LIBERTY FOR SECURITY

On 11 September 2001, we collectively endured the worst tragedy to touch American soil since the Civil War. In the wake of this horrible event, a national hysteria erupted. People are anxious to restore the lost security; but at what cost? Many Americans seem not to care about the costs, and national polls show that now, more than ever, Americans are willing to trade their precious civil liberties in an attempt to restore security. As the ACLU has stated these are difficult days. Not only are they difficult, they will define the future of America. This iBrief explores the reactions of the American government to this tragedy and the effect these reactions will have on the freedom of all Americans.

Introduction

On 11 September 2001, we collectively endured the worst tragedy to touch American soil since the Civil War. In one day America lost a number of innocent, civilian lives equal to one-eighth of the number of American military casualties in Vietnam, a ten-year war. America lost a symbol of its free-market, laissez-faire ideals, the World Trade Center. We all lost the security that we had come to take for granted as Americans. In the wake of this horrible event, a national hysteria erupted. People are anxious to restore the lost security. We can never resurrect the people we lost; we cannot easily recreate a monument to American dominance of the world economy like the World Trade Center. Perhaps the only thing we can salvage is our security, but at what cost? Many Americans seem not to care about the costs, and national polls show that now, more than ever, Americans are willing to trade their precious civil liberties in an attempt to restore security. For that reason, the ACLU has labeled these "difficult days." Not only are they difficult, they will define the future of America. What greater victory could the terrorists have sought than to fundamentally alter our way of life? Are we willing to let them?

Legislative Remedies

American society encourages legislative action in response to a problem. The question commentators always ask of our elected leaders is: "What are you going to do about [insert current issue of interest]?" The attitude that our federal government, through our elected representatives, should be doing something about every major issue and every new problem has become a part of our psyche. One must wonder if this is a healthy condition for a free society. One cannot blame politicians, though. They must consider periodic reelection. A politician that

returns to his district and informs his constituents that he has done absolutely nothing during his time in office quickly finds himself out of a job. The strongest human instinct, self-preservation, encourages a profuse legislative response to any issue of public concern.

It is doubtful one would find anybody suggesting that nothing should be done in response to the terrorist attacks of 11 September 2001, and that is certainly not the suggestion here. One must consider, though, that lawmakers are under intense pressure to seem as though they are addressing important issues and problems through lawmaking. Imagine the pressure they face now that there are an estimated 6,000-plus civilian casualties, the New York skyline is significantly diminished by the loss of an icon of American capitalism, and the vulnerability of the heart of our national defense organization has been exposed to the world. The pressure on lawmakers to do something, *anything*, is compelling. It is in this spirit that one should examine, with a careful eye, the legislation they enact.

Combating Terrorism Act of 2001

Two days after the tragedy, on Thursday, 13 September, the Senate passed an amendment to House appropriations bill H.R. 2500.[1] Titled the "Combating Terrorism Act of 2001," SA 1562 contains various provisions in the spirit of combating terrorism. Before one examines the provisions of SA 1562, one should consider the spirit in which it was passed. The key consideration is the political fallout that would be faced by any legislator who opposed the Combating Terrorism Act of 2001. Does a legislator's opposition of the Combating Terrorism Act indicate that the legislator is opposed to combating terrorism? Though it appears clear that such a claim is unjustified without further information, try to imagine the manner in which a political opponent might exploit (to the legislator's detriment) such a vote. It is probably obvious that, considering the hysteria surrounding terrorist acts, a vote against SA 1562 could easily end a politician's career.

The Combating Terrorism Act of 2001 contains sensible provisions like requiring an assessment report on the National Guard's readiness to respond to terrorism (Sec. 812) and relaxing guidelines that previously hindered the recruitment of terrorist informants (Sec. 815).[2] There are more dubious sections of SA 1562, though. On 19 September 2001, the Electronic Frontier Foundation (EFF) released an analysis of SA 1562.[3] Perhaps the most important

---

[1] *Combating Terrorism Act of 2001*, S. Amdt. 1562, 107th Cong. (2001), http://www.cdt.org/security/010913senatewiretap2.shtml. (last visited October 2, 2001).
[2] *Id.*
[3] Draft, Electronic Frontier Foundation, *EFF Analysis of SA 1562, Subtitle B* (Sept. 19, 2001), http://www.eff.org/ (last visited October 2, 2001).

observation contained in the analysis is that "the government does not need additional authority to investigate terrorism . . . [because] the current list of federal offenses that may support a wiretap order already includes virtually every felony that might be committed by terrorists."[4] This should raise questions in the minds of rational individuals. If the government does not need to pass this legislation to accomplish the stated goals, then what are the true goals of the legislation?

SA 1562 amends language in 18 U.S.C. § 2339A, removing the following important language: "An investigation may not be initiated . . . based on activities protected by the First Amendment . . . including expressions of support or the provision of financial support for the nonviolent political, religious, philosophical, or ideological goals or beliefs of any person or group."[5] Title III, 18 U.S.C. § 2518(11)(b), grants authority to law enforcement to employ roving wiretaps.[6] A traditional wiretap may be placed on only a specific, designated telephone line while a roving wiretap authorizes the tapping of any telephone line from any location that an investigated individual uses.[7] Combine the removal of restrictions prohibiting investigations based on one's politics, religion, philosophy, or ideology with Title III authority to perform roving wiretaps and it is clear that SA 1562 grants the government almost unlimited power to track, record, and scrutinize citizens' (perhaps we should begin referring to ourselves as subjects) phone conversations. Wiretapping phone lines is not the only area in which SA 1562 expands the surveillance ability of law enforcement.

The Combating Terrorism Act also amends the definition of pen/trap devices. For a complete discussion of pen/trap devices, please consult our previous Brief entitled "Carnivore: Will It Devour Your Privacy?" SA 1562 significantly broadens the definition of a pen register. 18 U.S.C. § 3127 defines a pen register as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted."[8] The definition under SA 1562 is expanded to include devices that record or decode "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted."[9] The important distinction between the issuance of a wiretap order and a pen/trap order is that a wiretap requires a showing of probable cause while a pen/trap order only requires the statement of a police officer that the information sought is "relevant to an

---

[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*

ongoing criminal investigation."[10] With the almost nonexistent standard of judicial review that is applied to applications for pen/trap orders, the result of the amendment is that law enforcement may monitor actual communication in the form of Internet "addressing information" such as URLs. Because a URL contains much more specific information than a telephone number, the monitoring of URLs is necessarily content based (compare (800) 555 – 1234 with http://www.eff.org/sc/eff_wiretap_bill_analysis.html). The same is true for terms entered into a search engine, which may also be treated as "addressing information."[11]

The Combating Terrorism Act of 2001 passed the Senate by voice vote.[12] The opposition was either non-existent or so muted that there was no need for a more precise vote. This is in spite of the Senator Leahy's (D – VT) complaint that copies of SA 1562 were distributed a mere thirty minutes prior to the vote. Senators are notorious for neglecting to read the bills and amendments they vote on, relying instead on a briefing by a lobbyist or an aide. With the unusually hurried manner in which SA 1562 was brought to a vote, it seems unlikely that many, if any, of the Senators read the amendment prior to voting. Again, who among them would be brave enough to vote against Combating Terrorism simply because they did not have the opportunity to consider the amendment? In the words of President Bush, ostensibly directed to world leaders but also intended for domestic ears, "Either you are with us, or you are with the terrorists."[13]

Anti-Terrorism Act of 2001

On Wednesday 19 September 2001, Attorney General John Ashcroft submitted a draft proposal for anti-terrorism legislation to Congress. The stated purpose of the bill, submitted by Ashcroft, is "To combat terrorism and defend the Nation against terrorist acts, and for other purposes."[14] Similar in many respects to the wiretapping amendments passed as the Combating Terrorism Act of 2001, the Anti-Terrorism Act of 2001 is more extensive and more complete. It has met with a storm of resistance from groups on all sides of the political spectrum. The Justice Department was judicious enough to concurrently release a Section-By-Section Analysis of the Anti-Terrorism Act of 2001.

---

[10] *Privacy: Opposition to FBI Computer Surveillance Emerges After Vote*, Nat'l J.'s Tech. Daily, Sept. 14, 2001, PM Edition, LEXIS, News Group File.
[11] *Id.*
[12] Summary, S. Amdt. 1562, 107th Cong. (2001), http://thomas.loc.gov/ (last visited October 2, 2001).
[13] President George W. Bush, Text: Bush Address to Congress (Sept. 20, 2001), http://news.bbc.co.uk/ (last visited October 2, 2001).

A detailed section-by-section analysis is beyond the scope of this iBrief; but the Justice Department's Analysis is fair.[15] Major sections of interest to cyber-criminologists fall under Title I (Intelligence Gathering) Subtitle A (Electronic Surveillance). Section 101, Modification of Authorities Relating to Use of Pen Registers and Trap and Trace Devices, performs essentially the same function as the pen/trap provisions of SA 1562, detailed above. Section 101 allows the government to apply for a pen/trap order that is valid in any jurisdiction in the nation. The law as it exists now requires an application for each jurisdiction in which authorities want to employ a pen/trap device. Section 101, like SA 1562, expands the applicability of pen/trap orders and devices to include Internet communications and also to include the tracking of content-based addressing and routing information. Section 101 allows law enforcement to engage in forum shopping, seeking a sympathetic judge whose pen/trap orders are valid in any jurisdiction.

Section 102, Seizure of Voice Mail Messages Pursuant to Warrants, reduces the burden law enforcement faces when seizing stored voice messages. Currently, the seizure of voice mail messages requires a Title III wiretap order. Section 102 would reduce the burden for examining voice mail messages to a simple search warrant. In essence it alters the classification of stored voice communication, placing it a level below live voice communication in terms of the burden law enforcement must meet to intercept or seize it.

Section 105, Use of Wiretap Information From Foreign Governments, removes Fourth Amendment protection from the communications of American citizens collected by foreign governments, as long as they were collected "without the knowing participation of any officer or employee of the United States or person acting at the direction thereof."[16] Under Section 105, information collected in wiretaps put in place by foreign governments that violate the Fourth Amendment can be used in a criminal prosecution in the United States against a U.S. citizen.

Currently the government can use a subpoena to compel information from an ISP such as a customer's name, address and length of service. Section 107, Scope of Subpoenas for Records of Electronic Communications, would further allow the collection of personal financial information such as credit card numbers with a subpoena. Currently, law enforcement must secure a court order to gain access to personal financial data.

---

[14] Anti-Terrorism Act of 2001, Administration proposal to the 107th Congress (proposed on September 19, 2001), *at* http://www.cdt.org/security/010920bill_text.pdf (last visited September 27, 2001).

[15] Department of Justice, Anti-Terrorism Act of 2001 Section-By-Section Analysis, at http://www.cdt.org/security/010919terror.pdf (last visited September 27, 2001).

[16] Anti-Terrorism Act of 2001, Administration proposal to the 107th Congress (proposed on September 19, 2001), *at* http://www.cdt.org/security/010920bill_text.pdf (last visited September 27, 2001).

Section 108, Nationwide Service of Search Warrants for Electronic Evidence, performs much the same function as the jurisdictional aspects of Section 101, only with respect to e-mail. Law enforcement must currently secure a search warrant in the district where the e-mail storage servers are located in order to compel the production of unopened e-mail. Section 108 would remove this hurdle and allow a search warrant issued in any district to apply to unopened e-mail stored in any district.

Section 110, Emergency Disclosure of Electronic Communications, has a two-fold effect on the law as it relates to ISPs. First, Section 101 authorizes the disclosure of electronic communications by an ISP if it reasonably believes that there is an immediate danger of death or serious physical injury to any person. Currently ISPs may disclose the contents of a customer's communications but not the customer's non-content records, such as login records, in order for the ISP to protect its rights or property. Section 110 erases this boundary, allowing the ISP to voluntarily disclose both content and non-content based customer records and communications in order to protects its rights or property.

In evaluating the relative attractiveness of the Anti-Terrorism Act (ATA), it is important to realize that law enforcement officials have been seeking these powers for years. Until now, the political climate has been unfriendly to power grabs of the nature of the ATA. The discussion of patriotism and political survival that applied to SA 1562 also applies to the ATA. Again, which politicians are brave enough to vote against an Anti-Terrorism Act? They face the risk of forever stigmatizing themselves as pro-terrorism.

To simplify exactly what is being proposed, Ashcroft is asking for Congress to lower the burden for the use of intrusive surveillance devices. Currently, law enforcement officials must make a showing of probable cause of a crime in order to intrude into and conduct searches of someone's car or home. If the ATA passes Congress in its current form, the bar will be significantly lowered, and law enforcement will simply have to assert that a suspect is likely to be engaged in terrorist activity to obtain permission to engage in the surveillance.[17]

The ACLU came out in opposition to the ATA the day after it was introduced. The ACLU points out that, though the bill is names the Anti-Terrorism Act, the reduction in burdens faced by law enforcement to secure surveillance orders will be apply to every American, not just terrorists. Possibly the most disturbing result of the ATA, from the ACLU's perspective, is the minimization of the role judges play in judicial oversight of law enforcement activities. The level of judicial oversight will be reduced from probable cause to a mandated grant of the surveillance

---

[17] Jackie Koszczuk, *Groups Want Plan that Would Encroach on Individual Liberties Scaled Back*, Knight Ridder Wash. Bureau, Sept. 21, 2001, LEXIS, News Group File.

order by a judge upon receipt of certification from a law enforcement officer that the information to be obtained is "relevant to an ongoing criminal investigation."[18] The ATA would also expand the use of Carnivore by relaxing and expanding the standards for employing pen/trap devices.[19]

According to the Center for Democracy & Technology, the ATA would do little to improve the ability of law enforcement to utilize surveillance and instead simply weaken the process of judicial review. The prospect of diminishing judicial review, perhaps the only true check on law enforcement's power, has brought groups of diverse interests together in opposition to the ATA. On 20 September 2001, at the National Press Club in Washington, more than 150 groups, from the ACLU to Gun Owners of America, the National Black Police Association to the National Lawyers Guild to the National Gay and Lesbian Task Force, expressed their support for a declaration entitled "In Defense of Freedom." Among the group were more than 300 law professors, and 40 computer scientists. The ten-point declaration urges caution, point number six being perhaps most poignant: "We should resist the temptation to enact proposals in the mistaken belief that anything that may be called anti-terrorist will necessarily provide greater security."[20]

Conclusion

John Ashcroft testified before the House Judiciary Committee on Monday, 24 September 2001. He urged immediate action and scoffed at the idea of including a sunset provision, saying, "If I thought the risk of terrorism was going to sunset in several years, I would be glad to say we ought to have a sunset provision."[21] Lawmakers scoffed at Ashcroft's inability to explain the faults they find in the ATA and his "inability to say that such measures could have prevented the Sept. 11 attacks."[22] Because of these deficiencies in Ashcroft's testimony, the committee was "unwilling to sign on to what appears to be one of the DOJ's old laundry lists."[23]

It seems appropriate to conclude with a charge for all of those who would call themselves lovers of America, lovers of freedom, patriots:

---

[18] *ACLU Says Congress Should Treat Administration Proposal Carefully; Says Many Provisions Go Far Beyond Anti-Terrorism Needs* (Sept. 20, 2001), *at* http://www.cdt.org/security/010920aclu.shtml. (last visited October 2, 2001).
[19] *Id.*
[20] *In Defense of Freedom* (Sept. 20, 2001), *at* http://www.indefenseoffreedom.org/. (last visited October 2, 2001).
[21] Audrey Hudson & David Boyer, *Lawmakers Closer on Taps, Detention of Immigrants*, Wash. Times, Sept. 27, 2001, http://www.washingtontimes.com (last visited October 2, 2001).
[22] Brandon Spun, *Judiciary Committee Balks at Proposed Antiterrorism Act*, Insight Magazine (Sept. 25, 2001), *at* http://www.insightmag.com/cgi-bin/ViewNews.cfm?Item=305. (last visited October 2, 2001).
[23] *Id.*

During this time of intense pressure to act first and consider the consequences later, we must give our utmost respect and patience to those legislators who are courageous enough to place the sanctity of our civil liberties above their self-interest and above the national hysteria.

Author: Morgan Streetman