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."[1]

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.[2]

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.[3] But a December 2001 *New York Times* poll suddenly found only 44 percent of respondents believed widespread governmental wiretaps "would violate American's rights."[4]

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.[5]

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, Naruslnsight, 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.[6]

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."[7]

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.[8] 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.[9]

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."[10] 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 brony 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."[11]

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."[12] 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."[13] 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.[14] 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."[15] 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."[16]

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."[17] In March 2013 Clapper lied to Congress, claiming that the NSA was not collecting "data on millions or hundreds of millions of Americans."[18] 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."[19]

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.[20] 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."[21]

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 contact. 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."[22] 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.[23]

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."[24]

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."[25] 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."[26] 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.[27] 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 metadata 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" found in her "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 Perlroth, "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.