The Reauthorization of the PATRIOT Act

Subcommittee on Crime, Terrorism, and Homeland Security
Committee on the Judiciary
United States House of Representatives

March 9, 2011

Statement of Nathan A. Sales
Assistant Professor of Law
George Mason University School of Law

Chairman Sensenbrenner, Ranking Member Scott, and Members of the Subcommittee, thank you for inviting me to testify on this important issue. My name is Nathan Sales, and I am a law professor at George Mason University School of Law, where I teach national security law, administrative law, and criminal law. Previously, I was Deputy Assistant Secretary in the Office of Policy at the U.S. Department of Homeland Security. I also served in the Office of Legal Policy at the U.S. Department of Justice, where I was a member of the team that helped draft the USA PATRIOT Act[1] after the terrorist attacks of September 11, 2001. The views I will express in this hearing are mine alone, and should not be ascribed to any past or present employer or client.

The gist of my testimony is as follows. The USA PATRIOT Act is a vital set of tools in our ongoing struggle against al Qaeda and like-minded terrorists. This is especially true of the three authorities that are up for renewal this year: "roving wiretaps," "business records," and "lone wolf." Notwithstanding the PATRIOT Act's controversial reputation, these three provisions are actually quite modest. In many cases, they simply let counterterrorism agents use some of the same techniques that ordinary criminal investigators have been using for decades – techniques that the federal courts repeatedly have upheld. Plus, each of these authorities contains elaborate safeguards – including prior judicial review – to help prevent abuses from taking place. Indeed, some of the PATRIOT Act's protections are even *stronger* than the ones from the world of ordinary law enforcement.

I. Roving Wiretaps

The policy rationale for "roving wiretaps" – in essence, court orders that apply to particular *people*, rather than particular *devices* – is fairly straightforward. Sophisticated targets like drug kingpins, mob bosses, spies, and terrorists are trained to thwart electronic surveillance by constantly switching communications devices or methods. They might use "burner" cell phones, for instance, or they might repeatedly swap out their phones' SIM cards. The result is a drawn-out game of cat and mouse.[2] Investigators obtain a court order to tap a suspect's new

[1] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[2] S. Rep. No. 99-541, at 31, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3585 ("[L]aw enforcement officials may not know, until shortly before the communication, which telephone line will be used by the person under surveillance.").

phone only to discover that he has already switched to an even newer one. So it's back to the judge for a fresh warrant. Not only is this cycle a waste of investigators' scarce time and resources, it also runs the risk that agents will miss critical communications in the gap before the court can issue an updated order.

Congress largely solved this problem for criminal investigators two and a half decades ago. The Electronic Communications Privacy Act of 1986 (ECPA) amended the federal wiretap statute – Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) – to allow investigators to conduct electronic surveillance when they cannot meet the ordinary statutory requirement of specifying "the facilities from which or the place where the communication is to be intercepted."[3] Instead, investigators may obtain a court order to operate a roving wiretap if, among various other things, they establish "probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility."[4] In effect, a single court order permits surveillance regardless of what device the target might be using.[5] Investigators may continue to monitor a suspect even if he switches phones, without first heading back to court to obtain further judicial approval.

Of course, terrorists and spies can be just as adept at evading surveillance as drug dealers and mobsters. Maybe even more so. And so the PATRIOT Act allows national security investigators to use the same sort of technique as their law enforcement counterparts. Section 206 of the law permits roving wiretaps under the Foreign Intelligence Surveillance Act of 1978 (FISA) where "the actions of the target of the application may have the effect of thwarting the identification of a specified person."[6] The basic idea here is to level the playing field between criminal cases and terrorism cases. If a roving wiretap is good enough for Tony Soprano, Congress concluded, it's good enough for Mohamed Atta.

Significantly, the PATRIOT Act's roving wiretaps authority contains exacting safeguards to protect privacy and civil liberties. As in the criminal context, a prior court order is necessary. FBI agents can't unilaterally decide to eavesdrop on every phone a person uses. They have to appear before the Foreign Intelligence Surveillance Court and convince a federal judge that there is probable cause to believe that the target is a "foreign power" (such as a foreign country or a foreign terrorist organization) or an "agent of a foreign power" (such as a spy or a terrorist).[7] In other words, Congress has interposed a "neutral and detached magistrate"[8] between investigators and targets – the same sort of protection that we have long trusted to strike the right balance between security and privacy in the law enforcement context. Agents also must demonstrate probable cause to believe that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign

[3] 18 U.S.C. § 2518(1)(b)(ii).

[4] *Id.* § 2518(11)(b)(ii).

[5] United States v. Hermanek, 289 F.3d 1076, 1087 (9th Cir. 2002).

[6] 50 U.S.C. § 1805(c)(2)(B).

[7] *Id.* § 1805(a)(2)(A).

[8] Johnson v. United States, 333 U.S. 10, 14 (1948).

power."[9] The government has to adopt "minimization procedures" – i.e., procedures to ensure that private information about innocent Americans is not collected, retained, or disseminated.[10] (To be precise, this requirement applies to any "United States person" – i.e., a citizen or lawful permanent resident alien.[11] For simplicity's sake, this testimony will use the term "American" as a shorthand for "United States person.") And, again, roving wiretaps aren't available in every national security case as a routine matter. They may only be used where the FISA court finds, "*based upon specific facts provided in the [government's] application*, that the actions of the target of the application may have the effect of thwarting the identification of a specified person."[12]

Federal courts agree that Title III's roving wiretaps authority is constitutional, and that consensus provides strong support for the constitutionality of roving wiretaps under the PATRIOT Act. For instance, in *United States v. Petti*,[13] the Ninth Circuit held that roving wiretaps are perfectly consistent with the Fourth Amendment's particularity requirement.[14] The court went on to emphasize that Title III presents "virtually no possibility of abuse or mistake."[15] This is so, it explained, because the statute only allows monitoring of telephones that the suspect is using, it requires minimization, and it only applies when the suspect is trying to evade surveillance.[16] (Roving wiretaps under PATRIOT feature virtually identical safeguards.) The Fifth Circuit expressly adopted the *Petti* court's reasoning a few years later,[17] and the Second Circuit likewise has upheld the use of roving wiretaps.[18] To my knowledge, no appellate court has reached a contrary conclusion. In short, there is a broad judicial consensus that, as the Ninth Circuit put it in another case, "[r]oving wiretaps are an appropriate tool to investigate individuals . . . who use cloned cellular phone numbers and change numbers frequently to avoid detection."[19]

Finally, let me say a few words about "John Doe" roving wiretaps – surveillance in which the FISA court order describes the target but does not indicate his precise name or the precise facilities to be tapped. The risk of misuse under the PATRIOT Act seems to me fairly low. There may be times when investigators don't yet know the specific identity of the terrorist in question.[20] (Indeed, the need to learn more about the target is precisely why one conducts

---

[9] 50 U.S.C. § 1805(a)(2)(B).

[10] *Id.* § 1801(h).

[11] *Id.* § 1801(i).

[12] *Id.* § 1805(c)(2)(B) (emphasis added).

[13] 973 F.2d 1441 (9th Cir. 1992).

[14] U.S. CONST. amend. IV ("[N]o warrants shall issue, but upon probable cause, supported by oath or affirmation, and *particularly describing the place to be searched*." (emphasis added)).

[15] *Petti*, 973 F.2d at 1445.

[16] *Id.*

[17] United States v. Gaytan, 74 F.3d 545, 553 (5th Cir. 1996).

[18] United States v. Piggott, 141 F.3d 394 (2d. Cir. 1997).

[19] United States v. Hermanek, 289 F.3d 1076, 1087 (9th Cir. 2002).

[20] 50 U.S.C. § 1805(c)(1)(A), (B) (directing the FISA court to specify the target's identity "if known," and the facilities to be surveilled "if known").

surveillance in the first place.) In these circumstances, investigators need not indicate his name, but they still must provide the FISA court with a "description of the specific target,"[21] which might include the names of his terrorist associates, his age, his country of origin, or other biographical details. (This was true even before the PATRIOT Act became law, incidentally.) Second, investigators still must comply with the bedrock requirement that they establish, to the satisfaction of the FISA court, probable cause to believe that the person to be surveilled is a foreign power or an agent of a foreign power.[22] They also must demonstrate probable cause that each of the "facilities or places" to be monitored "is being used, or is about to be used," by a foreign power or agent.[23] Nothing in PATRIOT did away with these basic rules.

Third, any risk of overcollection – i.e., the possibility that investigators might inadvertently intercept communications involving innocent third parties – is mitigated by FISA's minimization requirement: Investigators must follow a rigorous set of procedures that "minimize the acquisition and retention, and prohibit the dissemination," of Americans' private data.[24] Fourth, the active involvement of the FISA court stands as a significant bulwark against any misuse. Not only does the court provide oversight before any surveillance is approved, in the form of ex ante judicial review. It also provides ongoing oversight while the surveillance is taking place: Investigators who operate a roving wiretap must alert the FISA court no more than ten days after they begin monitoring any new facility, and they must explain the "facts and circumstances" that justify their "belief that each new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by the target."[25] The combination of these safeguards should adequately ensure that roving wiretaps do not infringe upon important privacy interests.

II. Business Records

Section 215 of the PATRIOT Act – the so-called "business records" provision – authorizes the national security equivalent of grand jury subpoenas. Criminals often leave behind trails of evidence in their everyday interactions with banks, credit card companies and other businesses. Federal grand juries routinely issue subpoenas to these entities in investigations that range from narcotics crimes to health care fraud. When a subpoena is issued, the recipient is required to turn over "any books, papers, documents, data, or other objects the subpoena designates."[26] The recipient must do so whenever there is a "reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation."[27]

---

[21] *Id*. § 1804(a)(2).

[22] *Id.* § 1805(a)(2)(A).

[23] *Id.* § 1805(a)(2)(B).

[24] *Id.* § 1801(h).

[25] *Id.* § 1805(c)(3).

[26] Fed. R. Crim. Pro. 17(c)(1).

[27] United States v. R. Enterprises, Inc., 498 U.S. 292, 301 (1991).

The PATRIOT Act amended FISA to establish a comparable mechanism for national security investigators to obtain the same sorts of materials. In particular, the FISA court may issue an order that directs a third party to produce "any tangible things (including books, records, papers, documents, and other items)."[28] To obtain such an order, the government must establish "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation."[29] (This is virtually identical to the standard that applies in the grand jury context; the Supreme Court has held that a subpoena is valid if there is a "*reasonable possibility*" that it will result in relevant information.[30]) In addition, agents must comply with a detailed set of minimization procedures that restrict the retention and distribution of private data about innocent Americans.[31] Once again, the basic idea behind this provision is to level the playing field. If officials investigating drug dealers and crooked insurance companies can subpoena business records, then officials investigating international terrorists should be able to as well.[32]

Like other parts of the PATRIOT Act, the business records provision features an extensive set of protections. In fact, there are several respects in which section 215's safeguards are even stricter than those that apply in the grand jury context:

- First, the PATRIOT Act has a narrower scope. Section 215 may only be used in national security investigations,[33] whereas a grand jury can issue a subpoena "merely on suspicion that the law is being violated, or even just because it wants assurance that it is not."[34]

- Second, PATRIOT provides for ex ante judicial review; investigators cannot acquire business records unless they first appear before the FISA court and convince it that they are entitled to them.[35] Grand jury practice is very different. Although subpoenas *in theory* are issued in the name of the grand jury and the overseeing court, *in practice* they are issued more or less unilaterally by Assistant U.S. Attorneys; judicial review does not occur until after the subpoena has issued, if at all.[36]

---

[28] 50 U.S.C. § 1861(a)(1).

[29] *Id.* § 1861(b)(2)(A).

[30] *R. Enterprises*, 498 U.S. at 301(emphasis added); *see id*. at 297 (stressing that "the Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists").

[31] 50 U.S.C. § 1861(g).

[32] The pre-PATRIOT version of FISA's business records authority was considerably narrower than the grand jury rules. It only applied to certain types of entities (such as airlines, hotels, and car rental companies), and it was only available when investigators established "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272 § 602, 112 Stat. 2396, 2410-12 (1998). The PATRIOT Act brought FISA closer in line with grand jury practices.

[33] 50 U.S.C. § 1861(a)(1).

[34] United States v. Morton Salt, 338 U.S. 632, 642-43 (1950).

[35] 50 U.S.C. § 1861(c).

[36] Fed. R. Crim. Pro. 17(c)(2) ("On motion made promptly, the court may quash or modify the subpoena if compliance would be unreasonable or oppressive.").

- Third, the PATRIOT Act requires minimization, thereby protecting the privacy of innocent Americans[37]; the grand jury rules do not.

- Fourth, the PATRIOT Act forbids the government from investigating an American "solely upon the basis of activities protected by the first amendment to the Constitution."[38] The grand jury rules offer no such guarantee.

- Fifth, PATRIOT offers heightened protections when investigators seek materials that are especially sensitive, such as medical records and records from libraries or bookstores.[39] (This provision was added in 2006.[40]) The grand jury rules lack any comparable restrictions.

- Finally, PATRIOT provides for robust congressional oversight: The government must "fully inform" the House and Senate Intelligence Committees, as well as the Senate Judiciary Committee, concerning "*all*" uses of this provision.[41] The grand jury rules contain no such notification requirement.

The constitutional principles concerning government access to third party records have been settled for decades, and these precedents strongly support the PATRIOT Act's business records authority. A long line of Supreme Court case law confirms that there is no "reasonable expectation of privacy"[42] in the information a person conveys to businesses and other third parties. As a result, the government's efforts to acquire such data – as with grand jury subpoenas, for example – do not amount to "searches" within the meaning of the Fourth Amendment. Investigators therefore need not secure a warrant or demonstrate probable cause. For instance, in the 1979 case *Smith v. Maryland*,[43] the Supreme Court ruled that police officers' use of a pen register – which records the numbers dialed by a particular telephone, but not the content of the resulting conversations – did not require a warrant or probable cause. "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[44] A few years earlier, in *United States v. Miller*,[45] the Court similarly ruled that police could obtain a person's financial records from a bank without a warrant or probable cause. According to the Court, "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government

[37] 50 U.S.C. § 1861(g).

[38] *Id.* § 1861(a)(1).

[39] *Id.* § 1861(a)(3).

[40] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 § 106(a)(2), 120 Stat. 192, 196 (2006).

[41] 50 U.S.C. § 1862(a) (emphasis added).

[42] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

[43] 442 U.S. 735 (1979).

[44] *Id*. at 743-44.

[45] 425 U.S. 435 (1976).

authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[46] If mere relevance is all that's required to obtain business records in ordinary criminal investigations, it is not readily apparent why something more than that should be required to obtain the same materials in national security investigations.

Section 215 isn't just known as the "business records" provision, of course. It's also known, unflatteringly, as the "libraries" provision. Section 215 isn't aimed at libraries, and the Justice Department has indicated to Congress that the provision has never been used to obtain library or bookstore records.[47] While section 215 conceivably might be applied to libraries or bookstores, it isn't unique in that respect: It's not unusual for grand juries to demand library records in regular criminal cases. For instance, during the Unabomber investigation, grand juries issued subpoenas to a half dozen university libraries; investigators wanted to know who had checked out various works that were cited in the "Unabomber Manifesto."[48] In the 1990 Zodiac gunman investigation, a New York grand jury subpoenaed records from a Manhattan library. Investigators believed that the gunman was inspired by a Scottish occult poet, and wanted to learn who had checked out his books.[49] In the 1997 Gianni Versace murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach.[50] The Iowa Supreme Court even upheld the use of library subpoenas in an investigation of cattle mutilations.[51] If libraries and bookstores aren't exempt from grand jury subpoenas in ordinary criminal cases, there is no obvious reason to exempt them from business records orders in terrorism cases – especially since the PATRIOT Act offers even more robust protections than the grand jury rules.

III. Lone Wolf

The third provision that is up for renewal this year is known as the "lone wolf" fix. (Note that lone wolf wasn't part of the PATRIOT Act. Congress adopted it in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), and also subjected it to PATRIOT's sunset provision.[52]) As a result of this measure, counterterrorism investigators may obtain the FISA court's approval to conduct electronic surveillance of certain international terrorists even if there is not yet enough evidence to formally link them to a foreign terrorist organization.

Two distinct yet related policy considerations suggest a need for lone wolf surveillance. First, there's the evidentiary problem. It may be difficult for investigators to establish that a given suspect is a member of, or otherwise has ties to, a foreign terrorist organization. The

---

[46] *Id*. at 443.

[47] CRS Report for Congress, *USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis* 4-5 n.18 (Dec. 21, 2006).

[48] *Library Records Led to Break in Unabomber Case*, NPR, June 2, 2005.

[49] Eric Lichtblau, *Libraries Say Yes, Officials Do Quiz Them About Users*, N.Y. TIMES, June 20, 2005.

[50] Al Baker & Soraya Sarhaddi Nelson, *Death & Drama / Cops: Body on Fla. Houseboat Looks Similar to Cunanan*, NEWSDAY, July 24, 1997.

[51] Brown v. Johnston, 328 N.W.2d 510 (Iowa 1983).

[52] Pub. L. No. 108-458 § 6001(a), (b), 118 Stat. 3638, 3742 (2004).

problem is likely to be especially acute during the early stages of an investigation, when agents are just beginning to assemble a picture of the target's intentions. According to the 9/11 Commission, the FBI faced this predicament in the weeks before 9/11. Agents believed that Zacarias Moussaoui – then in federal custody on immigration charges – was a terrorist.[53] Among other reasons for their suspicions, Moussaoui had paid cash at a flight school to learn how to fly a Boeing 747 jumbo jet, but he had no interest in becoming a commercial pilot. Investigators hadn't yet connected Moussaoui to any foreign terrorists, so it was unclear whether they could use FISA to search his apartment or laptop.[54] The 9/11 Commission later speculated that, if agents had investigated Moussaoui more fully, they might have unraveled the entire September 11 plot.[55]

Second, there's the growing danger of entrepreneurial terrorism. As Homeland Security Secretary Janet Napolitano warned last month, "[t]he terrorist threat facing our country has evolved significantly in the last 10 years – and continues to evolve"; we now "face a threat environment where violent extremism is not defined or contained by international borders."[56] Solitary actors who are inspired by foreign terrorist organizations like al Qaeda, or radical clerics like Anwar al-Awlaki, are capable of causing just as much death and destruction as those who are formally members of such networks. Indeed, some of the most chilling terrorist plots to emerge in recent years have involved operatives who may have been acting on their own, not at the direction of an overseas group. In November 2009, U.S.-born Army physician Nidal Malik Hasan opened fire on dozens of unarmed soldiers at Fort Hood, Texas, wounding 32 and killing thirteen.[57] In late February, a Saudi student named Khalid Aldawsari was arrested after planning to bomb the homes of former president George W. Bush and several soldiers who had served at Abu Ghraib prison in Iraq.[58] This trend toward entrepreneurial terrorism is on the rise and shows no signs of abating. (Candidly, the lone wolf provision could not be used to investigate all of these plots. A number of solitary terrorists are U.S. citizens or lawful permanent resident aliens, and the present version of lone wolf does not apply to them.[59])

The lone wolf fix helps investigators overcome these evidentiary difficulties, and meet this evolving terrorist threat, through a simple change to the Foreign Intelligence Surveillance Act. In particular, FISA provides that agents may not conduct surveillance unless they persuade the FISA court that there is probable cause to believe that the target is a "foreign power" or an "agent of a foreign power."[60] Lone wolf tweaked the latter definition. The term "agent of a

---

[53] NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 273 (2004).

[54] *Id.* at 276.

[55] *Id.*

[56] Keith Johnson, *Officials Warn of Domestic Terrorism Threat*, WALL ST. J., Feb. 10, 2011.

[57] Richard A. Serrano, *Failures by FBI, Pentagon Contributed to Ft. Hood Massacre, Report Says*, L.A. TIMES, Feb. 3, 2011.

[58] Peter Finn, *FBI: Saudi Student Bought Materials for Bomb, Considered Bush Home as Target*, WASH. POST, Feb. 25, 2011.

[59] 50 U.S.C. § 1801(b)(1).

[60] *Id.* § 1805(a)(2).

foreign power" has always included a non-American who is a "member" of "a group engaged in international terrorism or activities in preparation therefor."[61] Now, the term also includes a non-American who "engages in international terrorism or activities in preparation therefor."[62] As a result of this change, investigators may obtain a FISA court order to monitor any target who is engaging in international terrorism. There is no longer any need to make the additional showing that he is acting on behalf of a foreign terrorist organization. Note that this authority has a critical restriction: It does not apply to United States persons – i.e., persons who are either U.S. citizens or lawful permanent resident aliens. Americans cannot be surveilled under the lone wolf provision as it currently stands.[63]

As with the other two authorities that are up for reauthorization, lone wolf features important protections for privacy and civil liberties. Chief among them is the requirement of ex ante judicial approval. FBI agents cannot start monitoring a suspected lone wolf on their own; they must appear before the FISA court and convince it to authorize the surveillance.[64] Second, lone wolf still requires investigators to establish that a given target has a foreign nexus. The tool can only be used to investigate people who are engaging in "*international* terrorism."[65] This means it must be shown, among other things, that the suspects' activities involve "violent acts or acts dangerous to human life" that either "occur totally outside the United States" or "transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate."[66] Lone wolf thus cannot be used to investigate persons suspected of engaging in domestic terrorism.[67] Finally, FISA's minimization requirement applies to lone wolf surveillance, offering protection to the innocent Americans with whom the lone wolves come into contact.[68]

* * *

The terrorist threat isn't going away anytime soon. Al Qaeda and its followers are still mortal dangers to Americans at home and abroad, and Congress should make sure that our counterterrorism agents have the tools they need to detect and disrupt our enemies' bloody plots. This is no time to dismantle the USA PATRIOT Act. The three provisions that are on the verge of expiring – roving wiretaps, business records, and lone wolf – have been on the statute books for years without compromising vital privacy interests or civil liberties. Not only does the PATRIOT Act let counterterrorism agents use some of the same investigative techniques that

[61] *Id.* § 1801(a)(4), (b)(1)(A).

[62] *Id.* § 1801(b)(1)(C).

[63] *Id.* § 1801(b)(1).

[64] *Id.* § 1805(a).

[65] *Id.* § 1801(b)(1)(C) (emphasis added).

[66] *Id.* § 1801(c)(1), (3).

[67] *Cf.* United States v. United States District Court ("Keith"), 407 U.S. 297, 309 n.8 (1972) (using the term "domestic organization" to refer to "a group or organization (whether formally or informally constituted) composed of citizens of the United States and which has no significant connection with a foreign power, its agents or agencies").

[68] 50 U.S.C. § 1801(h).

regular cops and prosecutors have had in their arsenal for years. The act's safeguards and protections are at least as robust as – and in some cases are even more robust than – their law enforcement counterparts. Congress should promptly reauthorize these authorities before they sunset later this year.

Al Qaeda hasn't given up. We can't afford to either.