

2015

Security and Technology: Rethinking National Security

Sahar F. Aziz

Follow this and additional works at: <http://scholarship.law.tamu.edu/lawreview>



Part of the [Law Commons](#)

Recommended Citation

Sahar F. Aziz, *Security and Technology: Rethinking National Security*, 2 Tex. A&M L. Rev. 791 (2015).

Available at: <http://scholarship.law.tamu.edu/lawreview/vol2/iss4/9>

This Article is brought to you for free and open access by Texas A&M Law Scholarship. It has been accepted for inclusion in Texas A&M Law Review by an authorized administrator of Texas A&M Law Scholarship. For more information, please contact sphillips64@law.tamu.edu.

SECURITY AND TECHNOLOGY: RETHINKING NATIONAL SECURITY

By: *Sahar F. Aziz**

The expansive scope of national security makes it a topic of utmost importance to all Americans. National security law and policy affect nearly every aspect of our lives, our health, our safety, and our dignity. In fact, the topic is so far-reaching that the term “national security” is often exploited for ulterior commercial or political purposes to increase profits, obtain more government funding, and expand government authorities in areas that historically were not related to national security. Indeed, one could reasonably make the claim that we are now in the midst of a national security industrial complex that is self-perpetuating.¹

Due to various competing interests—political, military, and commercial—it is incumbent on us as citizens and lawyers to be attentive and critical of new laws, amendments to old laws, and new technologies employed by the government in purported furtherance of keeping us safer as a nation. Similarly, we cannot neglect the exponential growth of mass data collection in the private sector facially used for “mere commercial” purposes. And as more government work is outsourced to private companies, the line between the private and public sector is blurred. Thus, privacy can no longer be preserved by focusing solely on government action.

Whistleblowers Edward Snowden and Chelsea Manning, among others, have confirmed suspicions that the government has overreached in its mass surveillance of Americans and violated human rights in CIA-run torture programs.² The Senate Select Committee

* Associate Professor, Texas A&M University School of Law where she teaches national security, civil rights, and Middle East law. Professor Aziz thanks the *Texas A&M Law Review* students for their hard work in organizing an informative conference addressing issues that affect all Americans. She also thanks Dean Andrew Morris and Vice Dean Aric Short for their support of the conference as part of a broader scholarly initiative to make Texas A&M School of Law a center of excellence.

1. See, e.g., Heather McDonald, *The Security-Industrial Complex*, WALL ST. J., Sept. 7, 2006, at A20; Mark P. Mills, *The Security-Industrial Complex*, FORBES, Nov. 29, 2004, at 44; Louis Uchitelle & John Markoff, *Terrorbusters Inc.: The Rise of the Homeland Security-Industrial Complex*, N.Y. TIMES, Oct. 17, 2004, at BU1.

2. See, e.g., GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014); SENATE SELECT COMMITTEE ON INTELLIGENCE, COMMITTEE STUDY OF THE CENTRAL INTELLIGENCE AGENCY'S DETENTION AND INTERROGATION PROGRAM (2014), available at <http://www.intelligence.senate.gov/study2014/sscistudy1.pdf>. For further discussion on Chelsea Manning and the WikiLeaks disclosures, see DAVID LEIGH & LUKE HARDING, WIKILEAKS: INSIDE JULIAN ASSANGE'S WAR ON SECRECY 72–89 (2011); GREG MITCHELL, THE AGE OF WIKILEAKS: FROM COLLATERAL MURDER TO CABLEGATE (AND BEYOND) 38–50 (2011).

on Intelligence's 6,000 page report on the torture program confirms that we are not unreasonable in our skepticism to government claims to "trust us, we will not abuse our expanding authorities to abuse your rights" or "trust us, we will be using our powers to protect 'us' from 'them.'"³ Nor are we overreacting if we are critical of private sector claims that data or telecommunications providers will only use our data to sell it to advertisers so that they can keep their services low cost or free to the public.⁴ As we heard from Professors Finkelman and Wagner, the privacy and liberty stakes are in fact much higher than mere nuisance ads or email spam. Rather, our data has become an asset for profit and a means of expanding government powers with minimal transparency.

Going back thirteen years ago in the days following the September 11th attacks, I remember being among the small, and quite unpopular, group of advocates accused of disloyalty because we rang the siren warning of the coming surveillance state that was the precursor for a police state.⁵ Civil liberties advocates warned the public that the hastily passed PATRIOT Act was opening a Pandora's box that could not easily be closed, if ever closed at all, even if the so-called national security crisis ended. For what has been unleashed is a web of interests that seek to perpetuate a security crisis to feed the national security industrial complex. We were dismissed as alarmists when we warned of the proliferation of national security letters, business records requests, electronic surveillance based on laxer legal standards, and increased reliance on the secretive Foreign Intelligence Surveillance Court to collect information about the books we check out of libraries, the books we purchase online, the websites we visit, our financial records, and other private information.⁶

And some of us wonder had it not been for Edward Snowden's disclosures—which makes him a hero to some and a traitor to others—we may never have appreciated just how seriously our civil liberties are at risk.⁷ As Professor Vladeck discussed in his presentation and

3. Paul Krugman, Opinion, *Just Trust Us*, N.Y. TIMES (May 11, 2004), <http://www.nytimes.com/2004/05/11/opinion/11KRUG.html>; Editorial, *President Obama's Dragnet*, N.Y. TIMES, Jun. 6, 2013, at A26, available at <http://www.nytimes.com/2013/06/07/opinion/president-obamas-dragnet.html>.

4. Abraham R. Wagner & Paul Finkelman, *Security, Privacy, and Technology Development: The Impact on National Security*, 2 TEX. A&M L. REV. 597 (2015).

5. Sahar F. Aziz, *The Laws on Providing Material Support to Terrorist Organizations: The Erosion of Constitutional Rights or a Legitimate Tool for Preventing Terrorism?*, 9 TEX. J. C.L. & C.R. 45 (2003); *Spying on America: How the Pentagon is Overcoming Privacy Laws at Home*, DEMOCRACY NOW (June 15, 2004), http://www.democracynow.org/2004/6/15/spying_in_america_how_the_pentagon.

6. EMILY BERMAN, DOMESTIC INTELLIGENCE: NEW POWERS, NEW RISKS 1–8, 21–36 (2011), available at http://www.brennancenter.org/content/resource/domestic_intelligence_new_powers_new_risks/.

7. G. Michael Fenner, *Edward Snowden: Hero or Traitor?*, NEB. LAW., Nov.–Dec. 2014, at 13.

Pearlman and Lee illuminate in their paper, the government and the private sector collectively know everything about us—where we are throughout the day based on our credit card purchases, telephone calls, GPS tracking systems in our cars or smartphones, with whom we spend time, what we like and dislike, what we wear, what we eat, and the most intimate details of our private lives.⁸ Although some lawyers would argue that we have nothing to complain about because we voluntarily disclose such personal information on Facebook, Twitter, Tumblr, and other technologies,⁹ I proffer that this is a specious argument. It is a false choice to choose between a life of social and physical isolation where we revert back to the technological dark ages and a free and dignified life enriched by advances in science and technology arising out of human ingenuity.

The insightful presentations offered in this symposium should persuade us to be critical, skeptical, and even cynical in response to “trust us” messaging by the government or private sector. Failing to do so risks what Professor Vladeck eruditely warned of—an erosion of democratic legitimacy that has long lasting harmful effects on future generations that may be far more of a threat than the terrorists abroad.

But who are “those terrorists”? What images come to our minds every time someone mentions that term? The pictures of dark-haired, brown-skinned, “Muslim-looking” men and women who pop up on our television screens and our Internet browsers inevitably produce

8. Adam R. Pearlman & Erick S. Lee, *National Security, Narcissism, Voyeurism, and Kyllo: How Intelligence Programs and Social Norms are Affecting the Fourth Amendment*, 2 TEX. A&M L. REV. 719 (2015); Stephen I. Vladeck, Panel on Big Data & Mass Surveillance at the Texas A&M Law Review Symposium: New Technology and Old Law: Rethinking National Security (Oct. 17, 2014); see also Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735 (2015).

9. See, e.g., Def.’s Mot. Dismiss, *In Re Google, Inc. Privacy Policy Litigation*, No. 5:13-MD-02430-LHK (N.D. Cal. Jun. 6, 2013), ECF No. 44 (“Just as a sender of a letter to a business colleague cannot be surprised that the recipient’s assistant opens the letter, people who use web-based email today cannot be surprised if their communications are processed by the recipient’s ECS provider in the course of delivery. Indeed, ‘a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.’ *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). In particular, the Court noted that persons communicating through a service provided by an intermediary (in the *Smith* case, a telephone call routed through a telephone company) must necessarily expect that the communication will be subject to the intermediary’s systems. For example, the Court explained that in using the telephone, a person ‘voluntarily convey[s] numerical information to the telephone company and ‘expose[s]’ that information to its equipment in the ordinary course of business.’ *Id.* at 744 (emphasis added).”); Junichi P. Semitsu, *From Facebook to Mug Shot: How the Dearth of Social Networking of Privacy Rights Revolutionized Online Government Surveillance*, 31 SOC. NETWORKING & L. 291, 292 (2011) (recognizing the “Hobson’s choice” faced by the Facebook generation: “either live off the grid or accept that using modern communications technologies means the possibility of unwarranted government surveillance”).

stereotypes in our minds.¹⁰ This is of particular concern to groups and individuals whom by virtue of their ethnicity, race, or religion are collectively suspected as having divided loyalties at best or committing outright treason at worst simply because they share the same identities as suspected terrorists.

Soon after 9/11, Arab, Muslim, and South Asians feared they would suffer the same fate as the Japanese Americans in World War II as Japanese were suspected *en masse* of being sleeper cells and foreign agents for the Japanese government, and as a result interned in concentration camps.¹¹ Japanese Americans were forcibly taken from their homes, their communities, and their schools and jammed into crowded, sub-standard camps in the middle of nowhere to wait for an indefinite period.¹² Decades later, we discovered that the Dewitt military order relied upon to legally and politically justify Japanese internment was infected by false information and intentional inaccuracies about Japanese Americans' activities and loyalties.¹³ Indeed, the Solicitor General at the time suppressed critical evidence from the Supreme Court hearing challenges of the internment.¹⁴ Spurious grounds for interning an entire group of people simply based on their national origin and race went unchallenged by government officials or the public at the time because the negative stereotypes of Asians as suspicious, conniving, and disloyal permeated American society. Such biases compromised our government's ability to provide equal protection under the law to all persons and ultimately compromised our nation's rule of law.

Sixty years after this travesty that stained our nation's moral record, our nation was confronted with another national crisis that invited us to take the intellectual and political shortcuts to point the sharp blade of our law enforcement powers to Muslims, Arabs, and South Asians while misrepresenting racism as patriotic, rational acts in defense of the homeland. Despite calls to intern American Muslims *en masse*, the American public rejected such bigotry due in large part to lawyers, civil rights advocates, and historians' efforts to expose the injustices of the Japanese internment program.

10. See BRIGITTE LEBENS NACOS & OSCAR TORRES-REYNA, FUELING OUR FEARS: STEREOTYPING, MEDIA COVERAGE, AND PUBLIC OPINION OF MUSLIM AMERICANS (2007).

11. Khaled Beydoun, *Between Indigence, Islamophobia, and Erasure: Poor and Muslim in 'War on Terror' America*, CAL. L. REV. (forthcoming 2016).

12. *Korematsu v. United States*, 323 U.S. 214 (1944).

13. GREG ROBINSON, BY ORDER OF THE PRESIDENT: FDR AND THE INTERNMENT OF JAPANESE AMERICANS 209 (2009).

14. Neal Katyal, *Confessions of Error: The Solicitor General's Mistakes During the Japanese-American Internment Cases*, U.S. DEP'T OF JUST. (May 20, 2011), <http://www.justice.gov/opa/blog/confession-error-solicitor-generals-mistakes-during-japanese-american-internment-cases>.

However, calls for racial, ethnic, and religious profiling resonated with many Americans. This, in turn, granted the FBI, NYPD, LAPD, and other police departments political cover to aggressively spy on and investigate Muslims in their mosques, community groups, student associations, and businesses in search of the needle in the haystack, even if it meant burning down the haystack.¹⁵ That is, so long as the haystack is comprised of the lives, liberty, well-being, and dignity of those Muslims, Arabs, and South Asians in America (or anyone who looked like them), then the government's rights-violating preventive dragnet was warranted.¹⁶ Moreover, government profiling and selective anti-terrorism enforcement signaled to the public that suspicion of Muslims was legitimate. In turn, discrimination against Muslims spiked.¹⁷

Arising from such religious profiling that ebbs and flows—depending on our nation's foreign relations—is what Professor Hu accurately describes as predicting one's inclination to commit terrorism. Purported terrorist experts trained the FBI and local police departments that when a Muslim becomes more religious, frequents his mosque more frequently, visits certain websites, and condemns American military interventions in Muslim majority countries, that these are all predictors of terrorism warranting surveillance, prosecution, and imprisonment of the individual.¹⁸ All to protect “us” from “them.”

I want to end with what I warned audiences to whom I spoke in the weeks and months after 9/11: There is no such thing as “our” civil liberties and “their” civil liberties. Do not fall into this common fallacy, even if not explicitly stated, that causes you to let your guard down on government action because you do not think the expansive

15. Matt Apuzzo & Adam Goldman, *Documents Show NY Police Watched Devout Muslims*, ASSOCIATED PRESS (Sept. 6, 2011), <http://www.ap.org/Content/AP-In-The-News/2011/Documents-show-NY-police-watched-devout-Muslims>; see also Joe Coscarelli, *NYPD Even Spied on the Muslim Leaders Who Were Helping Them*, N.Y. MAG. (Oct. 6, 2011), http://nymag.com/daily/intelligencer/2011/10/nypd_even_spied_on_the_muslim.html (reporting that an imam was the target of New York City Police Department surveillance at the same time that he was welcoming officers into his mosque and attending hearings with Mayor Bloomberg and Commissioner Kelly); DOMESTIC INVESTIGATIONS & OPERATIONS GUIDE, FED. BUREAU OF INVESTIGATION § 4, at 21–38 (2008), available at <http://graphics8.nytimes.com/packages/images/nytint/docs/the-new-operations-manual-from-the-f-b-i/original.pdf> (permitting mapping of communities based on race or ethnicity so long as it does not serve as the sole basis for monitoring specific communities); Shirin Sinnar, *Questioning Law Enforcement: The First Amendment and Counterterrorism Interviews*, 77 BROOK. L. REV. 41 (2011).

16. See Sahar F. Aziz, *Caught in a Preventive Dragnet: Selective Counterterrorism in a Post-9/11 America*, 47 GONZ. L. REV. 429 (2012) (examining the various tactics used by government to profile Muslims, Arabs, and South Asians in the so-called War on Terror and how that legitimized private acts of discrimination); Sahar F. Aziz, *From the Oppressed to the Terrorist: Muslim American Women Caught in the Crosshairs of Intersectionality*, 9 HASTINGS RACE & POV. L.J. 1 (2012).

17. *Id.*

18. *Id.*

government powers or private sector information collection will ever be used to deny you your liberty, your privacy, your livelihood, or your dignity. If there were ever any doubts to that warning, Edward Snowden and other whistleblowers have put that debate to rest.¹⁹ Too often “we” dismiss injustice against “them” because we think it will never happen to us. But in our silence we are complicit.

I conclude by urging you to reject divisive narratives that portray our nation and its destiny as excluding certain groups, or worse, portraying those groups as fifth columns. As we wrestle with the complex security, privacy, and technological issues discussed at this symposium, let us learn from history and guard tightly our fundamental values and democratic processes that strengthen our nation from within. For internal threats to our civil liberties may turn out to be as much, if not more, of a threat to our national security than Al Qaeda, ISIS, or other violent extremists could ever be.

19. Yochai Benkler, *A Public Accountability Defense for National Security Leakers and Whistleblowers*, 8 HARV. L. & POL'Y REV. 281, 285 (2014) (“Whistleblowing is seen as a central pillar to address government corruption and failure throughout the world.” TRANSPARENCY INT’L, INT’L PRINCIPLES FOR WHISTLEBLOWING LEGISLATION (Nov. 2013), available at http://www.transparency.org/whatwedo/pub/international_principles_for_whistleblower_legislation).