gordon, "Pentagon Ordered to Lift Suspension of Kuwaiti Contractor's Affiliates," *Project On Government Oversight (POGO) Blog*, July 3, 2012, <http://pogoblog.typepad.com>.
42. David Beasley, "Agility Prosecutors Probing 'Potential New Charges' in U.S., Judge Writes," *Bloomberg News*, July 27, 2011, <http://bloomberg.com>.
43. Neil Gordon, "'POGO Obtains Second Helping of 'Compelling Reason' Memos," *POGO Blog*, October 9, 2013, <http://pogo.org>.
44. Project on Government Oversight (POGO), "Fluor Corporation," Federal Contractor Misconduct Database, <http://contractormisconduct.org>; Transparency International UK, "Defence Companies Anti-Corruption Index 2012," report, London, October 2012, <http://companies.defenceindex.org/report>.
45. Project on Government Oversight (POGO), "Top 100 Contractors," Federal Contractor Misconduct Database, <http://contractormisconduct.org>.
46. U.S. Department of Defense, "Department of Defense Annual Energy Management Report Fiscal Year 2011," report, September 2012; U.S. Energy Information Administration, Countries, n.d. [2013], <http://eia.gov/countries>.
47. Johnston, "The U.S. Government Is Paying Through the Nose for Private Contractors."
48. American Society of Military Comp-trollers, "Service Support Contractors: One of the FY 2012 Budget Efficiencies," powerpoint presentation, Department of Defense, October 2011, <http://asmconline.org>.
49. Amy Belasco, "The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11," Congressional Research Service, report, Washington, DC, March 29, 2011, 38, <http://asmconline.org>.
50. Inspector General United States Department of Defense, "Report of Investigation: United States Army General William E. Ward, U.S. Army Commander, U.S. AFRICOM," report, Alexandria, VA, June 26, 2012, <http://wired.com>.
51. Spencer Ackerman, "Top General Undone by Spa Treatments, Snickers, Broadway Show," August 17, 2012, <http://wired.com>.
52. Center for Responsive Politics, "Defense," <http://opensecrets.org>.
53. Center for Responsive Politics, "DynCorp International, Expenditures" <http://opensecrets.org>; "DynCorp International, Recipients," <http://opensecrets.org>.
54. David Isenberg, *Shadow Force: Private Security Contractors in Iraq* (Westport, CT: Praeger Security International, 2009), 65.
55. Center for Responsive Politics, "Halliburton Co., Profile: Summary, 2012 Summary," <http://opensecrets.org>.
56. Government Accountability Office, "Decision in the Matter of Kellogg Brown & Root Services, Inc.," File: B-400787.2; B-400861, Washington, DC, February 23, 2009, <http://gao.gov>.
57. Center for Responsive Politics, "Supreme Group USA, Summary," <http://opensecrets.org>.
58. Center for Responsive Politics, "Agility Public Warehousing Co, Summary," <http://opensecrets.org>.
59. Center for Responsive Politics, "Fluor Corp, Summary," <http://opensecrets.org>.
60. Sunlight Foundation, "German State of Rheinland-Pfalz," <http://foreign.influenceexplorer.com>.
61. AALEP, "EU Member States' Lobbying in the U.S.," list from Foreign Agent Registration Act's Report, December 31, 2010, [2011], <http://aalep.eu>, 6; Sunlight Foundation, "The City of Heidelberg, Germany," <http://foreign.influenceexplorer.com>.
62. Robert S. McIntyre, Matthew Gardner,

Rebecca J. Wilkins, and Richard Phillips, "Corporate Taxpayers & Corporate Tax Dodgers 2008-10," report, Institute on Taxation and Economic Policy, November 2011, <http://ctj.org>, 8; U.S. Government Accountability Office, "Corporate Income Tax: Effective Tax Rates Can Differ Significantly from the Statutory Rate," report to Congress, GAO-13-520, Washington, DC, May 2013, <http://gao.gov>.

63. Robert D. Hershey Jr., "Tax Questions For Military's Contractors," *New York Times*, February 12, 2004, <http://nytimes.com>.

64. Farah Stockman, "Top Iraq Contractor Skirts U.S. Taxes with Offshore Shell Companies," *Boston Globe*, March 9,

2008, E7. A 2008 change in U.S. tax law closed the loophole that allowed companies to avoid paying Social Security and Medicare taxes but left the loophole intact for unemployment taxes, meaning that former employees remain ineligible for unemployment insurance. Government Accountability Office, "Defense Contracting: Recent Law Has Impacted Contractor Use of Offshore Subsidiaries to Avoid Certain Payroll Taxes," Highlights of GAO-10-327, Washington, DC, January 2010, <http://gao.gov>.

65. Chatterjee, *Halliburton's Army*, 210-11; Laura Mandaro, "Halliburton's Dubai Move Raises Issue of Expat Taxes," March 13, 2007, <http://marketwatch.com>.

66. Congressional Research Service, "Tax Exemption for Repatriated Foreign Earnings: Proposals and Analysis," Report for Congress, Washington, DC, April 27, 2006, <http://congressionalresearch.com>.

67. Senate Republican Policy Committee, "Territorial vs. Worldwide Taxation," September 19, 2012, <http://rpc.senate.gov>; Emily Chasan, "At Big U.S. Companies, 60% of Cash Sits Offshore: J.P. Morgan," *Wall Street Journal*, May 17, 2012, <http://blogs.wsj.com>.

68. United States Government Accountability Office, "Defense Contracting: Recent Law."

69. Senate Republican Policy Committee, "Territorial vs. Worldwide Taxation."



**MONTHLY REVIEW FOUNDATION is pleased to announce an award** that will support the publication in English of a series of distinguished monographs concerned with the political economy of imperialism. Authors of unpublished manuscripts in English or any other language who are recipients of the award will receive \$5,000. Where the award is granted to books already published in languages other than English, the \$5,000 will be applied instead to covering translation costs.

**For details and more information about Sweezy, Baran, and Magdoff, please visit <http://monthlyreview.org/press/sweezy-baran-memorial-award/>**

# U.S. Control of the Internet

## *Problems Facing the Movement to International Governance*

**PRABIR PURKAYASTHA AND RISHAB BAILEY**

After the Snowden revelations, Internet governance has emerged from relative obscurity, involving only a small technical community, to occupy the center stage of human rights discourse and international relations. For those who have only a hazy idea of how the Internet functions, it is particularly difficult to translate their concerns—freedom of speech, privacy, social and economic justice, and protecting and advancing democratic rights—to Internet governance.

Everyone agrees that digital technologies, including the Internet, are transformative technologies. They reorder society as a whole, as well as relations between society and individuals. But the potential—providing a megaphone to everybody who wants to speak, to provide a TV studio in every home—has not been fully realized. A case in point: instead of the democratizing potential of the Internet, a few global corporations have created monopolies that are much bigger than those we have seen before, and this has happened in just two decades. What does this mean, for instance, for the plurality of media voices? We know that Internet advertising revenue in the United States, having previously overtaken the print media, has now overtaken even TV network advertising revenues.<sup>1</sup> How did monopolies on such a scale happen, and happen so quickly? Does it have to do with the nature of the Internet? Or its architecture and governance?

If we talk of Internet governance, we need to understand what it is we are governing. On the one hand, the Internet is an infrastructure. On the other hand, it is a broad collection of services and applications.<sup>2</sup> In addition, there are several ways of looking at Internet infrastructure and hence its governance. There is the narrow technical view of the Internet as the interconnection of various networks. In this view Internet governance relates to the control over the resources that makes these interconnections

---

**PRABIR PURKAYASTHA** (prabirp@gmail.com) and **RISHAB BAILEY** (rishab.bailey@gmail.com) are associated with the Knowledge Commons collective, New Delhi and with the Just Net Coalition. The authors would like to thank Richard Hill and Felicity Ruby for their comments and help in writing this article.

possible: critical Internet resources such as domain names, IP addresses (equivalent to telephone numbers in the telephone system), and the protocols through which the communications takes place.

A larger view of the Internet would add to this narrow view of interconnections the complex of networks and the different pieces of software and hardware that run the entire infrastructure. In this larger view, the telecommunications network on which the Internet services run would also be a part of the Internet. Governance then would involve control and regulation of *all* the elements that constitute the Internet, including its telecommunications layer. While these are elements that constitute the basic infrastructure of the Internet, the functions that the Internet performs are much wider. They comprise the whole range of services that are provided by Internet companies when we log online. Separately, there are the computers (including tablets, smart phones, and other intelligent devices) through which we connect to the Internet.

The Internet today has become the global marketplace, the repository of knowledge, the global media, and an essential means of communication. Each of these has enormous social significance. Not surprisingly, the development of the Internet has been compared to the communication revolution ushered in by the printing press.<sup>3</sup> It is this combination of services and infrastructure that affects us. So Internet governance, in the broadest sense, means not only the actual layers that provide the communication system, but also the services—all the transactions that are performed by using the application layer that runs on the cloud computing systems on the Internet as well as on our computers.

But there are contesting ideologies that drive different perceptions of the issues salient to Internet governance. The dominant ideology, promoted by the United States, is that of “free and open” Internet—free from all regulations and government control (except of course those regulations and controls imposed by the United States itself, such as copyright and prohibitions on online gambling). Contesting perceptions hold that this dominant ideology does not address the relationship between the control of these resources with the concept of the larger public good, or even public utility. This range of ideologies, and their areas of contestation, came sharply to the fore in the NETmundial Conference held in San Paulo in April 2014.<sup>4</sup> Originally called by Brazilian President Dilma Rousseff to address the blatant violations of sovereignty and privacy by the National Security Agency (NSA) of the United States, it also became about contesting models of Internet governance.

### The Snowden Revelations: A Loss of Innocence

The Edward Snowden revelations, published in leading newspapers around the world since June 2013, marked a watershed moment in how the Internet is viewed and governed. Since this moment, the Internet, hitherto looked upon as beneficial tool, has been treated with an entirely new level of suspicion.<sup>5</sup>

While the popular media has, by and large, focused on issues surrounding the invasions of privacy by the NSA's mass surveillance programs, there is a far more important issue at stake—control. The Snowden revelations have highlighted something rarely spoken about in the popular press or in political circles: the reality that the Internet is a centralized tool used to sustain economic and political dominance in a globalized world.<sup>6</sup>

When Snowden first met Laura Poitras and Glen Greenwald, two of the journalists working with him, he told them that the documents they would see would not only reveal surveillance on an unimaginable scale, but would also demonstrate the economic and political hegemony of the United States.

The list of targets exposed by Snowden is almost endless. Political targets include heads of state such as Angela Merkel, Dilma Rousseff, Gerhard Schroeder, and Enrique Pena Nieto; numerous embassies; UN offices; and public institutions and international negotiations.<sup>7</sup> The list of commercial/economic targets is bound to grow as more documents are made public from Snowden's trove. We already know of the United States and Canada spying on the Brazilian oil company Petrobras and the Ministry of Mines and Energy (which were involved in the auction of oil fields of the coast of Brazil), and the weakening and hacking of the SWIFT network (which is used by finance majors such as VISA and Mastercard for international settlements).<sup>8</sup> This is in addition to spying on the EU competition commissioner; spying by Australia on Timor-Leste (formerly East Timor) during negotiations regarding oil exploration rights in the East Timor sea; and, rather strangely, spying on a U.S. law firm that was advising the Indonesian government on trade disputes (on shrimp and clove cigarettes) with the United States.<sup>9</sup>

The most commonly used argument to justify mass surveillance of the kind undertaken by the NSA (as well as its British equivalent, the General Communications Headquarters—GCHQ) is the protection of civilians against political violence (or terrorism). This was indeed the default argument made when the Snowden revelations were first published. Various U.S. government officials stated that information gleaned through mass surveillance had been used to stop more than

fifty terrorist attacks in the United States and abroad. These statements did not stand for long: two U.S. senators, Ron Wyden and Mark Udall, scrutinized confidential documents of the intelligence agencies and reported that the collection of phone records had played “little or no role” in the disruption of terrorist plots.<sup>10</sup> There was a role played, however; the benefit, it became clear, lay elsewhere.

The European Union had earlier charged that information from Signal Intelligence programs (notably the Echelon program) was used to benefit U.S. companies.<sup>11</sup> And big global U.S. corporations, such as AT&T, Verizon, Microsoft and Google, have now been deeply implicated in the NSA’s dragnet surveillance.

There is little doubt that most countries today carry out mass surveillance of their citizens. What makes the Five Eyes mass surveillance program different is its sheer scale. The Five Eyes is a supranational surveillance alliance dominated by the United States; though formally called the UKUSA Agreement, it came into existence in 1946 between the United States and the United Kingdom, and was later extended to Canada, Australia, and New Zealand. The surveillance program has compromised every layer of the Internet: the telecom layer, both at the fiber optic backbone level and at the Internet Service provider (ISP) level; major Internet companies partnering the NSA, such as Google, Facebook, and Yahoo; software companies such as Microsoft, who have given access to the computer systems of their consumers through backdoors and other security holes; and, finally, hardware companies such as CISCO, Apple, and others.<sup>12</sup> The technical community—the supposed protector of freedom on the Internet—has been implicated in weakening encryption standards.

This has been greatly facilitated by the United States being the major hub of the global fiber optic network, followed by the United Kingdom, where a major part of the trans-Atlantic cables land.<sup>13</sup> The United States has used its position as a global hub to force various fiber optic network operators to give them physical access to their networks in order to obtain necessary U.S. licenses.<sup>14</sup> The AT&T Folsom Street case made public how AT&T was giving NSA access to its cable network.<sup>15</sup> This access has now been replicated for other network operators who have landing stations in the United States through specific agreements. As the bulk of global voice and Internet traffic pass through the United States, its surveillance agencies automatically have access to all this traffic.<sup>16</sup>

As if all this was not enough, the NSA has more tricks up its sleeve. Its Tailored Access Operations group can access specific machines through software or even hardware “implants.”<sup>17</sup> Computers have been

intercepted by introducing transit and spy devices that are then used to tap into the systems. The estimate is that up to four million machines could have been compromised in this way. In effect, these machines can then act as proxies of the NSA, and even mount attacks on other networks with the NSA claiming total deniability.

In other words, instances of surveillance which have no security concerns whatsoever have clear economic and political significance. The fact that the online sphere—both in terms of infrastructure/hardware and applications/services—is dominated by U.S. multinational corporations is an important aspect of this exercise of hegemony.

Perhaps the most dangerous part of the surveillance that Snowden has revealed has to do with the Computer Network Exploitations (CNEs). These are software implants in other countries' networks that have the ability not only to tap into the data streams of these networks, but also to take these networks down—they are cyber-weapons that have been armed and can be activated with just a single command. Fifty thousand CNEs have been reported to have been implanted in the global telecom networks. A map showing the location of the CNEs is instructive—five countries have no CNEs in their networks.<sup>18</sup> No prizes for guessing which are these five countries!

One of the most significant aspects of the Snowden disclosures which has not attracted adequate attention has to do with the cyber-attack targets that Obama has authorized—through Presidential Policy Directive 20.<sup>19</sup> It implies that foreign networks have been penetrated and their security systems already compromised; vital infrastructure of other countries has been pretargeted and awaits only a command to trigger a cyber-attack.<sup>20</sup> The United States has blocked all attempts to initiate a cyber-war treaty, arguing that such a treaty is not enforceable—while going ahead with its cyber-war preparations.<sup>21</sup> This increases, radically, the risk of triggering an arms race in cyberspace and fracturing the Internet.

A complex and insidious relationship, which has appropriately been called the “Digital Industrial Security Complex” in some quarters (to indicate the proximity of the military industries, massive technology companies, and political processes), acts as a self-reinforcing structure. With powerful political processes bent on ensuring unregulated (or minimally regulated) access to global consumers, the unprecedented monopolies and concentration of media and telecommunication industries, and the threat of terrorism (used as a red herring to weaken civil liberties), it seems as if there is almost no way in which online space can be reclaimed.

To put it simply, the United States and its allies will spy on anything and anyone—using any means possible—if they perceive that this will enhance their political and economic interests. For the United States, international economic affairs comprise an intelligence issue. The NSA is an instrument intended to serve the interests of centralized political and economic power in Washington. The corporate interests colluding with the state are its special beneficiaries.

Another intriguing aspect of the Snowden revelations is confirmation that surveillance data—with its economic, social, and political implications—has become an international currency to be bartered between nations. This explains the race to try and establish mass surveillance capabilities in numerous countries across the world (including India). The new great game of information exchange has to be played by every nation—even if no country from the global South will ever be in a position to win.

In sum, Snowden has revealed that if left unchanged, current practices—of governance, business, and online activity—pose risks, not only to the privacy of citizens, but to the capacity of governments to protect what remains of their sovereignty, and to the ability of the global economic system (purportedly based on a complex of arms-length negotiated agreements) to function fairly and effectively. This is what Rouseff had pointed out in her speech last September in the United Nations, placing before the world body the urgent need for a new model of Internet governance. It is this call that subsequently led to the NETmundial Conference in Sao Paulo in April this year.

### **Internet Governance: The Background**

This section will specifically address the control of the key critical resources of the Internet—the Domain Name System (DNS) and the protocols that make the Internet interoperable. Internet governance, in this narrow sense, essentially comprises two general requirements—policymaking and technical standardization.<sup>22</sup> At the moment, policymaking regarding domain names takes place almost entirely through the Internet Corporation for Assigned Names and Numbers (ICANN). Policymaking regarding IP addresses takes place in the Regional Internet Registries (RIRs), and the protocols are made in the Internet Engineering Task Force (IETF). (But the overall allocation of IP addresses is performed by ICANN, which assigns large blocks to the RIRs.) The telecommunications infrastructure is managed under domestic laws of different countries, with the International Telecommunication Union acting as a global coordinator.



On the domain name system, we need to understand that this is high-value real estate, even if it is in the virtual world. The Internet has the potential to create an unlimited number of domain names: it is a part of the unlimited global commons that has been, or can be, created. ICANN's powers to control DNS space exists by virtue of a U.S. enclosure of the digital commons, and its handover to ICANN. The development of the DNS system by the United States (and its control of the system through control of the authoritative master server) has permitted the enclosure of this global commons by virtue of a historical/first-mover advantage.<sup>23</sup> At present, no framework gives legal rights to global top level domains (g-TLD's)—to any of the regional or national registers. All the legal rights are derived through private contracts with ICANN, various registers, and the existing contract that ICANN has with the Department of Commerce—the Internet Assigned Numbers Authority (IANA) functions contract.<sup>24</sup> ICANN is currently operating the IANA function on the basis of this contract.

The DNS and the IP address system—the basis on which the interconnected, interoperable network runs—is, juridically speaking, controlled through ICANN.<sup>25</sup> There are thirteen root servers with a “hidden” or “master” server which updates all thirteen public root servers.<sup>26</sup> Together these servers act as the central repository of the Internet's address book. The Master Server is operated by VeriSign Inc. (formerly Network Solutions Inc.), though it is subject to oversight by ICANN, and, ultimately, the U.S. Department of Commerce. The present procedure for modifying the authoritative root zone file is that the requests from TLD operators are received by ICANN, which forwards them to the Department of Commerce for approval.<sup>27</sup> The Department of Commerce then transmits the approved requests to VeriSign, which edits and generates the new root zone file.

The unilateral control of the DNS system by the United States is problematic for a variety of reasons. The most important of these is that it enables the U.S. government to control the creation and deletion of online property. We have seen instances of the U.S. government or courts forcing registries the world over to remove domain names from the addressing system.<sup>28</sup> This is what happened, for example, with Wikileaks and ‘.iq’ before the Iraq war.

The problem is not that the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA)—the body tasked with the IANA contract—routinely interferes with ICANN decisions. The control of the DNS system by the U.S. government

means that it can be used in a U.S. version of permanent war based on global “national security” concerns to harm organizations and other countries. It is important to stress that the U.S. control over the DNS is not just through the Department of Commerce, but also through the U.S. judicial system, which has jurisdiction over ICANN and VeriSign.

The United States also continues to have technical and economic leverage over the digital ecosystem. What this means is that the bulk of billions of dollars of virtual real estate is “owned” by registries in the United States and other developed countries. Verisign has revenue of over a billion dollars for the g-TLD of .com, created by the U.S. enclosure of the global domain name system. ICANN currently generates revenue of about \$400 million from the DNS system—all registrars have to give a part of the money they realize from sale of domains. (Registrars are retailers of domain names, registries are wholesalers.) It is a myth that the functions carried out by organizations such as IANA and ICANN are purely “technical” in nature. The day-to-day maintenance and administration of the DNS system is a technical matter—but the policies imposed for the management of the DNS space are public in nature. For example:

Control and regulation of property rights or the assignment of domain names: Issues of competition law, intellectual property etc. affect the community at large and require global political consensus. Notably, Section 6(1) (c) of ICANN’s bylaws recognize that ICANN does indeed perform public policy functions in requiring the Board to request and account for the advice of the Government Advisory Committee on such issues.<sup>29</sup>

Free speech: ICANN has instituted a mandatory dispute resolution policy that serves to limit critical speech.<sup>30</sup> An analysis of case law under the Uniform Domain Name Resolution Policy (UDRP) demonstrates that “numerous complainants have used domain name challenges as part of an attempt to silence critics.”<sup>31</sup> Further, ICANN policy prohibits anonymous ownership of websites.<sup>32</sup>

The historical development of the Internet has necessarily meant that the most influential Internet governance/standard setting organizations are first-world-centric. The numerous problems in the structure and functioning of these organizations include the following:

First, organizations such as ICANN, IETF, and Internet Society (ISOC) are not recognized “international organizations.” While this is less important in the case of the standard-setting organizations, it is crucial for an organization such as ICANN. As a U.S. corporation—subject

to U.S. domestic law and various restrictive covenants and standard terms contained in its contractual arrangements with the U.S. government—ICANN lacks the basic immunities and privileges enjoyed by recognized international organizations.

Second, they are susceptible to corporate capture, particularly to the benefit of U.S. corporations. Neither are standard-setting organizations free from corporate control; the Interactive Architecture Board (IAB) and IETF are dominated by U.S. industry.<sup>33</sup>

Third, composition and attendance of these organizations is not sufficiently global or diverse in nature. Despite rules regarding geographic composition of the Boards of organizations such as The World Wide Web Consortium (W3C), all these organizations are dominated—both in terms of actual membership, as well as in terms of participation in decision making roles—by people from the first world.<sup>34</sup>

Fourth, rule making continues to be haphazard and, on occasion, arbitrary. For instance, ICANN's bylaws have been amended approximately twenty times, with various commentators stating that these changes merely reflect the composition of ICANN at the time.<sup>35</sup> Decision-making procedures in technical organizations are susceptible to abuse both by governments and business interests due to their informal nature.

Though ICANN is bound, under California law, to give its board members access to its financial information, Karl Auerbach, an elected member from the North American users constituency, had to go to court before he was given such access. And while ICANN had initiated a process for direct global elections to its board, this was halted after just one trial in the early 2000s, largely due to the interests of entrenched players.

Fifth, these organizations contain self-perpetuating structures, lack true transparency and openness, and lack appropriate external independent review and accountability. For instance, despite frequent references to “consensus,” what this consensus constitutes, or how it comes about, is not clear. Self-selection or mutual nomination and interlocking members are common features of these organizations.

According to Auerbach “ICANN does not ‘assure the technical stability of the internet.’ Rather, ICANN dispenses commercial rights and privileges. In exchange for its largesse, ICANN obtains monopoly rents, significantly restricts legitimate and innovative business practices, and imposes expansive trademark protection well beyond what is required by any law of any nation.”<sup>36</sup>

### The Neoliberal Multistakeholder Model: A Critique

A large part of the discourse prior to the NETmundial conference was centered around the issue of the best system for Internet governance. This has commonly been portrayed as a choice between a relatively undefined multistakeholder model, and a comparatively well-defined multilateral model recognized in International Law, in which a nation state is recognized as the representative of its citizens. The U.S. government had originally argued for a private-sector-led Internet governance model.<sup>37</sup> At some point this appears to have morphed into the current “multistakeholder” model.<sup>38</sup> The form of the multistakeholder model that developed in the ICANN is different from the well-known and accepted consultative process in which all stakeholders participate, but elected representatives still make the decisions. In ICANN, the governments have only an advisory role through the Government Advisory Committee. The exception of course is the U.S. government, which has oversight of ICANN through the Internet Assigned Numbers Authority (IANA) contract and other agreements. To be accurate, it is a one-government-plus-private-sector-led Internet governance model that has existed until now. And this is what is now referred to as the multistakeholder model of Internet governance by the ICANN community.

The view of a nongovernment multistakeholder model has now given way even among some sections of the U.S. government to a stakeholder model that includes governments as stakeholders—but only as one among equals. A *Wall Street Journal* commentator, for instance, talks about the two U.S. government views of the multistakeholder model: “The Obama administration proposal (on IANA transition) would have treated other governments as equal stakeholders, turning the concept of private-sector self-governance on its head. Robert McDowell, a former commissioner at the Federal Communication Commission, pointed out that... ‘multi-stakeholder’ historically has meant no government, not many governments.”<sup>39</sup>

Thus the private-sector-led Internet governance initially in vogue in U.S. documents is now postulated as a form of a multistakeholder model sans one stakeholder—the governments. Obviously, as long as the U.S. government was in control, keeping other governments out was a U.S. strategy. That is why the current IANA transition that the United States has proposed has the precondition of “no government control” of Internet governance.<sup>40</sup>

The view of the multistakeholder model embedded in the IANA transition offered by the Obama administration is—in our view—a

neoliberal multistakeholder model.<sup>41</sup> It demands that governments play little role in internet governance, and that any role they actually play be placed on an equal footing with other stakeholders, and decisions on all aspects of Internet governance be made through consensus. Any criticism of such a model, or discussions on the different roles and responsibilities of different stakeholders, are then labeled a multilateral or a statist model paving the way for repressive governments to capture the Internet. Such a binary formulation—multistakeholder versus multilateral—misses the fact that while some issues such as technical protocols can be worked out between various stakeholders through a consensual process (global standards are created in this way), the issues change when public policy is involved. Essentially, policy issues demand that a concept of public interest be introduced to override the sectoral interest of certain stakeholders.

The neoliberal multistakeholder model of decision making—with all stakeholders on an equal footing, and through consensus—does not take into account that stakeholders have differing interests. For example, corporations and consumers have obvious differences in objectives. This model, in effect, gives veto power to private corporations and denies public good or public interest. Such a model would allow the corporate stakeholder section to block any consumer interest regulation simply by not allowing consensus to form on the issue.

The problem with such a model also becomes apparent if we take examples from other sectors. In pharmaceuticals, for instance, there is agreement that all stakeholders, including pharmaceutical companies, should make decisions by consensus on issues such as safety or the pricing of drugs. If such a principle had indeed been followed for retrovirals in AIDS treatment, for example, it would have meant a death sentence for a large number of AIDS patients. Public interest demands that states regulate drug prices in the interests of their people; similarly, for the safety of drugs.

The key difference between governments and corporations is that the governments are accountable to their people (at least in political theory), while corporations are answerable to their shareholders. The primary driver of corporations is profit; for governments, avowedly, it is the good of its citizens (even if governments do not necessarily fulfill this responsibility). If the governments—in the sense of the state and not just the executive—fail in their duties to the citizens, it is possible for the people to change their governments, either through elections in electoral democracies or through other means, in response to the

state's failure to maintain the social contract. By extension, if the need of corporations for profit is in conflict with larger social interests, the state has the right as well as the obligation to regulate prices and the profits of corporations. (It is worth noting in this context that ICANN does regulate prices.) Similarly, policy issues such as the safety of consumers or the protection of the environment demand that the needs of the citizens override the interests of capital. This is the basis of regulating corporations and monopolies. For this reason, putting governments and corporations on an equal footing on all matters and privileging decision making through consensus means effectively giving up the state's right to regulate private monopolies.

Net neutrality has been widely discussed in the context of Internet governance. It is an extension to the Internet of the well-known common carrier principle, which is to provide services to the public without discrimination. The underlying principle in net neutrality is that the carrier cannot discriminate between different sets of data packets "by user content, site, platform, application, type of attached equipment, and modes of communication."<sup>42</sup> Again, net neutrality is a regulatory issue and cannot be expected to be achieved by consensus among various stakeholders.

The combination of intelligence agencies and large, global corporations has helped concentrate economic power and create large global monopolies on an unprecedented scale. The U.S. stewardship of the key Internet organizations has enabled the United States to ensure that there is no international regulation of the Internet, while allowing extraterritorial application of many of its own laws and regulations (or lack of laws and regulations, such as lack of general protection of data privacy). This has led to the emergence of global monopolies in this space.<sup>43</sup> The Internet economy tends towards monopolization due to economies of scale and network effects. This means that global Internet companies can build Internet platforms that will allow bundling services—horizontal monopoly (Google, Microsoft). If you are already on a Gmail platform, this can be used to connect you to Google docs, Google+, and a host of other services. Others try and bundle access and services together—vertical monopoly such as telecommunications companies offering Internet services and then implementing various tiered pricing models for different kinds of services. This is, of course, what the net neutrality battle is all about.

It is not surprising that an unregulated Internet has generated extremely powerful monopolies in a very short span of time. Today,

the top three Internet companies control more than 40 percent of the global digital advertising revenue.<sup>44</sup> In the triple-digit mobile advertising revenue, the concentration is even sharper, with Google alone taking more than 50 percent of the revenue. Digital ad revenues overtook broadcast television's in 2013, having earlier overtaken satellite/cable television, indicating that digital advertising is rapidly replacing other media forms.<sup>45</sup> Again, a handful of companies controls the global e-commerce market. An unregulated market therefore leads to the formation of powerful monopolies, which in turn stifle competition and generate very high (or super) profits.

The issue is not the dichotomy between multilateralism and multistakeholderism as posed by proponents of a certain kind of multistakeholder model. The issue relates to the functions or issues that can legitimately be dealt with through each of the processes to serve the interests of society as a whole. For example, how do you deal with something like cyber-warfare and surveillance, which fall squarely within the province of the states? How do you protect the right of a country against unilateral disconnection? Similarly, how do you address regulatory issues such as determining costs of access, or regulating monopolies—both global telecom and Internet monopolies—so as to protect the consumers? In all of these issues, the role of the states and global corporations are different.

Under the neoliberal paradigm, the role of the state has changed “from being an entity apparently standing above society and intervening in its economic functioning in the interests of society as a whole, even at the expense of the unbridled interests of finance capital (such as for instance the State in the era of Keynesian demand management), to being an entity acting exclusively to promote the interests of finance capital.”<sup>46</sup> Here, we would like to expand the neoliberal state working in the interests of finance capital to other forms of rentier capital, including intellectual property holders. So when a proposed model of Internet governance formally takes away the role of the state in regulating corporations, its relationship to the neoliberal paradigm is obvious.

It is now clear that dragnet global surveillance has been carried out by the United States and other Five Eyes governments in alliance with the most powerful global corporations. These are also the forces that have been the loudest voices in favor of a multistakeholder model that wants global corporations to have a veto over Internet governance. Internet governance is at present carried out by the U.S. government and global corporations through existing Internet organizations. After

the Snowden revelations, the U.S. “stewardship” is no longer feasible. The U.S. response has been to offer to shift what it calls its “oversight” (in reality its control) to a multistakeholder process that meets with its approval. In March 2014, the United States stated that, “To support and enhance the multistakeholder model of Internet policy-making and governance, the U.S. Commerce Department’s National Telecommunications and Information Administration (NTIA) today announces its intent to transition key Internet domain name functions to the global multistakeholder community.”

There are, however, serious doubts about whether such a transition would ever take place. The U.S. Congress has already raised the question of why the Internet, a U.S. property, should be transferred to any other body where other governments can grab it. A letter written by thirty-five members of Congress gave strong support for “the existing bottom-up, multistakeholder approach to Internet governance.”<sup>47</sup> Interestingly, the U.S. Congress does not believe that such a discussion on IANA transition should be multistakeholder in the United States, but purely the prerogative of Congress, showing U.S. hypocrisy in discussions on the multistakeholder model.

The congruence of such a multistakeholder model in which governments are treated on par with global corporations and the neoliberal paradigm is obvious. Underlying this model is that there should be no global regulations or laws. That is why ICANN, a private non-profit corporation registered in California, today runs the DNS system through private contracts with domain registrars.

The neoliberal paradigm’s central premise is that the state (or states) should not interfere with markets. But this cannot work where there are “natural monopolies” such as telecom, electricity, and water distribution. In such cases, the state’s task could be to (1) be the supplier of such services, and (2) regulate such services either directly or indirectly by creating a regulatory market. A complete withdrawal of the state from providing services or regulating private service providers would lead to obvious adverse consequences.

It is telling that in the United States, where Internet access is not regulated, the broadband costs have been far higher, and quality well below, that in other advanced countries.<sup>48</sup> Most consumers in the United States use either a cable operator or their telecom operator for provision of high-speed Internet. As a consequence of this duopoly, the U.S. internet speeds are of an order of magnitude lower than other countries. The telecommunications expert, Susan Crawford, in an



interview with NPR, talked about her visits to Seoul and Stockholm. According to Crawford, “For about \$25 a month they’re getting gigabits symmetrical service, which is 100 times faster than the very fastest connection available in the United States and for a 17th of the price.” For her, the answer is simple—the government must regulate the market: “That’s how we did it for the telephone, that’s how we did it for the federal highway system, and we seem to have forgotten that when it comes to these utility basic services.”

Incidentally, the costs of broadband in most parts of the global South are even higher than those in the United States. This is partly due to the high cost of interconnection, which helps the big players and penalizes the small ones. The big players interconnect among each other at no cost, while the smaller players have to pay the full cost of the interconnections. This, of course, is market economics; the markets help the big at the expense of the small. In the more civilized (and now gone) days of telephony, the development of the International Telecommunication Union meant a conscious decision to subsidize the small players at the expense of the big ones. The rationale was that an expansion of the network was in the larger social interest.

### **NETmundial: The Context**

The Snowden revelations have highlighted the importance of the World Summit on the Information Society (WSIS) Tunis Agenda regarding Internet governance.<sup>49</sup> At WSIS a number of countries challenged the U.S. control over the DNS system.<sup>50</sup> How can vital infrastructure, needed by every country for communications and commerce, operate under the jurisdiction of one particular government? WSIS raised this issue and underlined the need to enhance the role of other governments in Internet governance. Articles 68 and 69 of the Tunis Agenda addressed the need for such Enhanced Cooperation.

The WSIS identified the need for a more participatory structure for other governments. But the Internet Governance Forum set up after Tunis was a body that could only discuss issues; it could take no binding measures. The Enhanced Cooperation agenda—essentially a code for addressing U.S. control over the Internet—got nowhere with endless discussions; the United States and its allies, including the Internet organizations, stonewalled the issue.

Brazil initiated a process within the India-Brazil-South Africa (IBSA) dialogue forum for a different form of Internet governance. It developed into a Declaration in Tshwane, South Africa, in October 2011, for

a multilateral, democratic, and transparent Internet. It focused on the “urgent need to operationalise the process of ‘Enhanced Cooperation’ mandated by the Tunis Agenda” of WSIS, and to set up a multilateral body under the United Nations for Internet governance.<sup>51</sup> At the sixty-sixth meeting of the UN General Assembly on October 26, 2011, India proposed the setting up of a new UN-based body to act as a nodal governance agency of the Internet.<sup>52</sup> However, none of these efforts was pursued seriously by either the IBSA or the three countries individually.

Internet governance also came up at the 2012 World Conference on International Telecommunications in Dubai, with particular reference to revising the International Telecommunications Regulations (ITRs). Without getting into details, there was an attempt to paint the International Telecommunication Union as the villain trying to gain control over the Internet. Such a narrative was fashioned by the United States and a set of U.S. corporations, though a section of “civil society” also lent their voice to the chorus. The consequence was that though eighty-nine countries signed the new ITRs, the United States and the European Union refused to sign, citing grounds that were highly controversial.<sup>53</sup>

Things changed radically after the NSA revelations. In her speech in the UN General Assembly, Rouseff raised the issue of surveillance and called for a global meeting on multilateral Internet governance.<sup>54</sup> The NETmundial, organized in April 23–24 in Sao Paulo, Brazil, was a consequence of this call. A number of the organizations connected to Internet governance—including ICANN, IETF, IAB, the W3C, ISOC, and the five regional Internet address registries (the “I\* organizations”)—met in Uruguay on October 7, 2013, and issued a statement distancing themselves from the U.S. government and its actions.<sup>55</sup> They called for an “environment in which all stakeholders, including all governments, participate on an equal footing.” Fadi Chehade, the CEO of ICANN, then met with Rouseff and supported her call for a global conference. ICANN and the other Internet organizations soon became partners to CGI.br—the Brazilian Internet Steering Committee, the organization selected by the Brazilian authorities to run the conference and help set up INet, the counterpart of CGI.br in NETmundial.<sup>56</sup> Thus the United States gave itself a guarantee against an unacceptable outcome.

From the beginning, there were two currents to NETmundial. On the one hand were the issues identified by Rouseff regarding surveillance, the violation of sovereignty of countries, and the call for an increased multilateral oversight of the Internet. On the other hand, there was the call of Internet organizations such as ICANN for a multistakeholder

model, in which governments would participate, but along with other stakeholders—essentially the equal footing, multistakeholder model. If ICANN and other Internet organizations had not played the role they did, the Brazilian conference would, conceivably, have been more focused on the mass surveillance issues and the Enhanced Cooperation issue flowing out of the Tunis Agenda.

To return to the specific fallout of the Snowden revelations that we have already discussed: the U.S. “stewardship” and its direct control of the DNS is no longer feasible, given the huge trust deficit it faces. The U.S. response has been an offer to shift what it calls its “oversight” (in reality its control)—the IANA transition—to a multistakeholder process that meets with its approval.

The March 2014 NTIA announcement by the U.S. Department of Commerce is an attempt to steer the discussion into a narrow framework. By defining the limits of any transition under which the United States would be willing to give up its control, the United States ensures that it will not really have to do so. The condition set is a “multistakeholder model” in which governments either play no role, or, at best, they play a role equal to that of other stakeholders including business. The United States can then retain *de facto* control over the Internet, via its juridical control over the Internet organizations and the U.S. corporations, while giving up its *de jure* control of direct oversight.

The ICANN has already released a draft of the scope of the transition.<sup>57</sup> In effect, this means that all IANA functions will be transferred to ICANN, and anything outside such a transfer is out of scope.<sup>58</sup> The ICANN community broadly supports the private sector-led, multistakeholder model of Internet governance, in line with the U.S. precondition for giving up the IANA function.<sup>59</sup>

The multistakeholder model proposed by ICANN and the United States—as we have discussed earlier—considers that the Internet should be private and not regulated (except by U.S. laws and regulations). Those opposing this model and proposing an alternate model based on different roles and responsibilities for the stakeholders propose a greater role for the state in regulating the Internet and protecting the rights of citizens. Those who are against this model then use the rhetoric that any such role for the states in effect supports the takeover of the Internet by authoritarian states such as China, Russia, Iran, and Saudi Arabia.

Underpinning the two models of Internet governance is the question of what the Internet represents for the United States and its allies,

on the one hand; and other countries, particularly the BRICS countries, on the other hand. The European Union has not been happy with the sole control of the United States over the Internet, but has not done too much to rock the U.S.-controlled boat. (This is largely because a few countries, led by Sweden and the United Kingdom, strongly support the U.S. position within the EU discussions.) For the United States, the Internet is an instrument to pry open other countries—both economically and politically. It sees the economic monopoly of the global Internet companies as a means of expanding its control; and also, as we now know, as partners for its surveillance. If it wants regime change in a country, a “free and open” Internet is very much in its interest. Freedom of speech, in line with what the United States considers free speech, is again in its political interest.<sup>60</sup> If these two goals demand an unfettered Internet, its need for intellectual property or copyright protection needs a much more closed Internet. This is why global Internet companies and content companies have clashed on issues such as SOPA (Stop Online Piracy Act) and PIPA (Protect IP Act) and the dichotomy in the U.S. position has sharpened—a free and open Internet must be closed to even fair use provisions in copyright law.<sup>61</sup>

The BRICS countries, like many other global South countries, would like to protect their economic space. For countries such as China and Cuba, and also Iran, there is the additional threat of regime change. The Great Firewall of China has economic value in addition to serving its political need to block sites it considers dangerous. China is the only country that has built the equivalent of Google, Twitter, and Ebay. The Chinese microblogging sites, its search engine and the Internet e-commerce sites are not only dominant in China; they are also worth billions of dollars in the global stock market. For all practical purposes, China has built its own Internet that connects to the global Internet, but remains under its control. Other BRICS countries have not been able to match the Chinese achievement (or have not tried it as yet).

The Chinese therefore have the advantage that their Internet functions almost autonomously of the global Internet. They have an interest in global Internet governance, but are not much affected by it either way. Other countries such as Brazil, India, and even Russia are far more interconnected to the global Internet than China and so need to address the global Internet governance issue more vigorously. This difference was visible before and during the NETmundial, where China was for all practical purposes an observer while India and Brazil were important actors, though Russia less so.

The split between the states is understandable; there are some countries that benefit from the existing status quo while others lose. The flow of information over the Internet is completely asymmetric with the global South receiving and paying not once, but twice for the data packets they receive; once to download the information they need, the second time to “pay” for the advertisements they receive.

The split in “civil society” is less clear and depends on what the civil society groups think is important. For a number of civil society groups, freedom of speech and privacy are the major concerns. A number of them instinctively believe that the governments of the United States and other Western countries are preferable to the governments of countries in the global South, who are much more likely to interfere with the “free and open” Internet.<sup>62</sup> For them, the technical community is the final protector of freedom by hardwiring it in the structure of the Internet.<sup>63</sup> However, today’s Internet self-evidently does not preserve privacy, so this community cannot also “hardwire freedom” into the Internet. The issue here is that a set of actors in the civil society space, though shaken by the Snowden revelations, still believe that in matters of free speech and free Internet, the main threat is from nation states, particularly in the global South. Most of these civil society actors find countries such as Russia, China, Iran, and sometimes India (depending on India’s position) beyond the pale, and the Western countries and their corporations—in spite of dragnet surveillance—less of a threat.

Others in civil society have argued that digital colonialism and global corporations backed by the United States and other developed countries constitute the major threat today.<sup>64</sup> For these civil society groups, free speech is the narrative used to open the global South to penetration by the North, both politically and economically.<sup>65</sup> Such groups are not unaware of the mass surveillance or attacks on free speech in the global South. But they do not believe that the solution lies in aligning with the global North in supporting a neoliberal model of Internet governance and helping digital colonialism.

For both sets of civil society actors, the battles that need to be fought are identical; it is the priorities that decide the alignment. Much of the support for the multistakeholder model within civil society stems from alignment—if necessary with global corporations and Western powers, particularly if this also gives civil society actors a seat at the table of Internet governance. In aligning with the Western powers for a “free and open internet,” they eerily echo the white protagonist Marlow in

Joseph Conrad's famous novel set in Africa, *The Heart of Darkness*: "The conquest of the earth, which mostly means the taking it away from those who have a different complexion or slightly flatter noses than ourselves, is not a pretty thing when you look into it too much. What redeems it is the idea only...and an unselfish belief in the idea."<sup>66</sup> The "idea" then was civilization; the idea today is "a free and open Internet." We would like to grant them their unselfish belief "in the idea," even though the consequences for us—those with a different complexion or flatter noses—may be equally ugly. If in doubt, all we need to do is ask the Iraqis or the Libyans.

The Brazilian civil society has been fighting for Marco Civil—an Internet Bill of Rights—for the last three years. It has built its multi-stakeholder model around this struggle. However, the Brazilian groups have failed to see the analogy between a multistakeholder model within a nation state where national laws hold good, and a global multistakeholder model in which the equivalent of national laws are treaties. Transferring the Brazilian model to an international level without calling for treaties misses this important point, and results in calls for a multistakeholder model with no international norms to constrain corporate power.

The NETmundial was held within this context. For those who support a neoliberal multistakeholder model—ICANN and other I\* organizations—NETmundial was a platform to bury the multilateral, Tunis Agenda of WSIS and replace it with a new, multistakeholder model. This would also help in the IANA transition—as ICANN would then be accountable only to itself in the name of its stakeholders, and so be able to meet the U.S. preconditions for relinquishing its role.

### **NETmundial: The World Cup of Internet Governance**

The NETmundial had a structure of a High Level Committee of twenty-seven members, consisting of representatives of twelve governments and another twelve chosen from business, civil society, academia and the technical community, and three from the international organizations. An executive board of four members consisting of a representative from each of the stakeholders was selected to be co-chairs and run the conference. In keeping with most such multistakeholder processes, neither the criteria nor the process of such selection was ever furnished. INet, the body that ICANN had set up, called the shots and decided who the representatives of each of the stakeholders—the twelve members of the High Level Committee—should be. The civil

society co-chair of the conference proved to be highly controversial and drew protests from a section of the civil society.<sup>67</sup>

The NETmundial was conducted through an open process in which proposals on Internet principles and the Roadmap for the future were sought. Over 180 proposals were received, from which an initial draft was prepared and submitted (by the Executive Stakeholder Committee) to the High Level Committee.<sup>68</sup> Wikileaks leaked this draft and it appeared to be a reasonable compilation of the inputs. However, the High Level Committee effectively gutted the draft on three important counts. All references to surveillance and cyber-weapons were taken out; net neutrality was jettisoned despite the fact that surveillance was one of the topics mentioned most frequently in the inputs.<sup>69</sup> The final draft presented to the conference by the High Level Committee also had a number of references to an equal footing, consensus-based, multistakeholder process. Rousseff's NETmundial speech made it clear that the Brazilian government's position, as expressed in the UN General Assembly, had not changed.<sup>70</sup> She reiterated the need for a world free of mass surveillance and cyber-weapons and the importance of net neutrality. She also referred to the multilateral-multistakeholder process of Internet governance, setting the stage for a two-day contestation between the two sets of forces—the neoliberal multistakeholder model versus those arguing for the continuation of the Tunis Agenda—a multistakeholder model in which the stakeholders have their respective roles and responsibilities.

The NETmundial multistakeholder process showed that an open process allows a wide-ranging discussion—but it also showed its weakness. Though the number of interventions, including those from remote hubs, was large, the final non-binding outcome document was again prepared without a clear sense of who was driving which agenda. Business was allowed to smuggle in an Intellectual Property Right qualification to the right to share, create a proviso for private policing by ISP's on behalf of content owners, and bury net neutrality in the section on future action.<sup>71</sup> Surveillance came in, but in a watered down form—with no condemnation of mass surveillance, and in a language which the United States and United Kingdom would hold compatible with their practices.

On the key issue of the multistakeholder model, different people will read different meanings into the outcome text. Though some have argued that the WSIS Tunis Agenda was replaced by the NETmundial outcome, this did not happen.<sup>72</sup> On the contrary, the Tunis Agenda and

its key points are reaffirmed in the document. The roles and responsibilities of the respective stakeholders have been qualified by adding the word “evolving,” while the need for a consensual process has been qualified by “as far as possible.” Democracy has now been added to the multistakeholder process without defining what a “democratic multistakeholder process” actually means.

Russia and Cuba did not agree to the outcome document and disassociated themselves from it. India stated that it could not agree to the outcome without further consultations with their government. Business expressed its happiness while civil society groups were less than happy with the outcome.

The disquieting part of the NETmundial process was the obvious disarray within possible allies. Forget the traditional G77, the BRICS or even the smaller subset of IBSA were disunited. If Brazil signed the Final Acts of World Conference on International Telecommunications in 2012 while India stayed out, at NETmundial the roles were reversed; Brazil seemed willing, at least initially, to go along with the United States on an equal footing, neoliberal, version of the multistakeholder model, while India showed clearly its unhappiness with such a model. It was clear that the United States and its allies—the key Internet organizations—have worked out a game plan along with business. Sections of civil society have either been ideologically co-opted into this neoliberal multistakeholder formulation of Internet governance, or captured by active corporate interests.<sup>73</sup>

The saving grace in NETmundial is that the forces for the status quo could not get their way either, and achieve an unequivocal endorsement of the neoliberal multistakeholder model. Instead, we now have openings on both sides—for going further down this route or developing a truly democratic multistakeholder model with clearly defined roles for each of the stakeholders. The question before us is how we take back the Internet from the alliance of global corporate interests and the United States.

The battle for democratic Internet governance, where peoples’ interests prevail, calls for a much wider battle. It means a battle against the surveillance state. It is a struggle against digital colonialism and the rentier economy of the Internet. It is a struggle for enlarging the global knowledge commons which is made possible by the Internet. It is a battle for freeing our computer hardware and software from proprietary systems and moving on to free and open source platforms. It is also a part of the larger struggle of the global South against



imperialism. Unless we can bring all these strands together, it would be difficult to beat back this offensive of global capital. The Internet today is broken: people are under surveillance, and our data is being monetized and sold. If we want to change this, we need a different form of Internet governance. Cosmetic changes to existing institutions will not do. Deep-rooted changes are required, the kind of changes that will expand democracy and social and economic justice, preserve the rights of people as well as the sovereign rights of countries, and ensure that the Internet is used for peace—not war.

## Notes

1. Though the combined revenue of cable/satellite and broadcasting revenue is almost twice that of digital revenues in the United States, the digital ad revenues have overtaken individually the two segments of TV revenues.
2. See for example Richard Hill, "The Internet, Its Governance, and the Multi-Stakeholder Model," *Info* 16 no. 2, (2014): 16–46.
3. John Bellamy Foster and Robert W. McChesney, "The Internet's Unholy Marriage to Capitalism," *Monthly Review* 62, no. 10 (March 2011): 1–30.
4. *NETmundial*, <http://NETmundial.br>.
5. Prabir Purkayastha and Rishab Bailey, "Evolving a New Internet Governance Paradigm," *Economic and Political Weekly* XLIX, no. 2, January 11, 2014, <http://epw.in>.
6. See Shawn Powers and Michael Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom* (Urbana: University of Illinois Press, forthcoming) and Dan Schiller, *Digital Depression: Information Technology and Economic Crisis* (Urbana: University of Illinois Press, forthcoming).
7. See, for example, "Documentos da NSA apontam Dilma Rousseff como alvo de espionagem," *Globo*, September 9, 2013, <http://g1.globo.com>; Jens Glüsing, Laura Poitras, Marcel Rosenbach, and Holger Stark, "Fresh Leak on US Spying: NSA Accessed Mexican President's Email," *Spiegel*, October 20, 2013, <http://spiegel.de>; James Ball, "NSA Monitored Calls of 35 World Leaders After US Official Handed Over Contacts," *Guardian*, October 24, 2013, <http://theguardian.com>; Spiegel Staff, "Embassy Espionage: The NSA's Secret Spy Hub in Berlin," *Spiegel*, October 27, 2013, <http://spiegel.de>; Ewen MacAskill, et. al., "GCHQ Intercepted Foreign Politicians' Communications at G20 Summits," *Guardian*, June 16, 2013, <http://theguardian.com>. Public institutions and international negotiations include the G20 summit of 2008 and the climate change talks at Bali and Copenhagen in 2007 and 2009 respectively.
8. "NSA Documents Show United States Spied Brazilian Oil Giant," *Globo*, September 8, 2013, <http://g1.globo.com>; "NSA Accused of Spying on Brazilian Oil Company Petrobras," *Guardian*, September 9, 2013, <http://theguardian.com>; "Follow the Money: NSA Spies on International Payments," *Spiegel*, September 15, 2013, <http://spiegel.de>.
9. "GCHQ and NSA Targeted Charities, Germans, Israeli PM and EU Chief," *Guardian*, December 20, 2013, <http://theguardian.com>; "East Timor-Australia Spying Scandal," December 16, 2013, *Diplomat*, <http://thediplomat.com>; James Risen and Laura Poitras, "Spying by N.S.A. Ally Entangled U.S. Law Firm," *New York Times*, February 15, 2014, <http://nytimes.com>; Oliver Laughland and Bridie Jabour, "Indonesia: Australia and US Need to Clean Up Their Mess," *Guardian*, February 16, 2014, <http://theguardian.com>; Bridie Jabour and Martin Pengelly, "Australia Spied On Indonesia Talks With US Law Firm In 2013," *Guardian*, February 15, 2014, <http://theguardian.com>.
10. Ellen Nakashima, "Senators Say NSA Phone Records Played Little Role In Stopping Terror Plots," *Washington Post*, June 19, 2013, <http://washingtonpost.com>.
11. European Parliament, "REPORT On the Existence Of A Global System For the Interception of Private and Commercial Communications (ECHELON Interception System) (2001/2098(INI))," (section 13, "Conclusions and Recommendations), July 11, 2001, <http://cryptome.org>.
12. Timothy B. Lee, "Here's Everything We Know About PRISM To Date," *Washington Post*, June 12, 2013, <http://washingtonpost.com>; "File:PRISM Collection Details.jpg," accessed May 30, 2014, <http://en.wikipedia.org>; "File:PRISM slide 5.jpg," accessed May 30, 2014, <http://en.wikipedia.org>.
13. Prism slides available at "PRISM\_(surveillance\_program)," accessed May 30, 2014, <http://en.wikipedia.org>; map of global submarine cables system, see TeleGeography, "Submarine Cable Map," <http://submarinecablemap.com>.
14. For details of these agreements as are available, see Department of Defense, Department of Homeland Security, Department of Justice, Federal Bureau of Investigation, "U.S. Government Foreign Telecommunications Providers Network Security Agreements," July 9, 2013, <http://publicintelligence.net>.
15. Electronic Frontier Foundation, "AT&T's Role in Dragnet Surveillance of Millions of Its Customers," <https://eff.org>.
16. "File:PRISM slide 5.jpg," accessed May 30, 2014, <http://en.wikipedia.org>; TeleGeography, "Global Voice Traffic Map 2010," <http://telegeography.com>.
17. Staff, "Inside TAO: Documents Reveal Top NSA Hacking Unit," *Spiegel*, December 29, 2013, <http://spiegel.de>.
18. John Casaretto, "NSA-CNE-Map," November 28, 2013, <http://siliconangle.com>.
19. "We're Glenn Greenwald and Janine Gibson of the Guardian UK, and we've been breaking stories on the NSA Files since June. AUA!," *Reddit*, October 1, 2013, <http://reddit.com>; "Obama Tells Intelligence Chiefs to Draw Up Cyber Target List—Full Document Text," *Guardian*, June 7, 2013, <http://theguardian.com>.
20. Bruce Schneier is one of the top security experts in the world, who considers the Presidential Directive to be highly dangerous. See his "US Offensive Cyberwar Policy," *Schneier on Security*, June 21, 2013, <https://schneier.com>.
21. Barton Gellman and Ellen Nakashima, "U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations In 2011, Documents Show," *Washington Post*, August 30, 2013, <http://washingtonpost.com>.
22. For a broader discussion, see Richard Hill, "Internet Governance: The Last Gasp of Colonialism, or Imperialism by Other Means?," in Roxana Radu, Jean-Marie Chenou, and Rolf H. Weber, eds., *The Evo-*

*lution of Global Internet Policy: New Principles and Forms of Governance In the Making?* (Berlin: Schulthess/Springer, 2013) and Richard Hill, "The Future of Internet Governance: Dystopia, Utopia, or Realpolitik?," in Lorenzo Pupillo, ed., *The Global Internet Governance In Transition* (Berlin: Springer, forthcoming).

23. This could be seen as being similar to the United States claiming ownership and control of Mars as being the only or first country to have visited the planet.

24. IANA, the Internet Assigned Numbers Authority, is responsible in particular for the administrative processing of changes to the root zone for the Internet's Domain Name System (DNS).

25. See the MoU signed between ICANN and the U.S. Department of Commerce dated November 25, 1998 and extensions thereto.

26. Graham J.H. Smith, ed., *Internet Law and Regulation*, 4th edition (London: Thomas Sweet and Maxwell, 2007), 149.

27. The latest IANA functions contract effective October 2012 (<http://ntia.doc.gov>) states in Clause C.2.9.2 that: "the process flow for root zone management involves three roles that are performed by three different entities through two separate legal agreements: ICANN as the IANA Functions Operator, NTIA as the Administrator, and VeriSign (or any successor entity as designated by the U.S. Department of Commerce) as articulated in Cooperative Agreement Amendment 11, as the Root Zone Maintainer. Further, Clause C.2.9.2.a (At least notionally) permits ICANN to make changes (including additions) to the Root Zone File for TLDs."

28. For instance, in the case of Wikileaks numerous registries the world over were pressured to shut down the Wikileaks domain, see David Walsh, "US Government Preparing New Attacks Against WikiLeaks," *World Socialist Web Site*, August 26, 2011, <http://wsws.org>; Josh Halliday, "Wikileaks Site's Swiss Registry Dismisses Pressure To Take It Offline," *Guardian*, December 4, 2010, <http://theguardian.com>; Charles Arthur, "Wikileaks Under Attack: The Definitive Timeline," *Guardian*, January 8, 2010, <http://theguardian.com>. The Iraqi domain name .iq disappeared from the Internet prior to the launch of the Second Gulf War in 2003; see Dan Biddle, "Can We Find the All-Powerful 14th Server?," *BBC*, August 14, 2009, <http://bbc.co.uk>. The United States can enforce its courts' decisions over Internet websites by threatening deletion of the domain name as seen in the recent case where DVDfab, a Chinese company, was essentially chased off the Internet for not following U.S. domestic law. See Mike Masnick, "Ridiculously Broad Ruling Against DVD Ripper Software Has Court Allow Seizure Of Domains, Social Media &

More," March 11, 2014, <http://techdirt.com>. The United States can enforce its own decision regarding assignment of domain names—for instance the controversy over the Amazon domain name. See Lee Moran, "South America, Amazon Square Off in Fight Over Control of Amazon Domain Name," *New York Daily News*, December 4, 2012, <http://nydailynews.com>; Greg Bensinger, "Ruling: Amazon Can't Own 'Amazon'," *Wall Street Journal* blogs, July 17, 2013, <http://blogs.wsj.com>.

29. The board possesses final decision making powers.

30. For instance, the applicability of restrictive copyright law that ensures that critical websites (for instance ones that tag the word "sucks" onto various brand names) are removed.

31. This has resulted in websites that are critical of corporations etc., even if actually containing genuine content being barred if they utilize similar sounding names in their address (e.g., nikesucks.com will not be allowed to exist under this policy even if it contains genuine criticism of Nike). Milton Mueller, cf. Dawn C. Nunziato, "Freedom of Expression, Democratic Norms, and Internet Governance," 52 *Emory L.J.* 187 (2003), <http://scholarship.law.gwu.edu>.

32. *Ibid.*

33. The IAB board of directors lacks any global South membership and is dominated by people with industry affiliations. For instance, RFC 4440 states "Much of the early participation in the IETF as well as in the IRTF was from the academic and research communities. We don't have citation from this, but a look at the members of the IAB from the 1980s and early '90s shows IAB members from institutions such as MIT, UCLA, BBN, UCL, SDSC, and the like, while IAB members from the last few years were more likely to list their organizations as Cisco, IBM, Microsoft, Nokia, Qualcomm, VeriSign etc. See "IAB Thoughts on the Role of the Internet Research Task Force (IRTF)," March 2006, <http://tools.ietf.org>.

34. For instance, regarding ICANN, 81 percent of applications for membership in 2000 were from the European Union or United States, as compared to 19 percent from Latin America, Africa, and Asia/Pacific put together. Andrew McLaughlin, "Democratic Internet," slide presentation, June 15, 2000, <http://icann.org/en>. The IAB's present membership (in which almost all the concerned people have corporate affiliations) includes no representation from the global south, and only one woman; see IAB, "Members," accessed May 30, 2014, <http://iab.org>. Further, various insiders have commented on the lack of gender and racial parity and increasing corporate control of the W3C. See "An Angry Fix," July 17, 2006, <http://zeldman.com>; Molly E. Holzschlag, "Misplaced

Anger: A Rebuttal to Zeldman's Criticism of the W3C," July 26, 2006, <http://web-standards.org>.

35. "Rules for decision-making are frequently amended, often disregarded, and not reliably enforced.... If cyberspace is the 'electronic frontier,' ICANN has created a 'wild west' culture of politicized decision making." Hans Klein, "ICANN Reform: Establishing the Rule of Law," policy analysis for The World Summit on the Information Society, November 16-18, 2005, <http://internetgovernance.org>, 1.

36. Karl Auerbach, sample letter to U.S. congressional representatives, April 21, 2014, <http://cavebear.com/docs/ntia-icann-2014-others.pdf>.

37. The actual wording in the U.S. Department of Commerce 1997 White Paper and the 1998 Green Paper was "privatize the domain name system (DNS)." Interestingly, it was issued as a part of the Clinton administration Framework for Global Electronic Commerce. See U.S. Department of Commerce, "Management of Internet Names and Addresses, Docket Number: 980212036-8146-02," July 22, 2000, <http://icann.org/en>.

38. "However, it is worth mentioning that in the discussions on Internet governance during the first phase of WSIS, the term usually used to describe the existing arrangements was 'private sector-leadership,' in line with the language used in the setting up of the Internet Corporation for Assigned Names and Numbers (ICANN)." Markus Kummer, "Multistakeholder Cooperation: Reflections on the Emergence of a New Phraseology in International Cooperation," May 14, 2013, <http://internetsociety.org>.

39. L. Gordon Crovitz, "Keep the Internet Free—for Now," *Wall Street Journal*, April 13, 2014, <http://online.wsj.com>.

40. "In May 2012, the U.S. Congress resolved that U.S. authorities 'should continue working to implement the position of the United States on Internet governance that clearly articulates the consistent and unequivocal policy of the United States to promote a global Internet free from government control and preserve and advance the successful multistakeholder model that governs the Internet today.' Presumably this resolution refers only to keeping the Internet free from the control of governments other than that of the United States, because the United States continued to maintain its control over the Internet Assigned Names and Addresses (IANA) function." Richard Hill, "The Internet's Multi-stakeholder Model," World Telecommunication/ICT Policy Forum, May 14-16, 2013 (dated April 26, 2013), <http://google.co.in>, 4n12.

41. Slavka Antonova, "Power and Multistakeholderism: The ICANN Experiment," 2007, <http://lawlibraryarchive.contentdm.oclc.org>; Michael Gurstein, "The Multistakeholder Model, Neo-

- liberalism and Global (Internet) Governance," March 26, 2014, <http://gurstein.wordpress.com>.
42. "Net Neutrality," <http://savetheinternet.com/net-neutrality>.
43. Tim Wu, "In the Grip of the Internet Monopolists," *Wall Street Journal*, November 13, 2010, <http://online.wsj.com>.
44. "Google Takes Home Half of Worldwide Mobile Internet Ad Revenues," July 13, 2013, <http://emarketer.com>.
45. *IAB Internet Advertising Revenue Report: 2013 Full Year Results*, April 2014, <http://iab.net>.
46. Prabhath Patnaik, "The State Under Neo-liberalism," *MRZine*, October 8, 2010, <http://mrzine.monthlyreview.org>.
47. Cited in Camille Stewart, "35 Senators Ask Tough Questions Re: Internet Transition," April 2, 2014, <http://thedigitalcounselor.com>.
48. Susan Crawford, *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age* (New Haven: Yale University Press, 2013).
49. "Tunis Agenda for the Information Society," World Summit on the Information Society, Geneva 2003-Tunis 2005 (dated November 18, 2005), <https://itu.in>.
50. Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2010); Richard Hill, "WSIS+10: The Search for Consensus," *Latin America in Movement* no. 494, April 2014, <http://alainet.org>, 31-33.
51. "Tshwane Declaration-India-Brazil-South Africa (IBSA) Dialogue Fórum," October 18, 2011, <http://vascopress.com.blogspot.in>.
52. "India's Proposal for a United Nations Committee for Internet-Related Policies (CIRP)," 2011, <http://itforchange.net>.
53. Prabir Purkayastha, "WCIT-Why the US and Its Allies Walked Out," December 27, 2012, <http://newslick.in>; Richard Hill, *The New International Telecommunication Regulations and the Internet: A Commentary and Legislative History* (Berlin: Schalthess/Springer, 2013); Richard Hill, "WCIT: Failure or Success, Impasse or Way Forward?," *International Journal of Law and Information Technology* 21 no. 3 (2013): 313.
54. Dilma Rousseff, statement to the UN General Assembly, 68th session, September 24, 2013, <http://gadebate.un.org/68/brazil>.
55. "Montevideo Statement on the Future of Internet Cooperation," October 7, 2013, <https://icann.org/en>.
56. Paul Wilson, Director General of APNIC (APNIC is a regional registrar and a part of the Montevideo statement), said "During this time, ICANN proposed the name of '1net' as a banner of sorts, under which this movement could be formed." See Wilson, "What Is '1net' to Me," November 29, 2013, <http://circleid.com>.
57. "Scoping Document," <http://icann.org/en/about/agreements/iana/iana-transition-scoping-08apr14-en.pdf>.
58. Milton Mueller, "ICANN: Anything That Doesn't Give IANA To Me Is Out of Scope," April 16, 2014, <http://internet-governance.org>.
59. Steve DelBianco, ICANN's policy chair for the Business Constituency, said "Ultimately, I think that most of us in the ICANN community want the same thing: an accountable, stable organization that maintains its commitment to private-sector-led, multistakeholder management of the DNS." DelBianco, "The Path Forward: Accountability Through the IANA Transition," March 23, 2014, <http://circleid.com>.
60. In most countries hate speech is illegal, although not in the United States.
61. "SOPA/PIPA: Internet Blacklist Legislation," <https://eff.org>.
62. Jody Liddicoat and Avri Doria, "Human Rights and Internet Protocols: Comparing Processes and Principles," December 12, 2012, <http://internetsociety.org>.
63. Richard Hill, "The Internet as a Paradigm," April, 2013, <http://apig.ch/Internet%201-paradigm.doc>.
64. Just Net Coalition, "The Delhi Declaration," <http://justnetcoalition.org>.
65. This is not dissimilar to the original colonial narrative of bringing civilization to the natives.
66. Joseph Conrad, *Heart of Darkness*, <http://gutenberg.org>.
67. Full disclosure: both the authors were signatories to the letter signed by Indian civil society groups protesting the selection of the civil society co-chair.
68. "NETmundial: The Beginning of A Process," <http://netmundial.br/about>.
69. Richard Hill, "Quantitative Analysis of Contributions to NETMundial Meeting," March 20, 2014, <http://ip-watch.org>.
70. "NETmundial - Dilma Rousseff's Opening Speech," April 23, 2014, <http://netmundial.br>.
71. Julia Powles, "Big Business Was the Winner at NETmundial," April 28, 2014, <http://wired.co.uk>.
72. Milton Muller, "NETmundial Moves Net Governance Beyond WSIS," April 27, 2014, <http://internetgovernance.org>.
73. Google, Global Network Initiative, the State Department, all have been active in the civil society space. While a lot of the civil society activists are well meaning and are convinced of what they say, the corporate sector obviously wants to promote those sections that articulate positions that are similar to theirs. The multi-stakeholder model of all stakeholders on equal footing and decision making through consensus is one such position.



It is dangerous to confuse communications security with national security. In peacetime, far from ensuring security, secrecy only breeds suspicion and resentment, whereas more knowledge, whether freely given or surreptitiously obtained, can allay these suspicions.

—DAVID R. HEADRICK, *The Invisible Weapon*, 1991, 274

# Merging the Law of War with Criminal Law

## *France and the United States*

JEAN-CLAUDE PAYE

To support the “war on terrorism,” the concept of war has been introduced into the criminal code of all Western countries. This is the first step on the way to a merger between criminal law and the law of war. Massive spying by the secret services of a country on its citizens has today become the norm. The Snowden revelations on the operations of the NSA have only brought to light a widespread surveillance that is already legalized.

Despite the prominence given to the practices of U.S. intelligence agencies and the resulting indignation in France, the French parliament just adopted a military planning law that includes measures allowing practices similar to those of the NSA, specifically massive spying by intelligence agencies on citizens.

### **The U.S. Precedent**

The U.S. surveillance laws were the predecessor to European legislation. Section 215 of the Patriot Act, which was passed on October 26, 2001 to define the legislative framework for the war on terrorism, established that the collection and surveillance of communications could be made for a limited period of time without a warrant or court order.<sup>1</sup> These measures were passed under the form of an amendment to the FISA law, which was initially adopted in 1978 to provide a framework for spying on private communications.<sup>2</sup> Here also, it is on the basis of a law intended to “supervise intelligence activities” that espionage procedures were extended to all U.S. citizens.

The U.S. government’s viewpoint that the September 11 attacks were an act of war—and not just a crime—is based on a Congressional resolution of September 18, 2001, The Authorization for Use of Military Force, which gives special powers to the executive branch.<sup>3</sup> The interpretation of this resolution made by successive U.S. administrations is that the

---

JEAN-CLAUDE PAYE is a sociologist, and author of *L’Emprise de l’image: De Guantanamo à Tarnac* (Gap, France: Éditions Yves Michel, 2012).

This article is translated from the French by James Membrez.

state is at war, not against other nations, but against organizations that are not linked to a foreign government, or against private individuals. This interpretation redefines the concept of war. It takes on an asymmetrical character, a “fight to the death” between the world superpower and persons designated as enemies of the United States. This new concept, however, is not based on the existence of any real threat against the country. It is a pure product of the subjectivity of the government: the state of war exists simply because the United States says so.

These temporary measures in the Patriot Act opened the way to the current wide-scale surveillance of world communications by the United States, including communications inside the country. Surveillance has become unlimited in time due to the adoption of the “Patriot Act Improvement and Reauthorization Act of 2005,” which renewed all of the measures taken after the attacks and made permanent those that were previously temporary.<sup>4</sup>

#### **A Court Decision that Denies Its Unconstitutionality**

These measures, however, conflict with the Fourth Amendment to the U.S. Constitution that protects citizens from unreasonable searches and seizures. In order for the Fourth Amendment protection to be effective, a warrant is required, hence a justification for any data captures. Yet Judge William H. Pauley of the Federal Court of New York denied in his ruling of December 27, 2013, that there was any contradiction with the provisions of the Fourth Amendment, and stipulated that the NSA’s massive collection of telephone data was legal.<sup>5</sup> According to the judge, the fight against Al-Qaeda justified this widespread surveillance. Basing himself unconditionally on the testimony of high officials from the Obama Administration, he concluded that if the NSA had had recourse to its current program of electronic surveillance before September 11, 2001, the attacks would not have happened.

Judge Pauley cites approvingly the testimony of Deputy Directory of the FBI Sean Joyce before the House Permanent Select Committee on Intelligence. Joyce said: “Our mission is to stop terrorism, to prevent it. Not after the fact, to prevent it before it happens in the United States.... You ask ‘How can you put the value on an American life?’ And I can tell you, it’s priceless.”<sup>6</sup>

For the judge, the data collection is legal because of Section 215 of the Patriot Act. The role of the law is thus turned upside down. The Foreign Intelligence Surveillance Act (FISA), which provides an appearance of regulating intelligence agencies, is transformed into a means for providing a blank check for espionage against the U.S. population. This interpretation

of Section 215 first shifts the role of intelligence agencies from counterespionage to global surveillance of U.S. citizens, then proceeds to turn the function of the law upside down, from its traditional role of regulating action of the executive branch to legitimating absolute power.<sup>7</sup>

The ruling amalgamates the population and the government, thus removing any possibility of conflict between the rights of citizens and the interests of the state. To support the thesis that the defense of democratic rights can be left in the hands of the armed forces and intelligence services, the judge cites the 9/11 Commission Report: “The choice between liberty and security is a false one, as nothing is more apt to imperil civil liberties than the success of a terrorist attack on American soil.” Judge Pauley also asserts that each time a person uses a telephone, he or she “voluntarily” relinquishes his or her rights to privacy. He thus enjoins trust in the government without questioning its actions and assert that if the government attacks liberties, it must have good reasons for doing so.

### **Legal Uncertainty**

U.S. courts have reached different decisions on the issue of widespread surveillance. The ruling of the New York federal court is a reaction to a decision of December 16, 2013, by Richard Leon, judge of the U.S. District Court for the District of Columbia. In his decision, Judge Leon described as “almost Orwellian” the NSA’s massive spying operations, which involve the collection and storing of practically all the telephone call data, local or international, in the United States. He asserts: “I cannot imagine a more ‘indiscriminate’ and ‘arbitrary invasion’ than this systematic and high tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval.”<sup>8</sup>

Even more significantly, the judge rejected the justification of the war on terrorism invoked by the Obama and Bush administrations to legitimize all attacks against democratic rights. Judge Leon noted that the government did not cite “a single instance in which analysis of the NSA’s bulk metadata collection actually stopped an imminent attack.”

However, while the ruling stipulates that NSA practices “almost certainly” violate fundamental democratic rights, guaranteed by the Fourth Amendment, the judge has done nothing concretely to prevent the NSA’s unconstitutional spying. Thus, despite his conclusions, and “in light of the significant national security interests at stake in this case,” Judge Leon stayed his order of an injunction against NSA spying operations pending the government’s appeal. The appeals procedure could take years to reach the Supreme Court.

### **France: The Military Planning Law**

The latest French Military Planning Law, enacted on December 19, 2013, follows the trend begun in the United States. It exemplifies the evolution of law in the West that, while concentrating all power in the hands of the executive, puts the absence of law forward as the basis for reconstructing a new legal order.<sup>9</sup>

This year, the Military Planning Law goes beyond the context of defense to include “the fight against crime.” It includes various measures concerning both defense and national security. Article 20 extends the surveillance powers of French administrative authorities to “the prevention of crime.” Thus, by generalizing the tendency already initiated by the “anti-terrorist” fight, this article merges the law of war and criminal law. By aiming generically at “the prevention of crime,” this procedure will be applied not only to terrorism, but also to all offenses. By subjecting French citizens to a system of surveillance formerly reserved to agents of a foreign power, the law no longer separates the nation’s internal affairs from its external ones and no longer makes a distinction between criminal offense and management of hostility. This omnipresent process is not only identifiable within the country, but also at the level of international conflicts. France’s involvement in Libya makes no distinction between an act of war and a police function. War is no longer undertaken for defense or conquest, but to “protect a population from a tyrant.” It is the same with Syria. Following a chemical-weapons attack in Damascus attributed to Syrian government troops, President Hollande’s entourage, contemplating a limited intervention, emphasized “France’s great determination to react and not leave these crimes unpunished.”<sup>10</sup>

### **Merging the Military and the Penal**

In order to carry out this merger of the penal system and the military, the Military Planning Law supplants judicial power and concentrates power in the hands of the executive branch. Not only is the third branch totally circumvented, but the only a posteriori control institution, the National Commission for the Control of Security Interceptions (CNCIS—Commission nationale de contrôle des interceptions de sécurité) belongs to the executive and can only make “recommendations” to the prime minister.

The data collected includes telephone numbers, IP addresses, and the contact lists of callers, as well as data on real-time geolocation. Preliminary authorization from a specified judge or the CNCIS is necessary only in the last case.

Thus, Article 20 gives to the administration the right of real-time collection of information on the users of communication networks without recourse to a judge and without prior authorization from the administrative control body. Individually appointed agents from the ministries of Defense, Interior, the Economy, and the Budget (as well as “special representatives”) can now directly access the data. The law also includes the right to monitor all information and documents stored by the Internet host and not only technical data. Moreover, agencies are going to be able to demand data for a very wide range of reasons, particularly those provided for in Article 241-2 of the Internal Security Code, i.e., national security, prevention of terrorism, crime, and organized crime.

### **Seizure of Real-Time Data**

Article 20, which will enter into force in January 2015, allows the real-time capture of data on the basis of a simple administrative request (a “request to the network”) for information and documents handled by the latter and not just for the connection data of users. The direct collection of information will be made not only from Internet access providers and telecommunications companies, but also from all Internet hosts and providers of online services. No measure limits the volume of data collection. The latter could require the direct installation of signal or data capture devices at telecommunication companies and hosts. The inclusion of the terms “request to the network” means that the authorities hope to provide a legal framework for a direct interconnection. This law also transforms temporary measures into permanent ones.

The executive has always maintained that the new law does not include the content of the intercepted messages, but only the connection data. The French Data Protection Authority (CNIL—Commission nationale informatique et libertés), a control agency set up by the executive branch itself, has refuted this interpretation.

### **A Digital Military State**

Article 22 stipulates that ISPs, Internet hosts, and other operators whose infrastructure is considered of vital importance for the country must set up, at their expense, tools for “detecting events likely to affect the security of their information systems.” Since these tools would be used by certified third parties or by state agencies themselves, the law in fact authorizes the executive branch to install probes that it directly or indirectly controls.

The law does not define a cyberthreat and does not specify the competent authority to determine what constitutes an attack on “the Nation’s



military or economic capability, security, or survivability.” With such broad terminology, this legislation would make it possible, for example, to take action against a demonstration organized through social networks.

The policy of the United States is quite illuminating about the possibilities provided by the use of such concepts. The terms cyber-war and cyber-terrorism are central to the discourse of the U.S. government. The launching of the Iraq war already gave rise to an increase in alarmist declarations. Tom Ridge, Secretary of Homeland Security, announced that cyberterrorists are as dangerous as terrorists: “We will make no distinction between virtual and physical in this department,” he stated. Article 21 of the Military Planning Law authorizes such a lack of distinction between the real and the virtual. The threat exists merely because it is named as such.

Posing as a digital martial law in a permanent state of war, Article 22 allows the prime minister to cut off a server, reroute data along specific routes, or even force telecommunication firms to participate in counterattacks.

Article 23b of the law stipulates that agents of the national authority for the security of information systems can obtain from electronic communications operators the identity, postal address, and electronic address of users or holders of vulnerable, threatened, or attacked information systems. Thus, the law gives the Network and Information Security Agency (ANSSI—Agence nationale de sécurité des systèmes d’information) access to the files of subscribers. The agency will be able to obtain the coordinates for any Internet host, publisher, or Internet site subscriber “for the purpose of preventing attacks on automated processing systems.”

### **France at War Against Its Citizens?**

As a result of this law, the French are subject to procedures that formerly were used in surveillance of agents of an enemy power. This latest legislation, however, is only the most recent of a group of measures that began with the Internal Security Guidance and Planning Law (LOPSI—Loi d’orientation et de programmation de la sécurité intérieure), adopted on August 29, 2002.<sup>11</sup> This legislation already allowed remote access by the police to data retained by telecommunication companies and Internet service providers. In comparison to the 2001 Law on Everyday Security (LSQ—Loi sur la sécurité quotidienne), LOPSI makes it possible to evade the requirement of making a formal request to a telecommunication company. Formally, such a step requires a judicial authority to verify the legality of the request to the telecommunication operator. This requirement, which calls for a commission, includes an investigation procedure

and allows for possible recourse against the ordered measure. By abandoning the necessity of referring the request to a judicial authority, the 2002 law was an important step in moving police investigations in the direction of intelligence work. As for LOPSI 2, adopted on February 8, 2012, it permits a progressive screening of the Internet and legalizes the use of Trojan horses in private computers.<sup>12</sup>

The latest French law is part of a trend that assimilates a nation's internal security concerns with its external ones. By merging national defense and "crime prevention," it establishes general surveillance measures that apply procedures to citizens that were formerly used only for counterespionage. These procedures, in the past directed only at agents of an enemy power, are imposed on the population and the measures validating them are incorporated into the law, thereby obtaining the consent of citizens. The role of the law, then, is reversed. Instead of delimiting the action of public authority, it merely records the absence of limits on the exercise of executive power.

### **Citizen-Enemy of the State: Foundation of a New Legal Order**

In France, the concept of enemy is not yet, as in the United States, explicitly introduced into criminal law. However, it already functions as such in practice through legislation like LOPSI 1 and 2 and the military planning law.

In the United States, numerous surveillance measures established by the Patriot Act were at first provisional. Justified in the name of the existence of a state of war, they were passed with the intent of being applied for a limited period of time. It was only later, during their renewal, that they were adopted as measures with no temporal limit.

In France, the measures taken no longer refer to a state of emergency, but directly to a permanent state of war—although, unlike the United States, the concept of hostility is not yet formally part of criminal law.

In the United States, the inclusion of hostility into the internal legal order was first implemented through administrative acts justified in the name of a state of emergency. However, the Military Commissions Act of 2006 incorporates the concept of war into criminal law permanently.<sup>13</sup> It transforms this concept by allowing the president to designate U.S. citizens—as well as any citizen of a country which the United States is not at war with—as "enemy combatants."<sup>14</sup> This purely subjective law gives judicial prerogatives to the executive branch.

On October 28, 2009, President Obama signed the Military Commissions Act of 2009. The new law no longer speaks of "unlawful

enemy combatant,” but of “unprivileged enemy belligerent.” This expands the field of incrimination because it no longer focuses solely on combatants, but on “persons who are engaged in hostilities against the United States.”<sup>15</sup> The new definition makes it possible to go directly after not only persons captured in an armed engagement, but individuals who commit acts or voice words of solidarity towards those who oppose the United States armed forces or simply the war policies of the U.S. government.

## Notes

1. See 50 U.S.C. § 1861.
2. The 1978 Foreign Intelligence Surveillance Act establishes a special court charged with authorizing operations for surveillance of “agents of a foreign power.” This is a secret court composed of eleven judges designated by the Attorney General. See Electronic Privacy Information Center, “Foreign Intelligence Surveillance Act (FISA),” <http://epic.org>.
3. US Congress joint resolution of September 18, 2001, Authorization for Use of Military Force (AUMF), public law 107-40, 115 Stat. 224-5, <http://gpo.gov>.
4. H.R. 3199 (109th), <http://gpo.gov>.
5. Sari Horwitz, “NSA Collection of Phone Data is Lawful, Federal Judge Rules,” *Washington Post*, December 27, 2013, <http://washingtonpost.com>.
6. *ACLU vs James R. Clapper* 959 F.Supp.2d 724 (S.D.N.Y. 2013).
7. See, American Civil Liberties Union, “Reform the Patriot Act: Section 215,” <https://aclu.org>.
8. Ellen Nakashima and Ann E. Marimow, “Judge: NSA’s Collecting of Phone Records is Probably Unconstitutional,” *Washington Post*, December 16, 2013, <http://washingtonpost.com>.
9. LOI no. 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, <http://legifrance.gouv.fr>.
10. “Réforme pénale, Syrie, pression fiscal...Hollande s’explique dans ‘Le Monde’”, *Le Monde*, August 30, 2013, <http://lemonde.fr>.
11. Law no. 2002-1094 of August 29, 2002 on Internal Security Guidance and Planning, <http://legifrance.gouv.fr>.
12. Law no. 2001-1062 of November 15, 2001 on Everyday Security, <http://legifrance.gouv.fr>. The so-called LOPSI 2 law, the Law on Guidance and Planning for Achieving Internal Security (Loi d’orientation et de programmation pour la performance de la sécurité intérieure), follows up on LOPSI 1, <http://legifrance.gouv.fr>.
13. S. 3930 (109th), <http://govtrack.us>.
14. Jean-Claude Paye, “Enemy Combatant’ or Enemy of the Government?,” *Monthly Review* 59, no.4 (September 2007): 1-10.
15. Title XVIII of the “National Defense Authorization Act for Fiscal Year 2010,” <http://defense.gov>.



The secrecy system in this country is broken. No one is punished for using secrecy to conceal dangerous policies, lies, or crimes, yet concerned employees who wish to inform the American public about what the government is doing under their name are treated as spies. Our ‘accountability’ mechanisms are a one-sided secret court, which acts as a rubber stamp, and a Congressional ‘oversight’ committee, which has turned into the NSA’s public relations firm. Edward Snowden had no choice but to go to the press with information.

—DANIEL ELLSBERG, in “Edward Snowden to Join Daniel Ellsberg and Others in Freedom of the Press Foundations Board of Directors,” January 14, 2014, [pressfreedomfoundation.org](http://pressfreedomfoundation.org)

# The National Security State

## *The End of Separation of Powers*

MICHAEL E. TIGAR

On March 11, 2014, Senator Dianne Feinstein went to the U.S. Senate floor to announce that the CIA had sought to sabotage a Senate Intelligence Committee investigation of torture and unlawful detention. She set out in detail the ways in which the national security apparatus had frustrated meaningful oversight by the legislative branch of government.<sup>1</sup>

Already, government lawyers had convinced courts that there should be no *judicial* review of torture and unlawful detention. Such review, it was argued, was beyond the competence of judges, and the executive branch of government needed unfettered discretion to deal with national security threats.

The net result is that the CIA, the NSA, and all the other executive branch agencies engaged in surveillance, detention, torture, rendition of suspects, and even targeted killings by drone strike have claimed immunity from accountability by either of the two other branches—legislative and judicial. What they have done, why they have done it, and why their actions are or are not lawful—all of this has retreated behind a wall of secrecy. The claim made by government lawyers that there has been and will be legislative oversight turns out to be false.

In the November 2006 *Monthly Review*, I wrote an introduction to Jean-Claude Paye’s article “A Permanent State of Emergency.” It begins:

“The law is a mask that the state puts on when it wants to commit some indecency upon the oppressed.” I put these words into the mouth of a character in my play “Haymarket: Whose Name the Few Still Say With Tears.” ...In theory, the bourgeois democratic state, as defined in the American constitution, was to operate under two basic principles. The first of these was separation of powers. Legislative and executive action would be held to a standard of legality by the action of unelected and therefore presumably independent judges. The second principle, elaborated more fully in the Bill of Rights, is that certain invasions of

---

**MICHAEL E. TIGAR** is Emeritus Professor of Law at Duke University and Emeritus Professor of Law at Washington College of Law. He has been a lawyer working on social change issues for many years. His books include *Law and the Rise of Capitalism* (Monthly Review Press, second edition, 2000), *Fighting Injustice* (ABA Press, 2002), and *Thinking About Terrorism: The Threat to Civil Liberties in Times of National Emergency* (ABA Press, 2007).

individual personal liberty are forbidden, and that the judges will provide a remedy against those who commit such invasions.<sup>2</sup>

It is time to revisit these issues, and to see more fully the ways in which fundamental principles about restraints on state power are being and have been undermined. In this brief article, I can hope only to identify the questions that must be asked.<sup>3</sup>

### **Original Understanding—the First Promise**

The first promise was that executive power could be curbed by the other branches of government. In Federalist No. 68, James Madison spoke of the ways in which executive power would be controlled in the new U.S. Constitution: “unless these departments be so far connected and blended, as to give to each a constitutional control over the others, the degree of separation...essential to a free government can never in practice be duly maintained.”<sup>4</sup>

Patrick Henry, speaking against ratification of the U.S. Constitution, was pessimistic. He warned:

If your American chief be a man of ambition and abilities, how easy is it for him to render himself absolute! The army is in his hands, and if he be a man of address, it will be attached to him, and it will be the subject of long meditation with him to seize the first auspicious moment to accomplish his design, and, sir, will the American spirit solely relieve you when this happens? I would rather infinitely—and I am sure most of this Convention are of the same opinion—have a king, lords, and commons, than a government so replete with such insupportable evils. If we make a king we may prescribe the rules by which he shall rule his people, and interpose such checks as shall prevent him from infringing them; but the president, in the field, at the head of his army, can prescribe the terms on which he shall reign master, so far that it will puzzle any American ever to get his neck from under the galling yoke. I can not with patience think of this idea. If ever he violate the laws, one of two things will happen: he will come at the head of the army to carry everything before him, or he will give bail, or do what Mr. Chief Justice will order him.<sup>5</sup>

His words contain not only a warning but also a capsule version of 150 years of English history.<sup>6</sup> Those who disagreed with Patrick Henry did not doubt that the dangers of which he spoke were real. Rather, they believed that the Constitution they had drafted contained safeguards sufficient to prevent the harm of which he spoke.

The principle of separation of powers embodied in the Constitution—what is colloquially referred to as the system of “checks and balances”—was established by a series of revolutionary events

in the seventeenth century. In 1627, King Charles I needed funds to prosecute a war with France, and those who resisted financial impositions were both jailed by royal order, and denied judicial review of their detention. This led to debates in Parliament over the extent of unreviewable royal power, and specifically royal power with respect to national security and military matters. It was here that Lord Coke made his famous statement on limits to executive power: “God send me never to live under the law of conveniency or discretion.... Shall the soldier and the justice sit on one bench, the trumpet will not let the crier speak.... Where the common law can determine a thing, the martial law cannot.”

The struggle between Charles I and Parliament led eventually to the English Civil War. Charles surrendered in 1645, and was tried and executed for treason in 1649. In 1660, the monarchy was restored. Charles II became king, succeeded by his brother James II in 1685. James II apparently had not heeded the lessons of his father’s beheading, and was forced to abdicate in 1688. His abdication, and the installation of the Hanoverian monarch William III, has become referred to as “The Glorious Revolution.” Early in 1689, Parliament fixed the terms on which the monarchy was to survive, including the principle of separation of power and judicial review. In 1700, Parliament provided that judges were to be appointed for life, subject to removal only by consent of both houses of Parliament.

The U.S. Declaration of Independence, and the struggles that led to it, were in great measure based on the denial to the colonies of governance principles won by the seventeenth-century revolutionary struggles in England. Patrick Henry was wondering whether the new constitution would prove secure against a revival of claims to unreviewable power that Charles I had made.

### **Original Understanding—The Second Promise**

The Constitution’s second promise was that government would not use secrecy as a weapon against the governed. James Madison wrote: “Knowledge will forever govern ignorance. And a people who mean to be their own governor must arm themselves with the power that knowledge gives. A popular government without popular information or the means for acquiring it is but a prologue to a farce or tragedy or perhaps both.”<sup>7</sup> Lest we mistake his meaning, Madison also called out the “impious doctrine of the Old World that people were made for Kings and not Kings for people.”<sup>8</sup>

John Adams wrote: “And liberty can not be preserved without a general knowledge. But besides this they have a right, an undisputable, unalienable, indefeasible divine right to the most dreaded and most envied kind of knowledge, I mean of the characters and conduct of their rulers.”<sup>9</sup>

Those who wrote the Constitution provided that authors could enjoy copyright protection of their works. But they did not give government the power to use copyright to shield governmental information from public view.<sup>10</sup> That is, the government could not impose a form of literary or intellectual property on information in its possession, and by this means limit access to such information.<sup>11</sup>

These clues to original understanding of the Constitution permit an inference that governmental secrecy was to be narrowly defined in principle and sharply limited in practice. Thus, the second promise.

In the Presidential election of 1800, Thomas Jefferson defeated John Adams. Adams’s Federalist Party supporters viewed Jefferson and his allies as dangerous radicals, in part because of Jefferson’s known sympathy to the French Revolution. In order to maintain Federalist control of the federal judiciary, the lame-duck, Federalist-controlled Congress created new federal judicial posts. On March 3, 1801 (which, at this time, was the day before newly elected Presidents were inaugurated), Adams named William Marbury to a judgeship in the District of Columbia. Jefferson was sworn in the next day, and his Secretary of State, James Madison, refused to give Marbury the commission of office that Adams had signed.

Marbury sued Madison by filing an original action in the U.S. Supreme Court.<sup>12</sup> The Court issued an order that Madison should show cause why he should not be ordered—by a writ of mandamus—to deliver Marbury’s commission. The case attracted much attention, in part because Chief Justice Marshall had been appointed by Adams in January 1801, thus frustrating Jefferson’s intention to appoint his ally Spencer Roane to be Chief Justice.

Marshall’s opinion for the Court made three points. First, Marshall held that Marbury was entitled to receive his commission. Once the President had signed the commission, it became effective and no later act by the executive branch could undo what Adams had done.

Second, Marshall wrote of the right to redress:

The very essence of civil liberty consists in the right of every individual to claim the protection of the laws, whenever he receives an injury. One of the first duties of government is to afford that protection.... The government of the United States has been emphatically termed a government

of law and not of men. It will certainly cease to deserve this high appellation, if the laws furnish no remedy for the violation of a vested right.... If this obloquy is to be cast on the jurisprudence of our country, it must arise from the peculiar nature of this case.

Marshall noted that there might be cases not subject to judicial review, in a passage that has later been read more broadly than Marshall no doubt meant:

Is the act of delivering or withholding a commission to be considered a mere political act, belonging to the executive department alone, for the performance of which, entire confidence is placed by our constitution in the supreme executive.... By the Constitution of the United States, the President is invested with certain important political powers, in the exercise of which he is to use his own discretion, and is accountable only to his country in his political character.

These two statements of judicial duty and its limits are the first Supreme Court treatment of the separation of powers doctrine. Access to judicial review of a wrong suffered at the hands of government is a fundamental principle. There is an exception, for acts that the Constitution itself confides to Presidential power, and for which the President is nonetheless “accountable.” This accountability is in the President’s political capacity, that is by the force of public opinion, legislative control, and electoral politics. As we shall see, the national security state attacks both the idea of judicial review and that of popular limits on Presidential power.

The third point of Marshall’s opinion is the one for which *Marbury v. Madison* is most-often cited. Marshall held that the federal courts have the power to review acts of Congress and to declare them unconstitutional. Because the Constitution gives the Supreme Court an extensive power to decide appeals and a very limited power to hear original cases, the Judiciary Act provision giving the Court power to hear original petitions for mandamus was unconstitutional. If Marbury wanted his commission, he would have to bring suit in a lower court.

Jefferson was angered by the Court’s decision. Since the Court held it had no power to order the commission delivered, Jefferson thought Marshall should not have considered whether Marbury had been wronged. Jefferson also rebuked the Court for claiming the power to nullify Acts of Congress.

Marshall’s remark about unreviewable Presidential power was tested in three important judicial decisions during the next decade. In 1807, Jefferson ordered the U.S. Attorney for the District of Columbia to arrest Errick Bollman and Samuel Swartwout for treason, based on an Army



general's conclusion that the two men were plotting with Aaron Burr. Bollman and Swartwout sought habeas corpus. The circuit court for the District of Columbia rejected their petition, over the dissent of Chief Judge Cranch:

The Constitution was made for times of commotion. In the calm of peace and prosperity there is seldom great injustice. Dangerous precedents occur in dangerous times. It then becomes the duty of the judiciary calmly to poise the scales of justice, unmoved by the arm of power, undisturbed by the clamor of the multitude. . . . In cases of emergency it is for the executive department of the government to act upon its own responsibility, and to rely upon the necessity of the case for its justification; but this Court is bound by the law and the Constitution in all events.<sup>13</sup>

On appeal, in an opinion by Marshall, the Supreme Court upheld Cranch's position and ordered Bollman and Swartwout released.<sup>14</sup>

The second case was the treason prosecution of Aaron Burr.<sup>15</sup> Jefferson had orchestrated the case against Burr. At that time, Supreme Court Justices sat "on circuit" as trial judges; Marshall was the judge before whom Burr was tried in Virginia. The partisans of Jefferson and of Burr railed against one another. Jefferson and his allies attacked Marshall's handling of the case. In this political turmoil, which left Burr acquitted but nonetheless dishonored, Marshall's observations on issues in the case remain relevant.

Marshall discussed the attacks on his own conduct, and the careless use of the "treason" label for political purposes. As Robert Ferguson relates: he had not enjoyed finding himself "in a disagreeable situation." What person would? "No man is desirous of becoming the object of calumny," he reminded those who had abused him, including the President of the United States. "No man, might he let the bitter cup pass from him without self reproach, would drain it to the bottom."<sup>16</sup>

This observation on his own situation led Marshall to reflect on the meaning of treason: "As this is the most atrocious offence which can be committed against the political body, so it is the charge which is most capable of being employed as the instrument of those malignant and vindictive passions which may rage in the bosoms of contending powers struggling for power." Marshall noted that the Framers had "refused to trust the national legislature with the definition," fixing it instead in the body of the Constitution.<sup>17</sup>

Marshall's second memorable ruling was directly relevant to separation of powers. Burr sought to compel Jefferson to produce a letter that General Wilkinson had written to him in 1806. The prosecution resisted. Marshall held that the letter must be produced. He held

that the President was subject to judicial process.<sup>18</sup> “The propriety of introducing any paper into a case, as testimony, must depend on the character of the paper, not the character of the person who holds it,” he wrote. Indeed, the President might be compelled to appear personally, unless he could show that his duties interfered with his attending.

A third important separation of powers ruling was *Gilchrist v. Collector of Charleston*.<sup>19</sup> In 1807, Congress—seeking to retaliate against British and French interests—authorized an embargo on foreign seaborne commerce. In 1808, amending legislation authorized the customs collector at any port to detain any vessel suspected of engaging in foreign commerce. The customs collector at Charleston, South Carolina—a federal official—denied a ship belonging to Adam Gilchrist clearance to leave the port, suspecting that Gilchrist was not engaged in coastwise domestic shipping but rather foreign travel.

Justice William Johnson, sitting as circuit judge, heard evidence and ordered the collector to let Gilchrist’s ship leave the port. Johnson held that despite the broad statutory language, federal courts had the power to control actions of the executive branch. Jefferson, who had appointed Johnson to the Supreme Court, was enraged at the decision. He directed Attorney General Caesar Rodney to write a public letter attacking Johnson’s ruling. Johnson responded to the letter in a second published opinion. Johnson said he was reluctant to be drawn into public controversy, but felt compelled to do so: “But when a bias is attempted to be given to public opinion by the overbearing influence of high office, and the reputation of ability and information, the ground is changed; and to be silent could only result from being borne down by weight of reasoning or awed by power.”<sup>20</sup>

Johnson went on to repeat his insistence on judicial power to control executive action.

### **The Promises Constrained**

No one could sensibly claim that these principles of transparency and accountability were uniformly applied in the decades after they were first formulated. These were promises that the new regime made to the people generally. As promises, they were hedged about with limitations and conditions at the outset, and then in practice proved to be difficult to enforce. These were promises fashioned as instruments of bourgeois state power, setting out an idea that the state would stand as neutral guardian of principle, when in fact it was prepared to act as an instrument of social control.

But while the promises could never be wholly realized, keeping them gave state power its perceived legitimacy. That, in general terms, is the way of parliamentary democracy. Organs of state power remain open to influence; a set of declared rights is more or less guaranteed.

It is not, therefore, surprising that Chief Justice Marshall himself wrote the Supreme Court opinions that denied judicial review to Native Americans and African slaves. After all, the Constitution itself accepted the institution of slavery and provided that: “Representatives and direct Taxes shall be apportioned among the several States which may be included within this Union, according to their respective Numbers, which shall be determined by adding to the whole Number of free Persons, including those bound to Service for a Term of Years, and excluding Indians not taxed, three fifths of all other Persons.”<sup>21</sup>

That is, a slave was three-fifths of a person for the purpose of allocating Congressional seats, though without a vote or any of the political rights defined in the Constitution. Native Americans did not exist for purposes of taxes and representation, although the Congress would certainly legislate as to their status. In the early nineteenth century, Native Americans sought to assert their rights. As I wrote in *Law & the Rise of Capitalism*:

The Cherokee Nation of Georgia adopted a written constitution and asserted sovereignty over its land. The Georgia legislature responded by declaring Cherokee laws and customs void and opening Cherokee land to settlement. The federal Congress, at the urging of President Andrew Jackson, passed legislation seeking to compel Native Americans to give up and move westward. Georgia authorities arrested, tried, and hanged a Cherokee for an offense allegedly committed on Cherokee territory.

The Cherokee Nation sought relief in the courts. They were, after all, a nation. They sought to restrain the enforcement of Georgia laws which “go directly to annihilate the Cherokees as a political society, and to seize, for the use of Georgia, the lands of the nation which have been assured to them by the United States in solemn treaties repeatedly made and still in force.” The Cherokees’ lawyer invoked the Supreme Court’s power, saying that the lawsuit was between a foreign nation—the Cherokee—and the state of Georgia. Under the United States Constitution, the Supreme Court could exercise its original jurisdiction over such a lawsuit without waiting for lower courts to decide it and then hearing the case on appeal.

Chief Justice Marshall looked to the constitutional grant to Congress of the power to regulate commerce with “foreign nations, and among the several states, and with the Indian tribes.” He found the Cherokee to be “a domestic, dependent nation” that was “in a state of pupilage,” like “that of a ward to his guardian.” It was not, he said, for the Court a true

“foreign nation.” Thus, the Cherokee Nation had no legal existence. It could not even come to a federal court to vindicate its treaty rights.

The Supreme Court decided *Cherokee Nation v. Georgia* in 1830, over the dissents of Justices Story and Thompson. Two years later, in *Worcester v. Georgia*, Chief Justice Marshall retreated a bit, and held that Georgia did not have the right to regulate activities on the Cherokee lands. He did not reach this result by recognizing the position of the Cherokee Nation, but by denying the right of a state such as Georgia to interfere in matters that are essentially federal. That is, the national government had the constitutional power to deal with Native Americans and the states had only a limited role to play.<sup>22</sup>

Marshall spoke for the Supreme Court on the issue of slavery in an 1825 case, *The Antelope*.<sup>23</sup> The Constitution had forbidden Congress to regulate importation of “persons” until 1808. In a statute that took effect January 1, 1808, the Congress prohibited importation of slaves. Nonetheless, the slave trade continued, and in 1820, a U.S. coast guard vessel boarded and seized a ship, *The Antelope*, that was carrying 225 African slaves. *The Antelope* was taken into port on suspicion that the slaves were destined to be imported into the United States.

Here was a chance for Marshall, who acknowledged that slavery was “contrary to the laws of nature,” to translate this sense of injustice into a judicial command. However, he noted that “Christian and civilized” nations still engaged in the slave trade and that it could not therefore be said to be unlawful; the slaves were not to be set free but rather returned to their owners. Marshall’s failure to find controlling international law is the more surprising because the United States had agreed in the 1814 Treaty of Ghent to seek an end to the international slave trade.<sup>24</sup>

For Marshall and his colleagues on the Supreme Court, Native Americans did not exist as holders or bearers of rights, and the status of slavery was not an issue that the law could address. To complete the story, one must note the Court’s 1841 decision in *The Amistad*.<sup>25</sup> Between 1825 and 1841, treaties and customary international law had shifted the legal landscape. *The Amistad* was a Spanish ship carrying forty-nine slaves. The slaves took command of the ship, which eventually anchored off Long Island. The legal proceedings eventually reached the Supreme Court. The Spanish and British governments tried to exercise influence on the case: the British said that the capture of the slaves in Africa violated a treaty between Britain and Spain. Spain said the slaves were property and should be returned. The Supreme Court argument, led by John Quincy Adams, stressed that judicial review and not executive branch concerns should be the guiding principle of decision.

On March 9, 1841, Justice Story delivered the Supreme Court's opinion holding that the slaves must be freed.

Any hope that was kindled by the *Amistad* decision was extinguished by the *Dred Scott* decision in 1857.<sup>26</sup> The Supreme Court's decision that *Dred Scott* was not entitled to freedom from slavery despite having been taken into free territory was based upon an assertion that echoed the rationale of *Cherokee Nation v. Georgia*. African slaves and their descendants could not be "citizens" of any state and were therefore not entitled to be heard in federal court. They were, the Court said, "beings of an inferior order, and altogether unfit to associate with the white race, either in social or political relations, and so far inferior that they had no rights which the white man was bound to respect." That is, it was not only the political institution of slavery that forbade judicial review, but a theory that those of African descent were inferior beings destined to be ruled without voice as to their condition.

Chief Justice Taney, who wrote the majority opinion, and President James Buchanan, who was given advance notice of what the Court would do, thought that the *Dred Scott* decision would end the controversy about slavery. Of course, it did nothing of the kind, but rather made a military solution inevitable.

Thus, in 1857, for white male citizens, judicial review of governmental action was presumptively available. However, judicial review stopped short when a litigant challenged a system of social relations. The conquest and subjugation of Native Americans was a fundamental tenet of British, French, Spanish, and then U.S. occupation of the Eastern seaboard and then of Westward expansion. By definition Native Americans were not to be considered as bearers of rights that could be enforced against the state. And Taney's statement came at the end of a long pseudo-historical analysis that justified the institution of slavery as a part of the social fabric.

### **The Separation of Powers After 1857**

The Civil War amendments to the Constitution abolished slavery and provided for equal protection of the laws. It would be nearly a century before the promise of those amendments began to be fulfilled by the Supreme Court. For African-Americans, the Court's ruling in *Brown v. Board of Education* recognized the promise that the 14th Amendment equal protection clause indisputably made.<sup>27</sup>

The *Marbury-Gilchrist-Burr* model, as limited in *Cherokee Nation* and *Dred Scott*, posits a right of access to review of governmental action. Presumptively, the courts will provide review. In a narrow class of cases,

that review must be obtained through a political process. Nobody can rationally claim that either of these avenues of redress is efficient. Most of the significant cases about “rights” have been brought and litigated by labor, civil rights, and civil liberties organizations—the cost of what passes for justice is too great for most people. Of course, those who wind up in court testing their rights as criminal defendants will have counsel provided but the deficiencies of that system are well-known. The electoral political process is dominated by money, and is in many ways impossibly corrupt.

The point, however, is that the state has assiduously maintained the fiction that both of these avenues of redress are in fact viable. In order for this fiction to have any semblance of credibility, the institutions of redress must be seen to have some utility. The lawyer for the oppressed points to the promises and principles in the legal ideology of the dominant class, and argues for their application in ways that may contradict the interests of that class. Significant victories have been won for workers, women, people of color, political dissidents, and gay and lesbian people—in the judicial, executive, and legislative arenas. The courtroom battles for these rights produced significant victories in the 1950s, ‘60s, and ‘70s, and helped to empower movements for social change.

In the midst of these battles, there were disturbing signs that Patrick Henry’s forebodings—a President at the head of an army, and therefore indisposed to heed the commands of a Chief Justice—would be realized. And what if a President’s refusal to “do what Mr. Chief Justice will order him” was a problem compounded by Mr. Chief Justice’s timidity and moral obliquity? That is, what if Mr. Chief Justice—in the pattern of Marshall in *Cherokee Nation* or Taney in *Dred Scott*—were to acquiesce in declaring a “no law” zone because of the character of a claim or of the claimant? In such a case, the structure of separation of powers might crumble, not by conquest—but by surrender.

By way of example, the Supreme Court upheld the internment of Japanese-Americans during the Second World War, yielding to an exercise of Presidential power that was later held to have been improper and based upon false assumptions.<sup>28</sup> Some of the Court’s decisions on freedom of expression and association during the Cold War period failed to respect freedoms of speech and association. Yet, there were bright spots, as when the Supreme Court upheld the academic freedom of *Monthly Review* editor Paul Sweezy.<sup>29</sup>

The years since September 11, 2001, have witnessed a significant shift in the role of the executive and judicial branches. In the militarized

national security state, the dismantling of the constitutional separation of powers has largely come to pass. We can see how this has happened, as a matter of state power and legal ideology.

Two legal devices have been deployed to shut off accountability for governmental wrongdoing. The first of these is a judicially created doctrine of non-decision—the “political question doctrine.” The second is the state secrets privilege, the invocation of which forestalls all accountability because the rationale and details of government conduct are hidden from public view. Let us examine these in turn.

### Political Question

The political question doctrine is a device by which a federal court decides that it cannot hear and decide a matter because it lacks subject matter jurisdiction—jurisdiction *ratione materiae*—to give a decision. The matter is said to lie outside the bounds of “cases” and “controversy” over which Article 3 of the Constitution bestows judicial power. In a 1962 decision, the Supreme Court—in an opinion by Justice William Brennan—gave a broad reading to the doctrine:

Prominent on the surface of any case held to involve a political question is found a textually demonstrable constitutional commitment of the issue to a coordinate political department; or a lack of judicially discoverable and manageable standards for resolving it; or the impossibility of deciding without an initial policy determination of a kind clearly for non judicial discretion; or the impossibility of a court’s undertaking independent resolution without expressing lack of the respect due coordinate branches of government; or an unusual need for unquestioning adherence to a political decision already made; or the potentiality of embarrassment from multifarious pronouncements by various departments on one question.<sup>30</sup>

In setting out this general view, Justice Brennan referred to cases arising in times of domestic and foreign conflict, and to Marshall’s opinion for the Court in *Cherokee Nation*. This passage is remarkable for its generality. Although it reflects analysis of the Court’s precedents, it can easily be invoked as a free-wheeling, unprincipled, and utterly discretionary refusal to decide. Constitutional scholars soon began to point out this danger. During the Vietnam War, lawyers and legal scholars—with the concurrence of some political figures—attacked the war as a violation of domestic and international law. Some who refused to serve in the military invoked these legal principles in defense of defiance. The government pleaded the political question doctrine and courts refused to confront the issue.<sup>31</sup> One might say, in defense of these

decisions, that review of the decisions to commit troops in Vietnam would indeed involve the courts in a set of factual and legal inquiries that could plausibly be termed outside judicial competence.

Today, however, the political question doctrine is deployed in situations where that defense of its use cannot plausibly be advanced. Take the case of Jose Padilla. Padilla was arrested in Chicago on May 8, 2002. He is a U.S. citizen, but had been designated an enemy combatant by the Bush administration under the national security legislation enacted in the wake of September 11, 2001. The government then transferred Padilla to a military prison where he was tortured. His mother, Estela Lebron, sued federal officials for damages and to forbid Padilla's future treatment as an enemy combatant. The federal court of appeals held that the law did not provide a remedy for the wrongs done to Padilla.<sup>32</sup>

The court of appeals began by noting that Congress had authorized the use of military force against Al-Qaeda, and that successive administrations have said that the United States "continue[s] to fight a war of self-defense against an enemy that attacked us." With this beginning, the court reviewed the precedents on political questions and held that it would not recognize Padilla's legal claim for the injury done to him.

The court's analysis is constitutional nonsense. "War" and "declaration of war" are concepts with a settled meaning in international law. Congress did not declare a war. It authorized the use of military force under certain circumstances. It did so in haste, and to see its action as an open-ended authorization to engage in military action wherever in the world the President might decide ignores the constitutional limits on Presidential and Congressional power. Even if this view of the matter is utterly wrong, and even if one believes that the ongoing U.S. military presence in over a hundred countries is consistent with constitutional governance, and that classification of "enemy combatants" is proper, Padilla's treatment raises an issue on which courts are not only competent but uniquely situated to make a decision.

Padilla presented a simple claim: Was he the victim of torture? Torture is always and in every circumstance unlawful. It is forbidden by treaty, customary international law, and federal statute. The backdrop against which torture occurs, and the motives of those who do it and authorize it, are irrelevant. Thus, the court's entire disquisition on the war-making power is irrelevant. The court's syllogism is (a) we are at war with Al-Qaeda, (b) Padilla is a member of Al-Qaeda, (c) therefore he has no enforceable right not to be tortured. This is the syllogism of *Cherokee Nation* and *Dred Scott*. It identifies a group or class of people excluded



from judicial review. The court's analysis goes even further, for it places this no-law zone in the midst of an entire sphere of governmental activity that is held to be unexaminable and unreviewable.

Indeed, the Supreme Court long ago recognized that a violation of international law, even by military forces in an arena of conflict, is subject to judicial examination. In a 1900 case, *The Paquete Habana*, the Court held that two fishing vessels that the Navy had seized during the Spanish-American war were exempt from seizure under international law and should be returned to their owners.<sup>33</sup> The Court reaffirmed that customary international law was part of the Constitution, laws and treaties mentioned in articles 3 and 6 of the constitution. This customary law, the Court said, would be determined by consulting the recognized sources of international law, which include state practice and the opinion of jurists.

Consider then, another case involving a U.S. citizen, Anwar al-Aulaqi. He was born in the United States to Yemeni parents, spent most of his formative years in Yemen, and returned to the United States to go to college, staying in the country for over a decade, until 2002. He then returned to Yemen and was active in what has been termed an "anti-Western jihadist movement." He wrote and spoke against U.S. policies and actions, and supported the use of violence. In 2010, the CIA had listed al-Aulaqi as the potential target of a lethal drone strike—that is, the U.S. government had decided to use lethal force against a U.S. citizen without a judicial trial.

Anwar al-Aulaqi's father brought a suit to enjoin the government from killing his son. It hardly requires analysis of all the reasons for U.S. military activity to decide this issue. Yet, the federal court held that the case presented a political question and was not justiciable.<sup>34</sup> That decision was issued December 7, 2010. On September 30, 2011, a U.S. drone strike killed Anwar al-Aulaqi. On October 11, 2011, another drone strike killed Aulqi's sixteen-year-old son Abdulrahman and five other civilians. Attorney General Holder admitted that Abdulrahman had not been "specifically targeted," which is as close to admitting that his killing was an error as the government is likely to get.<sup>35</sup> After the killings, families of the victims sued U.S. government officials, and a federal judge dismissed that suit as well.<sup>36</sup>

In another case, the family of Chilean General Rene Schneider sued Henry Kissinger and other officials for their complicity in the 1970 kidnapping and assassination of General Schneider. The kidnappers' goal, shared by the United States, was to destabilize the government of Salvador Allende. The court of appeals held that the case was barred

by the political question doctrine.<sup>37</sup> In the Schneider case, there had not been any Congressional authorization, or even official Presidential pronouncement, authorizing invading the Chilean territory to kill one of its officials. Thus, there could not be any constitutional commitment of a decision to the executive branch. There was hardly any factual complexity, as State Department cable traffic that had been released under the Freedom of Information Act amply revealed Kissinger's role, and witnesses to events had been interviewed. Rather, "political question" was simply a label for another no-law zone in the U.S. empire.

These cases illustrate the national security state pushing to create and enlarge no-law zones based on the existence of military action, and/or the character of the person who claims that his or her rights have been invaded. The first of these justifications reminds us of what Patrick Henry said. The second recalls Cherokee Nation and Dred Scott.

A judicial decision from 1980 presents an interesting parallel. On September 21, 1976, agents of the Pinochet regime assassinated Orlando Letelier and Ronni Moffitt in Washington, D.C., with a car bomb. Letelier had been an official of the Salvador Allende government in Chile, and—in exile after the 1973 military coup—was a forceful and effective opponent of the Pinochet junta. My law firm sued the Chilean junta on behalf of the Letelier and Moffitt families. The junta claimed to be immune from suit, and that the killings were a discretionary political act. The judge rejected this claim: "Whatever policy options may exist for a foreign country, it has no 'discretion' to perpetrate conduct designed to result in the assassination of an individual or individuals, action that is clearly contrary to the precepts of humanity as recognized in both national and international law."<sup>38</sup>

For U.S. policymakers, therefore, the rule of law is that *other* countries are not free to violate sovereignty and territorial integrity to kill and maim.

Perhaps open spaces remain within the legal ideology of the national security state. The U.S. Court of Appeals for the District of Columbia Circuit has held that there is judicial power to review the conditions of confinement at Guantanamo, though the administration is challenging that ruling.<sup>39</sup> A federal district judge has held the NSA surveillance program unlawful; that decision is disagreed with by another federal court and is also being appealed.<sup>40</sup> The revelations about NSA surveillance recall another separation of powers concern that is reflected in the Constitution. I wrote in *Thinking About Terrorism*:

During the colonial period, tax evasion was a popular pastime. The Boston Tea Party was only one dramatic example. In order to enforce taxes, the British authorities employed writs of assistance, which were

orders obtained from complaisant judges authorizing customs and revenue officers to enter premises where goods were stored and search at large and at will.

Colonial resistance to the writs of assistance was widespread. The most famous challenges were those mounted by Massachusetts lawyers led by John Adams and James Otis. On the Boston Common in 1761, James Otis delivered a famous denunciation of the writs. Of that speech John Adams later wrote “then and there the child Independence was born.”

In England at about the same time arose two cases involving the English radical John Wilkes. Lord Halifax, then Secretary of State, issued a paper authorizing royal officers to search Wilkes’ premises and papers for evidence of crime, including sedition—which was simply speech criticizing the Crown. Wilkes was arrested and thrown into the Tower of London—and expelled from Parliament. He sued and won. Two cases, *Wilkes v. Wood* in 1763, and *Entick v. Carrington* in 1765, decided that the executive branch of government had no authority to issue warrants and that Halifax should pay damages. Every lawyer who participated in writing the Constitution and its Bill of Rights was familiar with the writs of assistance struggle and with *Entick* and *Wilkes*. They wrote the fourth amendment with those cases in mind.<sup>41</sup>

Yet, today the national security state conducts surveillance of billions of people, intercepting their emails, telephone calls, and correspondence, all without judicial approval.<sup>42</sup> When Edward Snowden revealed this illegal activity, government officials were quick to denounce him as a “traitor,” bringing to mind Marshall’s statement that the careless application of this label contradicts the constitutional text.

### **Hypocrisy**

The United States has supported, or at least acquiesced in, creation of international criminal courts for Yugoslavia, Rwanda, Cambodia, and Sierra Leone. These courts have tried hundreds of defendants—including heads of state and other government officials—for torture, kidnapping, unlawful detention and homicide. It could not plausibly be argued, and the United States has not argued, that trying these cases presents political questions that are beyond the institutional competence of courts, nor that the inevitably political character of these cases, nor the political motivations of the accused, makes the cases inappropriate for judicial resolution. The concept of “justiciability” around which the political question issue is debated in U.S. federal courts, is not some uniquely fragile idea of judging found only in the U.S. Constitution. This concept was meant by the Framers to carry the full weight of judicial responsibility that the seventeenth-century English history had shown to be necessary and appropriate. That

robust idea of judicial duty was, indeed, the intellectual and ideological foundation of the Nuremburg tribunals, source of much law and learning.

One must also note in this connection that while the United States participated in the discussions leading to the creation of the International Criminal Court, it has not ratified the resulting treaty. Rather, the United States has taken strong steps to make sure that no U.S. national will be tried in that court. The American Service-Members Protection Act, passed in 2002, endorses the U.S. refusal to join the International Criminal Court, authorizes use of force to free any United States “or allied” person from the control of the International Criminal Court, prohibits state and local governments from cooperating with the Court, and forbids military aid to any country that are parties to the treaty establishing the Court.<sup>43</sup> This last prohibition has been modified to allow continued aid to NATO allies and other significant military partners such as Taiwan. In short, the United States takes the position that judicial review of its actions cannot take place in any tribunal anywhere.

I am not, by this reference, uncritically endorsing the procedures of the international criminal tribunals. They were, as Diane Johnstone has written of the Yugoslavia tribunal, “set up by the Great Powers, using the UN Security Council, in order to judge the citizens of smaller, weaker countries which were excluded from making the rules or interpreting them.”<sup>44</sup> My point, rather, is that the inconsistency of position shown by U.S. action with respect to these courts underscores the hypocrisy of political question arguments advanced by lawyers for the United States in the U.S. Court system. More seriously, these arguments represent a claim of imperial power. The United States announces, devises, and enforces rules, invoking the rhetoric of human rights and humanitarian law. It does not acknowledge a duty to obey rules.

### **State Secrets**

*United States v. Reynolds* was a suit brought by the widows of three civilian observers aboard an Air Force plane that crashed in 1948.<sup>45</sup> The U.S. government resisted the suit, saying that inquiry into the reasons for the crash would require disclosure of state secrets. The Supreme Court agreed that such disclosure might require dismissal of the suit, but cautioned that “judicial control over the evidence in a case cannot be abdicated to the caprice of executive officers.”

Sixty years later, the flight records were unsealed, revealing that the crash was caused by a routine maintenance failure and that the government’s invocation of “secrecy” was baseless and mendacious.<sup>46</sup>

Senator Feinstein's speech on March 11, 2014, tells a tale of executive officer caprice. One is reminded of Justice Frankfurter's characterization of a similar charade, when he observed that a theory of privilege that immunized an executive officer from accountability reflected "a fox-hunting theory of justice that ought to make Bentham's skeleton rattle."<sup>47</sup> Feinstein began by noting that the Senate was investigating torture and unlawful renditions, a subject on which the CIA itself had expressed concern and conducted an internal inquiry. The Senate Intelligence Committee, which conducts much of its oversight work in secret, began its investigation by seeking documents. The CIA hedged and demanded that the relevant documents not be delivered to Congressional premises, but to an offsite secure facility in effect controlled by the CIA. The Senate agreed. The CIA delivered 6.2 million pages of badly indexed documents—a "document dump," as Senator Feinstein termed it. Senate staff members were forced to look, first, for the haystacks in this field of material, and then for the needles they might contain.

Throughout this process the CIA interfered with access to the documents, removed relevant materials from the review process, and then threatened Senate staff members with criminal prosecution for allegedly handling the documents in ways that compromised national security. As Senator Feinstein pointed out, the criminal referral was made by a lawyer who had himself been responsible for the illegal actions the Committee was investigating, and was therefore an effort to invoke secrecy for his own protection from accountability.

The Feinstein revelations are just one example of the way that secrecy is invoked by the national security state. Of course, there are reasons why some governmental activity is shielded from view. A grand jury meets in secret, in some measure to protect the reputations of people, and legitimately to preserve law enforcement information. However, the state secrets privilege invoked by the national security state sweeps far broader and bespeaks a particular rationale.

Many evidentiary privileges are designed to protect personal autonomy. The right to consult a lawyer, a doctor, or a religious advisor in private is an essential part of personal liberty. The rights to live, sleep, talk, write, join an organization, or have sexual encounters without government intrusion are also protected to different extents and in different ways by the Constitution.

The state secrets privilege is different because it erects a barrier between the state and the governed. It blocks the governed from access to information about the decisions that affect their lives. The privilege

as invoked by the national security state is qualitatively different from the law enforcement privilege that attaches to grand jury proceedings. That privilege shields information about particular events and persons, and does not draw the curtain of secrecy over an entire governmental process. The mode by which grand jurors are selected, and the legal rules that control their activities, remain open to examination. The grand jury's procedures can be challenged by someone subject to subpoena, and an indictment that the grand jury returns may be dismissed if the grand jury has been used in an improper way.<sup>48</sup>

The privilege as viewed by the national security state blocks access to entire sets of government decisions, and to the justifications for those decisions. That is, government claims the right to hide what it does and the reasons for what it does.

Consider this case. The *New York Times* and others asked the Department of Justice for documents relating to drone strikes. They were seeking material that would reflect government consideration of the legality or illegality of targeted killings. That is, they wanted to know the policy reasons, if any, for these actions. One evident purpose of their inquiry was to foster public discussion of the drone program, that is, accountability of the President in his political capacity. The Department of Justice refused to produce responsive documents. The *Times* and other requesters brought suit in federal court.

Judge McMahon began by noting that her published opinion would not disclose the entire basis of her ruling. That is, the review of secrecy would be done, at least in part, in secrecy. She wrote:

This opinion will deal only with matters that have been disclosed on the public record. The Government has submitted material to the Court *ex parte* and for *in camera* review. It is necessary to discuss certain issues relating to this classified material in order to complete the reasoning that underlies this opinion. That discussion is the subject of a separate, classified Appendix to this opinion, which is being filed under seal and is not available to Plaintiffs' counsel. In crafting that Appendix, the Court has done its best to anticipate the arguments that Plaintiffs would have made in response to the Government's classified arguments.<sup>49</sup>

Judge McMahon then summarized her rationale for denying disclosure of the documents, even as she wrote at length about the slender justifications for targeted killings:

The FOIA requests here in issue implicate serious issues about the limits on the power of the Executive Branch under the Constitution and laws of the United States, and about whether we are indeed a nation of laws, not of

men. The Administration has engaged in public discussion of the legality of targeted killing, even of citizens, but in cryptic and imprecise ways, generally without citing to any statute or court decision that justifies its conclusions. More fulsome disclosure of the legal reasoning on which the Administration relies to justify the targeted killing of individuals, including United States citizens, far from any recognizable “hot” field of battle, would allow for intelligent discussion and assessment of a tactic that (like torture before it) remains hotly debated. It might also help the public understand the scope of the ill-defined yet vast and seemingly ever-growing exercise in which we have been engaged for well over a decade, at great cost in lives, treasure, and (at least in the minds of some) personal liberty.

However, this Court is constrained by law, and under the law, I can only conclude that the Government has not violated FOIA by refusing to turn over the documents sought in the FOIA requests, and so cannot be compelled by this court of law to explain in detail the reasons why its actions do not violate the Constitution and laws of the United States. The Alice-in-Wonderland nature of this pronouncement is not lost on me; but after careful and extensive consideration, I find myself stuck in a paradoxical situation in which I cannot solve a problem because of contradictory constraints and rules—a veritable Catch-22. I can find no way around the thicket of laws and precedents that effectively allow the Executive Branch of our Government to proclaim as perfectly lawful certain actions that seem on their face incompatible with our Constitution and laws, while keeping the reasons for its conclusion a secret. But under the law as I understand it to have developed, the Government’s motion for summary judgment must be granted, and the cross-motions by the ACLU and the *Times* denied, except in one limited respect.

These are paragraphs that conjure Patrick Henry’s forebodings and Chief Justice Marshall’s reassuring words. The “American chief” has arrived, not at the head of his army but in command of missiles that kill persons identified in secret by secret procedures and secret principles. Mr. Chief Justice is represented by his surrogate, an Article 3 judge. The judge quotes the constitutional idea that the Constitution and laws are supreme, and then holds herself to be without power even to ask the President what he is doing and why—let alone to see if it is lawful.<sup>50</sup> Only the courage of “leakers” who are then calumniated and targeted for prosecution has given us what we know about what the national security state is doing.

On April 21, 2014, the United States Court of Appeals for the Second Circuit reversed this decision, and held that the government must release some information about the use of drone strikes to kill Anwar Al-Aulaqi and others.<sup>51</sup> The court of appeals decision remains in conflict with other decisions by other courts, so the issue is not

yet resolved.<sup>52</sup> Indeed, the rationale of decisions compelling disclosure may well create more problems than it solves. The court of appeals held that documents containing legal justification for drone strikes must be released because government officials had made public statements revealing the alleged legal basis for such strikes. So the message is not that government conduct just be open to inquiry, but rather that government officials must maintain absolute secrecy from the outset in order to avoid disclosure.

This is a testing time for federal judges. There are dozens of lawsuits raising the issues of transparency, accountability, and legality.<sup>53</sup>

Even if the official memoranda sought in the *New York Times* suit are eventually revealed, the larger issue remains. On Sunday, May 11, 2014, Senator Rand Paul wrote in the *New York Times* that the Obama administration has refused to release the entire collection of documents concerning the alleged legality of drone strikes. Paul and others had requested release in order to assess the nomination of Harvard Law professor David Barron to the U.S. Court of Appeals for the First Circuit. While at the Justice Department, Barron had advised the administration that the drone killing of U.S. citizens was lawful. As Paul noted: “I believe that killing an American citizen without a trial is an extraordinary concept and deserves serious debate. I can’t imagine appointing someone to the federal bench, one level below the Supreme Court, without fully understanding that person’s views concerning the extrajudicial killing of American citizens. But President Obama is seeking to do just that.”<sup>54</sup>

### Historical Context

As the Second World War came to an end, U.S. military, diplomatic, and intelligence officials were already planning for the next conflict. General Leslie Groves, the military head of the Manhattan Project that built the atomic bomb, testified that the bomb project “was conducted on [the] basis” that “Russia was our enemy.”<sup>55</sup> After the war, the United States enforced its sphere of influence by building military bases and creating military alliances.<sup>56</sup> It intervened—openly and covertly—to destabilize and overthrow governments it regarded as hostile or dangerous to its policies of control.<sup>57</sup>

The United States created a set of institutions devoted to violence, invasion of sovereign countries, secrecy, and deceit. These institutions receive billions of dollars in secret funding. They carry out policy objectives of imperial domination. The design and nature of these institutions moves them to escape accountability. As Byron wrote:



The thorns which I have reap'd are of the tree  
I planted; they have torn me, and I bleed.  
I should have known what fruit would spring from such a seed.<sup>58</sup>

(Or, more pithily, in the Spanish proverb *Cría cuervos y te sacarán los ojos*—"If you raise a crow it will pluck out your eyes.")

Where and how will we find resistance to and accountability for torture, detention, and killing? One paradigm may be found in the struggle to end the Vietnam War. In the United States, the anti-war movement focused largely on the domestic consequences of the conflict—the sacrifice of young men's lives and the liberties of all of us. The anti-imperialist rhetoric of this movement was more muted, it seemed. But at the same time, international resistance to U.S. military power and tactics grew in strength, until the Vietnamese achieved victory. By similar token, there is resistance today to the exercise of U.S. power.

This resistance is not solely, and perhaps not even principally, of a military character. Despite the U.S. refusal to make its own courts and international tribunals available to victims, courts of other countries are opening inquiries into these issues. The theories of accountability and judicial power in these cases are controversial, but to the extent that they are being used in the service of a progressive agenda they hold some promise. That is, these efforts derive their validity as elements of struggle from the support of movements for meaningful change.

For example, the courts of Argentina have opened to victims of the U.S.-supported Franco regime in Spain, because Spain has closed the doors of its courts to such inquiry. At this writing, a magistrate in France is looking into the torture of three French citizens at Guantanamo. The path to accountability charted in these cases is based on the U.S. refusal to acknowledge universal norms of conduct, and on the general recognition that violation of such norms can be addressed by any sovereign with a plausible connection to the harm caused by the violation.<sup>59</sup>

## Notes

1. "Statement on Intel Committee's CIA Detention, Interrogation Report," press release, March 11, 2014, <http://feinstein.senate.gov>. Former CIA director, General Michael Hayden, went on television to denounce Senator Feinstein's comments as "emotional" and not "objective," as though the only rational response to torture is acquiescence. Ruth Marcus quickly denounced Hayden's comments as sexist nonsense; see "The Emotional Double Standard Applied to Sen. Feinstein," *Washington Post* opinions, April 8, 2014

<http://washingtonpost.com/opinions>.

2. Michael E. Tigar, "The Twilight of Personal Liberty: Introduction to 'A Permanent State of Emergency,'" *Monthly Review* 58, no. 6 (November 2006): 24–28. Jean-Claude Paye's four *Monthly Review* articles are a valuable background to this discussion: "Guantánamo and the New Legal Order," *Monthly Review* 57, no. 1 (May 2005): 45–55; "The End of Habeas Corpus in Great Britain," *Monthly Review* 57, no. 6 (November 2005): 34–43; "A Permanent State of Emergency," *Monthly*

*Review* 58, no. 6 (November 2006): 29–37; "Enemy Combatant' or Enemy of the Government?," *Monthly Review* 59, no. 4 (September 2007): 1–10.

3. My thanks to John Mage for fostering the basic idea behind this article and the *MR* issue of which it is a part. I thank Lord Justice Stephen Sedley for helpful thoughts about separation of powers; he has shared with me the text of his 2014 Oxford Lectures, in which he notes that the concerns discussed in this article have also arisen in the United Kingdom. More com-

plete discussion of the issues may be found in some my earlier work: on legal history *Law and the Rise of Capitalism*, second edition (New York: Monthly Review Press, 2000); *Judicial Power, the "Political Question Doctrine," and Foreign Relations*, 17 U.C.L.A. L. Rev. 1135 (1970), reprinted in Richard Falk, ed., *The Vietnam War and International Law*, vol. 3 (Princeton: Princeton University Press, 1972) (hereinafter "Political Question"); *Thinking About Terrorism: The Threat to Civil Liberties in Times of National Emergency* (Chicago: American Bar Association, 2007), *The Right of Property and the Law of Theft*, 62 Tex. L. Rev. 1443 (1984) (hereinafter "Theft Law"). I continue to post entries on the subject of this article at [tigarbytes.blogspot.com](http://tigarbytes.blogspot.com).

4. Federalist No. 68.

5. Quoted in Political Question, 1172 n158; Henry Steele Commager, ed., *Documents of American History*, vol. 1 (New York: F.S. Crofts, 1944), 147.

6. See generally Christopher Hill, *Reformation to Industrial Revolution* (New York: Pantheon Books, 1967). For the precise text and source of Lord Coke's remarks, as well as many insights into the struggles over separation of powers, see Stephen Sedley, "The Separation of Powers," Oxford Lectures 2013 (fifth lecture), in *The Lion Beneath the Throne* (forthcoming).

7. James Madison to W.T. Barry, letter of August 4, 1882, <http://press-pubs.uchicago.edu>. This often-quoted statement was made in the context of the need for institutions of education. Some have said that Madison was not talking about citizen access to governmental information. This is an unduly constricted meaning. Madison believed—and said—that without knowledge of all kinds, citizens could not exercise meaningful control of government.

8. Federalist No. 45.

9. John Adams, "A Dissertation on the Canon and Feudal Law," <http://digitalhistory.uh.edu>.

10. In England, the institution of "Crown copyright" persists to this day.

11. For an extended discussion of this issue, see Theft Law.

12. *Marbury v. Madison*, 5 U.S. 137 (1803):6

13. The story of this case is told in Bloch & Ginsburg, *Celebrating the 200th Anniversary of the Federal Courts of the District of Columbia*, 90 Georgetown Law Journal 549 (2002). This article discusses many examples of judicial control of executive action.

14. *Ex parte Bollman*, 8 U.S. 75 (1807).

15. See Doug Linder, *The Treason Trial of Aaron Burr*, 2001, <http://law2.umkc.edu>; Robert A. Ferguson, "Treason, Aaron Burr & the National Imagination," in Michael Tigar and Angela Davis, eds., *Trial Stories* (New York: Foundation Press, 2008), 47–81. See also Gore Vidal's 1973 novel, *Burr*

(New York: Random House, 1973).

16. Ferguson, in Tigar and Davis, eds., *Trial Stories*, 111–12.

17. *Ibid.*

18. *United States v. Burr*, 25 F. Cas. 30, 34 (No. 14,692d) (CC Va. 1807).

19. 10 Fed. Cas. 355 (No. 5,420) (C.C.D.S.C. 1808).

20. Discussed in Tigar, *Thinking About Terrorism*, 167–70.

21. U.S. Const., art. 1, §2, abrogated by the 14th amendment.

22. Tigar, *Law and the Rise of Capitalism*, 291–325 (see especially 309–10).

23. 23 U.S. 6 (1825).

24. "Transcript of Treaty of Ghent (1814)," <http://ourdocuments.gov>.

25. 40 U.S. 518 (1841).

26. *Scott v. Sandford*, 60 U.S. 393 (1857).

27. 347 U.S. 483 (1954).

28. See Peter Irons, *Justice At War* (Berkeley: University of California Press, 1993); see also Neal Katyal, "Confession of Error: The Solicitor General's Mistakes During the Japanese-American Internment Cases," May 20, 2011 <http://blogs.justice.gov>, for the story of the original 1940s Supreme Court cases and of Judge Marilyn Hall Patel's courageous decision forty years later finding that the government had presented false evidence in support of its legal claims, and setting aside the judgment as to Fred Korematsu. The history of racial bias against Japanese and Chinese immigrants and their descendants is brilliantly told in Jacobus TenBroek, Edward Norton Barnhart, and Floyd W. Matson, *Prejudice, War and the Constitution: Causes and Consequences of the Evacuation of Japanese Americans in World War II* (Berkeley: University of California Press, 1954); Eric Muller, *American Inquisition: The Hunt for Japanese American Disloyalty in World War II* (Chapel Hill: University of North Carolina Press, 2007). The internment, and the denial of meaningful judicial review to its victims, prefigured many of the issues now being raised in the national security state.

29. *Sweezy v. New Hampshire*, 354 U.S. 234 (1957).

30. *Baker v. Carr*, 369 U.S. 186, 217 (1962), discussed in Political Question.

31. See, e.g., dissent by Justices Stewart and Douglas from denial of certiorari in *Mora v. McNamara*, 389 U.S. 934 (1967). The Court refused to hear a case brought by draftees seeking to challenge the legality of the Vietnam War. The dissent points up the serious and justiciable issues arising from the prosecution of that war.

32. *Lebron v. Rumsfeld*, 670 F.3d 540 (4th Cir. 2012).

33. 175 U.S. 677 (1900), discussed in Tigar, *Thinking About Terrorism*, 167.

34. *Al-Aulaqi v. Obama*, 727 F.Supp.2d 1 (2010).

35. See Nasser al-Awlaki, "The Drone that Killed My Grandson," *New York Times*, July 17, 2013, <http://nytimes.com>. Drone strike killings are said to focus on persons identified by intelligence reports as "enemies," but the government also concedes that 10–20 percent of those killed are innocent of alleged wrongdoing.

36. *Al-Aloqi v. Panetta*, --- F. Supp. 2d ---, 2014 WL 1352452 (D.D.C. 2014).

37. *Schneider v. Kissinger*, 412 F.3d 190 (D.C. Cir. 2005), cert. denied, 126 S. Ct. 1768 (2006), discussed in Tigar, *Thinking About Terrorism*, 31–36.

38. *Letelier v. Republic of Chile*, 488 F. Supp. 665 (D.D.C. 1980).

39. *Aamer v. Obama*, 742 F.3d 1023 (D.C. Cir. 2014).

40. *Klayman v. Obama*, 957 F.Supp.2d 1 (D.D.C. 2013) (finding surveillance violates the constitution); *ACLU v. Clapper*, 959 F.Supp.2d 724 (S.D.N.Y. 2013) (finding that surveillance is "lawful"). The *Clapper* decision begins by noting that the NSA's program is designed to be virtually limitless in scope, and acknowledges that "such a program, if unchecked, imperils the civil liberties of every citizen." However, the court says that any "checks" should come from the "other two coordinate branches of government."

41. Tigar, *Thinking About Terrorism*, 150–51. For citations to the cases and relevant history, see *Boyd v. United States*, 116 U.S. 616 (1886). Some of the *Boyd* holding has been undermined in later cases, but the Court's essential analysis of the fourth amendment and the judicial duty to control searches remains valid.

42. Some small part of this surveillance is approved by a Foreign Intelligence Surveillance Court, established in 1978. That "court" meets in secret, hears only the government's arguments and issues secret rulings. Not surprisingly it has not chosen to limit the scope of government intrusion. See "Foreign Intelligence Surveillance Court (FISC)," <http://epic.org>.

43. 22 U.S.C. §§ 7421-7433, <http://llaw.cornell.edu>.

44. Diana Johnstone, *Fool's Crusade: Yugoslavia, NATO, and Western Delusions* (New York: Monthly Review Press, 2002); Jean Bricmont, *Humanitarian Imperialism: Using Human Rights to Sell War* (New York: Monthly Review Press, 2006). See also Michael Bohlander, Roman Boed, and Richard J Wilson, *Defense in International Criminal Proceedings: Cases, Materials and Commentary* (Ardley, NY: Transnational Publishers, 2006).

45. 345 U.S. 1 (1953).

46. Tigar, *Thinking About Terrorism*, 175.

47. Frankfurter, J., concurring in *U.S. ex rel. Tuohy v. Ragen*, 340 U.S. 462, 473 (1951).

48. The reference is only for purposes of comparison. The review of grand jury proceedings is far from perfect, and grand jury abuse in the name of "national security" and crime-fighting has been widespread. For an overview of the relevant law, see Wayne R. LaFave, Jerold H. Israel, and Nancy J. King, *Principles of Criminal Procedure: Investigation*, 4th edition (St. Paul, MN: Thomson/West2004), chapter 15.

49. *New York Times Co. v. Department of Justice*, 915 F.Supp.2d 508 (S.D.N.Y. 2013).

50. Seekers of information on government surveillance have also been frustrated. See, e.g., *Electronic Frontier Foundation v. Department of Justice*, 739 F.3d 1 (2014).

51. --- F.3d ---, 2014 WL 1569514 (No. 13-422-cv).

52. See, e.g., *First Amendment Coalition v. U.S. Dep't of Justice*, 2014 WL 1411333 (N.D. Calif. 2014). See also *ACLU v. CIA*, 710 F.3d 422 (D.C. Cir. 2013).

53. The tally of suits and their status is set out in 82 U.S. Law Week 1409 (March 25, 2014).

54. Rand Paul, "Show Us the Drone Memos," *New York Times*, May 11, 2014, <http://nytimes.com>.

55. U.S. Atomic Energy Commission, In the Matter of J. Robert Oppenheimer: Transcript of Hearing Before Personnel Security Board 173 (1954). This was the hearing at which General Groves, Edward

Teller and others attacked Oppenheimer's "loyalty" and revealed much about U.S. Cold War strategy. Indeed, the atomic bombs were dropped on Hiroshima and Nagasaki to prevent the USSR from having any role in the post-war events in the Far East; see P.M.S. Blackett, *The Military and Political Consequences of Atomic Energy* (London: Turnstile Press, 1948), and Gar Alperowitz, et. al., *The Decision to Use the Atomic Bomb and the Architecture of an American Myth* (New York: Knopf, 1995). I reached and documented this conclusion in my senior thesis "Atomic Science and Social Responsibility" (University of California, Berkeley, History Dept., 1962).

56. See elsewhere in this issue David Vine, "'We're Profiteers': How Military Contractors Reap Billions from U.S. Military Bases Overseas," *Monthly Review* 66, no.3 (July-August 2014): 82–102.

57. See William Blum, *Killing Hope* (Monroe, ME: Common Courage Press, 2000).

58. Childe Harold's Pilgrimage, Canto iv. Stanza 10.

59. For the Argentina case, see Jim Yardley, "Facing His Torturer as Spain Confronts Its Past," *New York Times*, April 6, 2014. The French case and related matters are discussed at "Universal Jurisdiction: Accountability for U.S. Torture," <http://ccjustice.org>. An important caveat: the fact that judicial forums distant from the place of harm may

be available does not mean that all such forums are legitimate, or that exercises of their power are proper. For example, the International Court of Justice (ICJ) in 2002 wisely held that Belgium could not proceed against a government official of the Democratic Republic of Congo for alleged human rights abuses in the Congo. See Christian J. Tams and James Sloan, eds., *The Development of International Law by the International Court of Justice* (Oxford University Press, 2013), 120 et. seq. The court explicitly denied an exception for war crimes and crimes against humanity to existing international law standards of personal immunity. While the ICJ opinion was a sharp reassertion of traditional standards of personal immunity, it is also possible to read the opinion as influenced by the idea that Belgium giving human rights lessons to the Congo was ludicrously inappropriate. This was brilliantly set out in the Separate Opinion of ad hoc Judge Sayeman Bula-Bula ("Opinion Individuelle de M. Bula-Bula," <http://icj.cj.org>) which persuasively insists on the placing of so-called "universal jurisdiction" in the context of history, and the power of the predominant imperialist jurisdictions. He concludes that the ICJ opinion, properly understood, "should call for greater modesty from the new fundamentalist crusaders on behalf of humanitarianism 'skilled at presenting problems in a false light in order to justify damaging solutions' including a certain trend of legal militancy."

(continued from page 160)

William Franklin ("Bill") Ash, who wrote for *Monthly Review* in the 1960s and was the author of the *Monthly Review* Press book, *Marxism and Moral Concepts* (1964), died at age 96 on April 26, 2014. Ash was an American-born British Spitfire pilot (he had enlisted in the Royal Canadian Air Force early in the war) who was shot down in 1942, and made numerous escapes from Nazi prison camps. He became perhaps the chief inspiration for Steve McQueen's character "the cooler king" in the 1963 Hollywood film, "The Great Escape." After the war Ash studied politics, and became head of the BBC's Indian operations. He was a cofounder of the Communist Party of Britain (Marxist-Leninist) and became the chair in the 1970s and '80s of the Writers' Guild of Great Britain. His wartime experiences were depicted in his 2005 book *Under the Wire*, on which he collaborated with Brendan Foley. An excellent obituary of Ash by Foley appeared in the *Guardian*, April 29, 2014 ("Bill Ash obituary"). The best way to remember Bill Ash is in the terms that he himself used when writing an obituary for Bill Blake in MR in June 1968. Quoting Mao, Ash said: "Though death befalls all men alike, it may be weightier than Mount Tai or lighter than a feather.' The death of one who spent his life serving other people and spreading a knowledge of the liberating force of Marxism is 'weightier than Mount Tai.'"



**Correction:** In Samir Amin, "Popular Movements Toward Socialism" (MR, June 2014), page 17, due to an editing error, the CPI-M was misidentified as the Communist Party of India-Maoist; it is the Communist Party of India-Marxist.