William Mitchell Law Review

Volume 34
Issue 5 *Journal of the National Security Forum*

Article 3

2008

Targeting Terrorists: The Counterrevolution

Paul Rosenzweig

TARGETING TERRORISTS: THE COUNTERREVOLUTION

Paul Rosenzweig†

New twenty-first century technologies, ranging from link analysis and data-integration to biometrics and new encryption techniques, offer great advantages in achieving the compelling national goal of preventing terrorism. But there is substantial political resistance to many of the new technologies. The enduring problems in the development of a domestic air travel screening program are but one cautionary tale.[1]

The resistance arises from legitimate fears: government access to and use of personal information generates concerns about the protection of civil liberties, privacy, and due process. But the stirring of those fears by the advent of new technologies has given rise to a disturbing pattern in America—a counter-reaction that threatens to swamp not only the valuable new protective measures being taken but also many of the tried and true, traditional means of combating terror. There is a frequently repeated pattern where the pendulum swings back against post-9/11 security improvements to question not only those post-9/11 developments, but proven pre-9/11 practices.

---

† Paul Rosenzweig is the Acting Assistant Secretary for International Affairs and Deputy Assistant Secretary for Policy at the Department of Homeland Security. The views expressed in this article are his own and do not reflect the views of the Department or any other United States government entity.

1. For years, passengers boarding domestic flights were selected for additional screening based upon certain algorithms. This Computer Assisted Passenger Pre-Screening system was known as CAPPS I. Because those rules were widely known and, thus, readily avoidable, the government proposed an enhanced watch list matching system, known as CAPPS II. CAPPS II was widely criticized and was never implemented. *See, e.g.*, U.S. GEN. ACCOUNTING OFFICE, AVIATION SECURITY: COMPUTER ASSISTED PASSENGER PRESCREENING SYSTEM FACES SIGNIFICANT IMPLEMENTATION CHALLENGES 30–31 (2004). Recently, DHS proposed a much slimmed down pre-screening program (now known as Secure Flight), but that program will not be implemented until 2008. *See* System of Records; Secure Flight Records, 72 Fed. Reg. 63,711 (proposed Nov. 9, 2007). Thus, because of concerns about civil liberties we have yet to fully implement a modernized domestic passenger screening system—more than six years after September 11.

Given the geopolitical situation today, that natural pendulum swing is dangerous. The pre-9/11 legal regime is inconsistent with post-9/11 reality. A return to that earlier vision is a greater threat to security than many realize, yet that is what many in the public sphere are urging. This pendulum swing, if unchecked, could short-circuit national security. All the new technology in the world will be of little use if an unwarranted fear of the loss of individual liberty prevents the deployment of both new and old systems.

I. BACKGROUND OF THE COUNTERREVOLUTION

Historians of revolutionary movements call the political pendulum swing back towards a pre-revolutionary state the "Thermidor." It is named after the French month of Thermidor, in which Robespierre was guillotined and the French Revolution effectively ended.[2] The counterrevolutionary impulse is not uncommon. Change is often difficult and public institutions have a natural impulse to swing in pendulum cycles. But, the post-9/11 Thermidor, if unchecked, bids fair to short-circuit national security.

The genesis of the post-9/11 counterrevolution is, in its current manifestation, an elitist skepticism of the idea that the revolution was necessary. It questions whether the terrorism we encounter today really is any different from that of the anarchist Red Brigades who committed acts of violence in Europe in the 1970s. In fact, in recent months we have been treated to a chorus of critics and skeptics, including former government officials, who have begun to downplay the seriousness of the threat that we face in a world after September 11, 2001.[3] Dr. Zbigniew Brzezinski, who served as National Security Advisor to President Carter, is a prime example. In a recent article in the *Washington Post*, he contended that the United States is hyping the War on Terror in order to promote a culture of fear. Dr. Brzezinski argued that the use of the phrase "war on terror" itself caused damage—damage that is "greater than any wild dreams entertained by the fanatical

2. The use of "Thermidor" in this fashion has become commonplace for historians of revolutionary movements. *See, e.g.*, CRANE BRINTON, THE ANATOMY OF REVOLUTION 205–36 (Vintage Books 1965) (1938).

3. Much of the analysis in these three paragraphs is derived from remarks given by Michael Chertoff, Secretary of Homeland Security, Remarks at Westminster College: The Battle for Our Future (Oct. 17, 2007), *available at* http://www.dhs.gov/xnews/ speeches/sp1193063865526.shtm.

perpetrators of the 9/11 attacks."[4]

Some critics deny that we are at war with terrorism. Others admit that we are at war but believe that we can simply unilaterally withdraw from the engagement; that we can simply walk away from the field of battle. Writing in the *Washington Post*, on our nation's birthday last year, William Arkin suggested that we should declare our own independence from the war on terror.[5]

But any suggestion of this nature flounders on the words of Osama bin Laden and Ayman al Zawahiri and their fellow travelers, who very much think we are at war. In his fatwa of 1998, bin Laden made an open declaration of war, starting with the false accusation that America had declared war on Islam. Bin Laden's declaration ended with the command, "to kill the Americans and their allies—civilians and military . . . in any country in which it is possible to do it."[6] It was not a hollow promise. In the decade that followed, bin Laden and his cohorts plotted strikes not only against the United States, but against the entire global system of security, safety, and prosperity. Every time bin Laden has spoken since, including in his recent videos, he has made no secret about his intent. He has promised that he will continue to escalate the war.

So this is a war. And it is not a war from which we have the luxury of unilateral disengagement. The war has been declared upon us, upon our allies and all decent people, by ideological fanatics with a dramatically different world view than the view of freedom and human rights which have characterized Western aspirations for the past hundred-plus years.

And that is why the counterrevolutionary reaction we see today is such a grave risk. It calls into question not only the new counterterrorism practices of the post-9/11 world, but also risks sweeping aside with the pendulum many of the tried and true investigative techniques that predate September 11.

---

4. Zbigniew Brzezinski, *Terrorized by 'War on Terror': How a Three-Word Mantra Has Undermined America*, WASH. POST, Mar. 25, 2007, at B01.

5. Early Warning: A New Declaration of Independence, http://blog.washingtonpost.com/earlywarning/2007/07/a_new_declaration_of_independe.html (July 4, 2007, 9:00 EST).

6. Osama bin Laden, et al., Jihad Against Jews and Crusaders: World Islamic Front Statement (Feb. 23, 1998), *reprinted in* JAMES JAY CARAFANO & PAUL ROSENZWEIG, WINNING THE LONG WAR: LESSONS FROM THE COLD WAR FOR DEFEATING TERRORISM AND PRESERVING FREEDOM app. 16, at 251 (2005).

II. ANALYSIS OF SYSTEMS TODAY

A. *The Automated Targeting System*

The Automated Targeting System (ATS) serves as a prime example. When the Department of Homeland Security (DHS) published a System of Record Notice (SORN) describing the system,[7] it became the subject of excited congressional and public commentary. Some members of Congress wildly called ATS "a warrantless well of evidence from which any law enforcement, regulatory, or intelligence agency could dip at will—without any probable cause, reasonable suspicion, or judicial oversight," and suggested that it constituted a major expansion of how DHS operated.[8] The truth was much less cataclysmic.

ATS is an enforcement screening tool consisting of six separate components, all of which rely substantially on information in the Treasury Enforcement Communications System (TECS). ATS assists Customs and Border Protection (CBP), an operating component of the Department of Homeland Security, in preventing terrorists and terrorist weapons or material from entering the United States and in identifying other violations of U.S. laws while facilitating legitimate trade and travel across the U.S. borders. It is the cornerstone for all CBP targeting efforts.

1. *How the Automated Targeting System Is Used*

ATS data has been a proven resource for connecting the dots associated with terrorist activity and serious transnational crime. Investigations after the September 11th attacks showed that more comprehensive and immediate access to data and analytical tools, like those in ATS, might have facilitated interdiction of the nineteen hijackers at the time of their entrance into the United

7. *See* System of Records, 71 Fed. Reg. 64,543 (proposed Nov. 2, 2006) (initial publication); U.S. Customs and Border Protection, Automated Targeting System, System of Records, 72 Fed. Reg. 43,650 (proposed August 6, 2007) (final SORN). DHS also published a Privacy Impact Assessment for ATS. *See* DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED TARGETING SYSTEM (Nov. 22, 2006).

8. *See* Marc Perelman, *D.H.S. Traveler Screening System under Fire from Privacy Advocates*, NAT. J., Sept. 28, 2007, http://www.govexec.com/dailyfed/0907/092807nj1.htm. DHS received over 600 comments on SORN. For comments and responses regarding SORN, see DEP'T OF HOMELAND SEC., DISCUSSION OF PUBLIC COMMENTS RECEIVED ON THE AUTOMATED TARGETING SYSTEM (2006).

States by linking their methods of payment, phone numbers, and seat assignments.[9]

One component of ATS, known as ATS-P (for "Passenger"), was of particular concern to some in the public.[10] ATS-P is a passenger screening module that compares data that passengers provide to the airlines (known as Passenger Name Records (PNR) and Advanced Passenger Information (API)) with law enforcement lookouts and threat-based scenarios. This allows law enforcement officials to identify patterns of suspicious activity. The scenarios are drawn from previous and current law enforcement and intelligence information.[11] In short, ATS assists CBP in making assessments of persons and cargo prior to their arrival in the United States based on information DHS receives in advance.

Most importantly, for purposes of discussion, this information is relevant to the decision whether to admit someone into the country and is data that DHS would otherwise be authorized to collect at the point of entry.[12] But ATS does not replace human decision making. It is a decision support tool for use by law enforcement officials and does nothing more than assist the border authorities in targeting scarce inspection resources at those

9. *See* Newton N. Minnow, *Seven Clicks Away*, WALL ST. J., June 3, 2004, at A14; *see also* U.S. DEP'T OF DEF., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM: REPORT OF THE TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE 45–46 (2004).

10. ATS consists of six modules that provide selectivity and targeting capability to support CBP inspection and enforcement activities: ATS-Inbound—inbound cargo and conveyances (rail, truck, ship, and air); ATS-Outbound—outbound cargo and conveyances (rail, truck, ship, and air); ATS-Passenger (ATS-P)—travelers and conveyances (air, ship, and rail); ATS-Land (ATS-L)—private vehicles arriving by land; ATS-International (ATS-I)—cargo targeting for CBP's collaboration with foreign customs authorities (in development); and ATS-Trend Analysis and Analytical Selectivity Program (ATS-TAP) (analytical module).

11. Thus, ATS is based on non-invidious facts and scenarios. It does not profile on race, ethnicity, or arbitrary assumptions.

12. Congress, since the beginning of our government, "has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country." United States v. Montoya de Hernandez, 473 U.S. 531, 537 (1985) (citing Act of July 31, 1789, ch. 5, 1 Stat. 29, *construed in* United States v. Ramsey, 431 U.S. 606, 616–17 (1977)). "It is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." United States v. Flores-Montano, 541 U.S. 149, 153 (2004). That plenary authority includes, *inter alia*, the authority to stop and question individuals at the border in order to determine their admissibility. *See* Tabbaa v. Chertoff, No. 05-CV-582S, 2005 WL 3531828, at *10 (W.D.N.Y. Dec. 22, 2005).

travelers who appear to pose a greater risk. In short, ATS is employed as an analytical tool to enhance CBP screening and targeting capabilities by permitting query-based comparisons of different data modules associated with the data holdings of CBP, as well as comparisons with data sets from sources outside of CBP.

Without ATS, the United States would be significantly impaired in its efforts to identify potential threats until after they have entered the United States, and screening at points of entry would be slower and more cumbersome. Port of entry risk assessment is an analysis of the threat-based scenario(s) that a passenger matched when traveling on a given flight. CBP uses ATS to: improve the collection, use, analysis, and dissemination of intelligence; target, identify, and prevent potential terrorists and terrorist weapons from entering the United States; and identify other violations and violators of U.S. law. In this way, ATS allows CBP officers to more effectively and efficiently focus their efforts on cargo shipments and travelers that most warrant further attention. In lieu of manual reviews of traveler information and intensive interviews with every traveler arriving in or departing from the United States, ATS-P allows CBP personnel to focus their efforts on potentially high-risk passengers.

A couple of examples demonstrate the utility of this system of analysis. In June 2003, using PNR data and other analytics, one of CBP's inspectors at Chicago's O'Hare airport pulled aside an individual, Ra'ed al-Banna, for secondary inspection and questioning. When the secondary officers were not satisfied with al-Banna's answers they took his fingerprints and denied him entry to the United States. The next time we saw those fingerprints—or at least parts of them—they were left by a suicide bomber in a car he had blown up, killing 132 people in Iraq. Was al-Banna planning a suicide attack in America? Now, nobody will ever know.

Somewhat more prosaically, in January 2003, CBP in Miami used PNR to disrupt an internal airline conspiracy to smuggle cocaine between Venezuela and Miami. A corrupt ticket counter agent would identify low-risk travelers (typically families) and add an additional bag to their reservation after they departed the ticket counter. This bag would be filled with cocaine. Corrupt airline employees in Miami were scheduled to remove the added bags from circulation prior to inspection by CBP in Miami.[13] That

13. Letter from Michael Chertoff, Sec'y of the Dep't of Homeland Sec., to

loophole is now closed—the ATS system has a targeting rule that provides closer screening of luggage that is checked in after the traveler has checked in.

2. The Debate over the Automated Targeting System

When DHS published a SORN regarding the ATS system, many called it a new intrusion that should be rejected.[14] These calls are a classic counterrevolutionary pendulum reaction. In reality, the system is not a new one, and those who challenge it are actually seeking a reduction in the types of scrutiny for international passengers from the level that existed on September 10, 2001. ATS-P first became operational in 1999, and CBP began receiving PNR data voluntarily from air carriers in 1997.[15] Today, CBP collects this information as part of its border enforcement mission and pursuant to the Aviation and Transportation Security Act of 2001 (ATSA).[16]

A second counterrevolutionary myth is that the ATS-P is somehow a "secret" system that covertly judges Americans and their suitability for travel. Little could be further from the truth. In fact, targeting of passenger information was widely known and fully complies with all applicable U.S. laws relating to privacy.[17] Individuals, regardless of citizenship, may seek access to most of their information in the ATS database. Through FOIA, the Privacy Act, and as a matter of CBP policy, individuals may obtain any of their PNR information collected in ATS, or information used by ATS originating from another government source system.

Finally, ATS has operated without any documented improprieties since its inception. Access to ATS is strictly controlled—it may only be accessed by personnel with a need to access information in the course of completing their official duties. Indeed, ATS employs auditing systems to identify unauthorized

---

Members of the European Parliament (May 14, 2007), *available at* http://www.dhs.gov/xlibrary/assets/press_chertoffltreuroparliament20070514.pdf.

14. *See supra* note 8.

15. *See* U.S. Customs and Border Protection, Automated Targeting System, System of Records, 72 Fed. Reg. 43,650, 43,651 (Aug. 6, 2007) (reciting the history of ATS).

16. Air Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001) (codified as amended at 49 U.S.C. §§ 44903, 44909, 19 C.F.R. 122.49(b) (2005)).

17. *See* Shane Harris, *No Secret...Maybe*, NAT. J., Dec. 8, 2006, http://nationaljournal.com/about/njweekly/stories/2006/1208nj2.htm.

access and misuse, and DHS punishes transgressions whenever they are identified. Significant system safeguards have been implemented to protect the traveling public from the unauthorized disclosure of their personal information.

In short, ATS is an old, well-designed system that is being put to new uses in the counterterrorism field. And yet, the discussion of this tool in the counterterrorism context has caused some to question the tool itself and urge a retrenchment that would actually provide less protection for America than existed prior to 9/11. That sort of counterrevolutionary pendulum swing needs to be recognized for what it is and resisted at all costs.

B. The National Applications Office

A similar counterrevolutionary reaction occurred with the announcement by DHS of the creation of a National Application Office, to coordinate the use of "national technical means" (i.e. satellites) for homeland security purposes. This new office was portrayed in Congress[18] and the press[19] as a massive new intrusion into American privacy. Angry committee hearings were held.[20] The reality, again, was much less sinister.

The technical collection capabilities and resources of the intelligence community have been deployed for decades in civilian and homeland security applications. These capabilities were historically deployed for civilian use on an ad hoc basis through the Civilian Applications Committee ("CAC"). In June 2005, an independent study group recommended that the U.S. Government improve its ability to make available the technical collection

18. *See, e.g.*, Letter from Rep. Bennie G. Thompson, Chairman, H. Comm. on Homeland Sec., Rep. Jane Harman, Chair, H. Subcomm. on Intelligence, Info. Sharing, and Terrorism Assessment, and Rep. Christopher P. Carney, Chairman, H. Subcomm. on Mgmt, Investigations, and Oversight, to Michael Chertoff, Sec'y of the Dept. of Homeland Sec., and Charles Allen, Assistant Sec'y for Intelligence & Analysis, Dept. of Homeland Sec. (Sept. 6, 2007), *available at* http://homeland.house.gov/SiteDocuments /20070907154522-02923.pdf (calling for a moratorium on the office and arguing that there is "effectively no legal framework" governing the domestic use of satellite imagery).

19. *See, e.g., All Things Considered: New Office to Usher Domestic Use of Spy Satellites* (NPR radio broadcast Aug. 15, 2007) (transcript available at http://www.npr.org/templates/story/story.php?storyId=12819895).

20. *See Turning Spy Satellites on the Homeland: the Privacy and Civil Liberties Implications of the National Applications Office Before the H. Comm. on Homeland Sec.*, 110th Cong. (2007) (video feed and prepared statements *available at* http://homeland. house.gov/hearings/index.asp?ID=84).

capabilities and resources of the intelligence community for civilian and homeland security applications.

These capabilities will now be deployed through a more disciplined and systematic approach in the National Applications Office (NAO). The Director of National Intelligence (DNI) endorsed the establishment of the NAO and designated DHS as its Executive Agent and Functional Manager.

The NAO does not collect intelligence. Its role is to review civilian requests for access to certain technical intelligence capabilities ("technical capabilities") and to endorse and prioritize those requests that propose appropriate uses of the capabilities. The NAO is limited to evaluating requests for civil, homeland security, and, potentially, law enforcement use of these capabilities. The NAO may also perform the limited additional function in certain cases of analyzing and packaging lawfully-collected information into a tailored product that meets the legitimate needs of the requester. The NAO will not accept requests from law enforcement agencies until the scope, lawfulness, and appropriateness of the proposed use of technical capabilities has been assessed and agreed upon by the Department and other relevant parties.

The NAO's first priority is to ensure observance of the law. Thus, the NAO has no plans to endorse any use of technical capabilities that exceed the lawful authority of the requesting agency. In particular, if a proposed use requires a warrant or consent under the laws and Constitution of the United States, the NAO does not endorse that use unless it is satisfied that the requirement will be met.

Many requests for access to technical capabilities have a long history of endorsement by the CAC. Typical uses of these capabilities included: saving lives through support to forest firefighters, support to the U.S. Coast Guard for search and rescue operations, and support to response teams following a disaster; assessment of readiness in advance of a natural disaster; damage assessment following the occurrence of a natural disaster, such as hurricanes, earthquakes, and floods; geospatial mapping; and environmental studies relating to geologic features, forestation, studies of wildlife, and other environmental research.

The constitutional protections that apply to the NAO depend on a number of factors, including the location of the target, individual, or activity to be observed, which informs the

determination of whether there is a reasonable expectation of privacy. To a certain extent, the type of technology utilized may be a factor. For example, the "open fields" line of cases makes clear that the surveying of open fields from the air does not constitute a search within the meaning of the Fourth Amendment because an individual has no reasonable expectation of privacy in his open fields.[21] Thus, satellite surveillance of "open fields" or activities conducted within those areas will not trigger Fourth Amendment protection, regardless of the method or technology employed. By contrast, if the government uses highly sophisticated equipment not generally available to the public to observe activities in an individual's home, particularly details that are not otherwise observable with a naked eye, a warrant or consent may be required.[22]

Requests for the use of intelligence community imagery capabilities through the NAO must also be consistent with the Posse Comitatus Act.[23] The Posse Comitatus Act prohibits the U.S. Army and Air Force (and the National Guard when acting under federal or Title 10 authority) from direct or active military participation in civilian law enforcement activities. Similar principles enacted in Department of Defense regulations prohibit the use of Marines or Navy personnel in a similar manner. Indirect or passive military support to civilian law enforcement is permissible and must be consistent with Executive Order 12,333 and Department of Defense procedures.[24] Any request that may involve a military-controlled capability (whether people or property) is carefully analyzed, taking into consideration the authority under which the capability will be used, the source of funding, and other factors, to determine if the use would constitute "direct or active" or "indirect or passive" military participation in civilian law enforcement activities.

To assure that these rules are followed, every agency or organization requesting the use of the intelligence community's technical intelligence capabilities will submit an annual memorandum that both defines its requirements and intended uses and specifies the legal and policy restrictions governing use of any information provided. The proposed uses will be screened by

21. *See, e.g.*, Oliver v. United States, 466 U.S. 170, 178 (1984).
22. *See generally* Kyllo v. United States, 533 U.S. 27, 40 (2001).
23. 18 U.S.C. § 1385 (2006).
24. *See* United States v. Red Feather, 392 F. Supp. 916, 922–23 (D.S.D. 1975).

the NAO staff to identify special uses requiring further review within the Department. The NAO staff will be assisted by the DHS Office of General Counsel and by other policy, privacy, and civil liberties offices as those offices deem necessary. In reviewing the proposed uses, the staff of the NAO is encouraged to consult with other departments and agencies. During their review, the staff will give careful scrutiny to any uses that fit into the following categories:

- The collection is requested for or reasonably expected to reveal information about the activities of U.S. persons or other persons in the United States;
- The collection supports any law enforcement organization or other U.S. agency/department that is performing statutory and authorized law enforcement functions;[25]
- The collection supports a regulatory enforcement organization or purpose, or could reasonably be expected to support or become involved in regulatory enforcement proceedings;
- The anticipated use of collected imagery is likely to result in a request to disclose classified sources or methods or presents a risk of unapproved disclosure of such sources and methods;
- The nature of the imagery collected could reasonably be considered intrusive or could reasonably be considered to raise privacy issues;

25. Exec. Order No. 12,333, § 2.6, 46 Fed. Reg. 59,941, 59,951 (Dec. 4, 1981), authorizes the intelligence community to provide limited support to law enforcement authorities. With regard to the NAO, the intelligence community may (1) render any other assistance and cooperation to law enforcement authorities not precluded by applicable law; (2) when lives are endangered, provide specialized equipment, technical knowledge, or assistance of expert personnel to support local law enforcement agencies; and (3) provide specialized equipment, technical knowledge, or assistance of expert personnel for use by any department or agency. Despite the ability of the intelligence community to provide this support, the NAO will not process any request on behalf of law enforcement agencies, unless and until the National Applications Executive Committee determines appropriate limits on and procedures for doing so.

- The requested collection otherwise raises novel or significant legal or policy issues.

After this screening, the NAO will determine whether to endorse a request and how it should be prioritized. If it is assessed that a request may fit in one of the above categories, this will be highlighted in the request package that is forwarded to the appropriate intelligence community for its review and final decision.

To further ensure that any decisions regarding these uses receive the highest level review, DHS has committed that certain categories of proposed uses *must* be referred to an internal review committee consisting of the leaders of the Policy, Office of General Counsel, and Intelligence & Analysis Directorates and receive the endorsement of the Secretary or Deputy Secretary before the NAO may endorse the use. In particular, these special uses include: (1) any novel or significant homeland security uses, and (2) the potential application of any new technology that has Fourth Amendment implications.[26]

In determining whether a proposed use raises novel legal or policy issues, the NAO takes into account limitations that may stem from constitutionally based search and seizure rights, privacy concerns, and restrictions on either the collection of information about the activities of specific U.S. persons or the gathering of data for a law enforcement purpose. New and emerging technologies will also be reviewed to ensure that new policy and legal concerns are not raised by their application to the specifics of a given request.

In short, here again the counterrevolutionary reaction runs grave risks. Because of fears of misuse—fears that are readily answered through an internal oversight process and, no doubt, through frequent Congressional review—critics have thought to throw the baby out with the bath water and prohibit all use of intelligence assets for non-intelligence purposes. Think about that kind of overreaction next time you see a satellite photograph of a fire in Southern California or a bridge collapse in the heartland of Minnesota.

26. *See, e.g.*, Kyllo v. United States., 533 U.S. 27 (2001).

III. CONCLUSION

Trying to stop the deployment of new technology is like King Canute trying to sweep back the tide. Using that development to question settled practices is even more fruitless. Rather than vainly trying to reverse progress and return to a time when we were not at war, it is time (and perhaps past time) for the United States to recognize the reality of what we face and to go about the business of answering the hard questions of oversight and implementation. The wrong reaction is the counterrevolutionary one of the Thermidor—to discard not only new capabilities but to also question ones of established utility.

***