LD Nationals 2014
Aff Analysis

This year's LD Nationals topic is **Resolved: The United States ought to prioritize the pursuit of national security objectives above the digital privacy of its citizens**. Today, we're going to discuss some options for building a case strong enough to withstand the rigors of national competition!

We'll start out with an investigation of some key terms.

If you've made it this far, I'm sure you're experienced in debating "**prioritize**," so I won't waste much space discussing it here. As a reminder, though, "prioritize" does not mean the two imperatives are wholly mutually-exclusive, or that digital privacy is always bad. Instead, you just need to win that national security is of greater importance, when the two are compared. Or, you can argue that "prioritize" means national security comes first, then we move on to privacy. Either way, you aren't responsible for claiming that national security justifies *unlimited* privacy violations, or that privacy is not important at all.

National security is the next important phrase in the resolution. There is no universally agreed-upon or legal definition of national security, but chances are you have a good intuitive idea of what it means. If you're interested in providing a specific interpretation, Wikipedia offers links to a range of definitions. You can select the one that best suits your individual case.

From a strategic standpoint, we should note that the phrasing of this resolution does not mandate that the affirmative win *that any particular national security initiative(s) achieve(s) solvency*. The resolution

says "the PURSUIT of" national security objectives should be prioritized over digital privacy. So, you are only responsible for defending that national security is a more pressing objective than digital privacy, not that *any specific policy is actually successful* at achieving national security. Of course, you may decide that you want to defend one or more existing (or potential) policy initiatives. That is your prerogative. However, be aware that if the negative makes arguments like "NSA surveillance is ineffective" you have the option to argue that the success or failure of a particular program is irrelevant to the *fundamental question of which objective ought to be prioritized*. This will probably become very strategically useful in some of your debates.

Digital privacy is another phrase from the resolution that lacks any universal definition. However, it generally means privacy in electronic communications, particularly those that pertain to personal identity. You may want to familiarize yourself with general privacy rights in the United States and apply this understanding to digital technologies. Because of the connotations of "digital," you should plan on the core of this topic involving discussions of the internet, smart phones, cloud computing, data surveillance, etc. Be aware that there will be some differences between how we understand privacy rights as they relate to our physical property (such as a home search) and digital communications. The differences and similarities here have yet to be fully fleshed out by any branch of government, or society in general (hence the reason we're having these debates).

The phrasing of this resolution refers to "digital privacy OF ITS CITIZENS," with "its" referring to "the United States." Additionally, the clash between digital privacy and national security implies a government perspective, since governments are the actors who must concern themselves with national security. When we consider these two factors together, we can see that we are discussing *American programs that affect Americans* (as opposed to USFG surveillance targeting foreign actors). Although this isn't explicitly required by the resolution, most debates will probably focus on American government efforts, although the actions of domestic corporations may also become somewhat relevant.

At this point, you're probably inferring that many debates will involve discussions of the **NSA, its PRISM program, FISC, etc**. Although this resolution is really written to invite conceptual discussions of the clash

between privacy and security, these relevant, material examples will still certainly play into many of your rounds. It would thus be helpful to familiarize yourself with background information on these topics.

You are encouraged to do more thorough research, but here are a few highlights of what you need to understand:

- The Obama administration claims PRISM cannot be used to monitor domestic targets without a warrant.
- The stated goal of this program is not to monitor domestic communications. However, the NSA is permitted to keep American communications where they intersect with foreign targets, if they contain intelligence material or evidence of a crime, or if they are encrypted.
- The two bullets above, together, establish that while the NSA is NOT authorized to conduct warrantless surveillance on an American citizen residing inside the United States. However, they ARE authorized to keep and use any data created by an American citizen residing inside the United States that is "swept up" during their surveillance operation targeting a foreign target. So, for example, if you make a phone call to a foreign citizen subject to NSA surveillance, the metadata related to that call may be investigated by the NSA.
- The data collected is referred to as "metadata" because, according to the NSA, it does not trawl data for the *contents* of the communications, but rather looks at factors like who is being contacted, the number/frequency of communications, etc. So, it concerns itself with *who* someone talks to, *when*, and *how often*, rather than *what they say*.
- The NSA stores this metadata (for 5 years, according to popular understanding) and can obtain a warrant to use it for an investigation. It receives these warrants from a secretive federal court called FISC (also sometimes called FISA Court).
- Knowledge of these programs became public when documents were leaked by former contractor Edward Snowden and published by journalist Glenn Greenwald. Release of new information is ongoing, and Greenwald says we have not yet received the most shocking news. He expects this release will come in June or July of 2014, so keep your eyes on the news as you prep for Nationals.

You may also find this timeline of United States surveillance programs helpful.

However, although these US government programs are heavily tied-up in popular discussions of digital privacy versus security, remember that this resolution is fundamentally asking you to debate about *principles*, not the mechanics of specific programs.

Obviously, the core clash of this topic is the classic debate of **liberty versus security**. How much privacy are we willing to give up in order to ensure physical security? This has been a complicated question since the founding of the Republic, and oceans of ink have been spilled on the subject. So, you should have no trouble finding vast amounts of high-quality cards. I will not provide you with any of these generic liberty/security cards here, because you probably already have them. Below, I will give you some cards that address this issue specifically from the context of American digital surveillance.

Many debates will focus on **terrorism**, because combatting terrorism is at the center of America's current national security efforts. Preventing terrorist attacks is also the stated primary purpose of most digital surveillance programs. However, any problem or conflict that could represent a threat to United States national security is fair game on this topic. For example, you may also want to talk about the threat of hackers, cyber warfare, etc.

Here is **evidence** claiming digital surveillance halts terrorism:

> *(Josh Gerstein, legal/national security reporter, Politico, "NSA: PRISM stopped NYSE attack," http://www.politico.com/story/2013/06/nsa-leak-keith-alexander-92971.htm,l June 18 2013)*
>
> Recently leaked communication surveillance programs have helped thwart more than 50 "potential terrorist events" around the world since the [9/11] attacks, National Security Agency

> Director Keith Alexander said Tuesday. Alexander said at least 10 of the attacks were set to take place in the United States, suggesting that most of the terrorism disrupted by the program had been set to occur abroad. The NSA also disclosed that [C]ounterterrorism officials targeted fewer than 300 phone numbers or other "identifiers" last year in the massive call-tracking database secretly assembled by the U.S. government. Alexander said the programs were subject to "extraordinary oversight." "This isn't some rogue operation that a group of guys up at NSA are running," the spy agency's chief added. The data on use of the call-tracking data came in a fact sheet released to reporters in connection with a public House Intelligence Committee hearing exploring the recently leaked telephone data mining program and another surveillance effort focused on Web traffic generated by foreigners. Alexander said 90 percent of the potential terrorist incidents were disrupted by the Web traffic program known as PRISM. He was less clear about how many incidents the call-tracking effort had helped to avert. Deputy FBI Director Sean Joyce said the Web traffic program had contributed to arrests averting a plot to bomb the New York Stock Exchange that resulted in criminal charges in 2008. Joyce also indicated that the PRISM program was essential to disrupting a plot to bomb the New York City subways in 2009 and 40 potential cyber attacks in the years 2001-2009. "Without the [Section] 702 tool, we would not have identified Najibullah Zazi," Joyce said.

To really strengthen your terrorism-based contentions, you will want to be sure to read some impacts to terrorism. For example, terrorism leads to foreign wars, which cause more loss of life (empirically true); terrorism hurts the economy, which causes yet more problems (also empirically true); or terrorism leads to crackdowns on civil liberties (I'll give you evidence on this in a minute). Your friends in CX probably have loads of these cards, if you feel like asking for a favor. You can also consult the Open Evidence Project.

Now, here is some **evidence** that is particularly useful, because it directly compares the imperatives of privacy and security in the context of digital privacy:

> *(Neil C. Livingstone, terrorism & national security expert, board member for John P. Murtha Institute of Homeland Security and the International Institute for Homeland Security, PhD from the Fletcher School of Law & Diplomacy, The Economist, Debate on Privacy & Security, Proposition Opening Remarks, http://www.economist.com/debate/days/view/131#pro_statement_anchor, February 5 2008)*
>
> Today we face unprecedented security risks to our lives and the fragile infrastructures we depend on to sustain our livelihoods and well-being. Our enemies are far more sophisticated than the stereotype of a bearded jihadist toting an AK-47 hunkered down in the mountains of Pakistan or Afghanistan, an illiterate and superstitious Luddite eager to impose the nostrums and doctrines of the 7th century on the modern world.
>
> In reality, many jihadists are technologically sophisticated and linked together by the Internet, which they use to download information on our vulnerabilities and assist them in the design and construction of explosive devices and even chemical, biological and radiological weapons. And, as a Senate Permanent Subcommittee on Investigations report directed by former Georgia Senator Sam Nunn concluded, "It is not a matter of 'if' but rather 'when' such an event [chem, bio, or nuclear] will occur."
>
> In response to this very real and ongoing threat, the US government has taken a number of steps to monitor the activities, communications and movements of potential terrorists and other aggressors here and around the globe and to amass data, with the assistance of advanced information technologies, to authenticate and verify the identities of both citizens and non-citizens alike. The president has also signed a recent directive that expands federal oversight of internet traffic in an attempt to thwart potentially catastrophic attacks on the government's computer systems.
>
> We live in information-based societies and it is inevitable that law enforcement and security forces will utilise these technologies in an effort to better protect us from malicious actors. In Britain, closed-circuit television (CCTV) cameras are used to fight crime and have elicited little public concern or criticism. Authorities are also monitoring the internet more closely in an effort to curtail child pornography.

These actions are seen by some as an assault on privacy and a reduction of personal freedom, yet few would suggest that authorities be barred from access to such data.

In a 1902 case, Judge Alton B. Parker noted, "The so-called right of privacy is, as the phrase suggests, founded upon the claim that a man has the right to pass through this world, if he wills, without having his picture published, his business enterprises discussed, his successful experiments written up for the benefit of others, or his eccentricities commented upon either in handbills, circulars, catalogues, periodicals or newspapers."[2]

Such a view, however, is quaint and unsuited to contemporary times. Does it mean that a man should not have his business enterprises discussed if he is making dangerous products or evading his taxes? More to the point, what if a bank is laundering money to facilitate terrorist attacks? And should a person's "eccentricities" be overlooked if they include bomb building or, on a more domestic level, the dissemination of predatory child pornography?

Americans have no expectation of complete privacy. The Constitution does not explicitly grant or even address the right of privacy. It is what an Economist article describes as a "modern right", not mentioned by 18th-century revolutionaries in their lists of demands or even "enshrined in international human-rights laws and treaties until after the second world war".[3] The Declaration of Independence, on the other hand, states without equivocation that every man is entitled to "life, liberty, and the pursuit of happiness". Note that life is the pre-eminent value. Above all else, it is for the protection of the lives of its citizens and their cherished freedoms, that the government has undertaken some of the steps that might be considered as intrusions on privacy.

We submit to checks of our baggage and person in order to board an aircraft, and most of us do so with little complaint, despite the inconvenience, because we want to arrive safely at our destinations. Likewise, most Americans are not terribly concerned by warrantless wiretaps of terrorist suspects, because they believe that their security and that of their families depends on aggressive measures by the government to combat terrorism.

The current debate over privacy is, in many ways, specious, and it has become a cliché , as T.A. Taipale has written, "that every compromise we make to civil liberties in the 'war on terrorism' is itself a victory for those who would like to destroy our way of life".[4]

While most Americans have an expectation of privacy in their own homes, especially in terms of their intimate relations, the current debate does not revolve around such issues. Rather it

concerns technologies that are, in most respects, public, where there is no presumption of privacy in a traditional sense.

Airline travel, the use of telephones and access to the internet are not rights, rather they are privileges and, as such, they are very much public activities and endeavours. Accordingly, some level of government oversight is not unreasonable in order to maintain the integrity of the systems that underpin such technologies and to prevent them from being used to harm others.

If someone wants to opt out and not be subject to government scrutiny, he or she can forgo airline travel, the use of the telephone and the internet, and even personal identification and credit cards. I would even be willing to implement a two-tier security system at the airport which has one line for flyers who voluntarily surrender some personal data and perhaps even a biometric in order to expeditiously pass through security and a second line for those desiring anonymity, who therefore will be subjected to a complete and thorough search of their person and luggage.

The great civil libertarian and Supreme Court Justice Hugo L. Black wrote that, "I like my privacy as well as the next one, but I am nevertheless compelled to admit that government has a right to invade it unless prohibited by some specific constitutional provision."[5] Our Constitution clearly protects us from egregious violations of our rights and I fully embrace appropriate measures to ensure that government does not abuse its power. At the same time, Americans are a pragmatic and commonsense people who understand that there are few, in any, absolutes in life and that their privacy is not being unreasonably eroded by efforts taken to ensure their security and prevent terrorist and other malicious attacks. They believe, moreover, that the first obligation of government is to protect its citizens, and are willing to grant authorities a measure of latitude in this task.

The above card makes a couple of significant points:

- America's enemies are sophisticated and threatening, seeking to use weapons of mass destruction against us. This high threat level justifies giving up some small measures of privacy.
- These privacy sacrifices are minor and don't really matter very much to begin with.
- Americans have no expectation of total privacy. We tolerate this sort of calculated giving up of privacy on numerous other fronts, such as TSA security measures throughout airline travel and closed-circuit video cameras to prevent crime. Few would disagree that this is the correct choice. Why is digital surveillance different?
- Life is the most foundational value. We cannot care about our privacy if we are dead.
- The internet is a privilege, not a right, and internet usage is an inherently public activity. An internet user should not expect full privacy. If you're not comfortable with this, you can choose to opt out of online endeavors.
- The constitution protects Americans against the most egregious violations of privacy, so there is no "slippery slope."

Here's more **evidence**:

> *(Neil C. Livingstone, terrorism & national security expert, board member for John P. Murtha Institute of Homeland Security and the International Institute for Homeland Security, PhD from the Fletcher School of Law & Diplomacy, The Economist, Debate on Privacy & Security, Proposition Rebuttal, http://www.economist.com/debate/days/view/132#pro_statement_anchor, February 8 2008)*
>
> My honourable opponent, Mr Barr, has offered up a great many generalisations about privacy that may be fine in theory but which have little application in the modern world. Like Mr Barr, I believe that privacy is a basic right that should be supported to the extent possible, but whereas he regards privacy as underpinning all other rights, I view it as one of the benefits of a secure nation capable of successfully thwarting foreign assaults by those who neither share our values nor subscribe to our democratic principles.
>
> In other words, if you have little security you most assuredly will have little privacy, for privacy is one of the benefits of a secure society, just like political freedom. Any people who live in constant fear and trepidation are unlikely to place great value on abstract rights like privacy and

freedom. Adlai E. Stevenson observed: "A hungry man is not a free man." Well, Mr Barr, neither is a frightened man.

The right to privacy, moreover, does not mean that every man can live completely apart from society, anonymous and uncounted like Thoreau at Walden's Pond, free from any obligations to the welfare of his or her fellow citizens. As I suggested in my opening remarks, we may no longer consistently avoid the notice of others simply by minding our own business; the contemporary world is just too complicated for that and the threats too serious. We may offer nonconformists some anonymity so long as they don't try to board an airplane, use the internet, or pay for a purchase with a credit card. But it is not too much to ask that every citizen have some form of secure personal identification. This is critical to an orderly and smoothly functioning society, and not only helps in the fight against terrorism but is the key to halting illegal immigration.

Mr Barr argues that it is a suspension of common sense that the so-called "good guys" must be profiled to discover the "bad guys". But what is he suggesting? That we should forgo any effort to collect data about airline passengers because we will necessarily accumulate more data about non-terrorists than terrorists, given that there are tens of millions of ordinary flyers compared with only a handful of terrorists? Our task is to differentiate between malicious actors like terrorists and criminals and the great mass of ordinary humans who simply want to go about their activities free from the threat of being mugged, robbed, defrauded, sexually assaulted, hijacked, maimed or killed in a terrorist blast, or harmed in some other way. Most citizens are willing to permit governments, in the words of K.A. Taipale, to employ "advanced information technologies to help identify and find actors who are hidden among the general population and who have the potential for creating harms of such magnitude that a consensus of society requires that government adopt a preventative rather than reactive approach".[1]

Mr Barr also contends that "In this universe, every person—neighbour, co-worker, fellow passenger—is and will remain a potential terrorist." In reality, the truth is precisely the opposite. The use of advanced information technologies will enable us to draw distinctions between ordinary law-abiding citizens and what Mr Barr refers to as the "bad guys". Scarce resources can then be focused on potential suspects rather than on the broad masses. Once this is accomplished, our safety, as well as our privacy, can be better preserved.

Barr further asserts that "You will find terrorists, if at all, by gathering good intelligence, and by adhering to sound intelligence and law enforcement techniques." I concur, but what does he think these "techniques" consist of? I certainly hope he is not advocating a return to the naive period characterised in US Secretary of State Henry L. Stimson's famous remark that

"Gentlemen do not read each other's mail." It was because of short-sighted men like Mr Stimson that little more than a decade later the US suffered the Japanese sneak attack at Pearl Harbor, in large part because the US had no real intelligence service and was reluctant to employ modern technologies to monitor potential challenges from abroad.

The advent of modern terrorism and the existence of chemical, biological and nuclear threats make it impossible to consider concepts like privacy in the framework of old laws and attitudes. At the same time, we should not make a fetish out of security or the new technologies on which it depends. But neither should we ignore these technologies because we are afraid they might be misapplied or misused. Today, for example, we utilise modern information technologies to protect our societies and keep track of terrorists and other malefactors. This includes the use of surveillance cameras, access to major databases, telephone and email intercepts, and various methodologies for authenticating identity. Protecting privacy in this era calls for appropriate rules and regulations to ensure that such information is not used promiscuously or out of context, and there must be independent government oversight by, in the US, the Congress and the courts.

It is absolutely incumbent on us that we protect our societies and promulgate a sense of security among our citizens, for not only do we face unparalleled threats from abroad, but it should be remembered the tyrant always comes in the guise of the protector. The first duty of government is to protect its citizens and if it fails this test then all of our other rights and privileges, including privacy, will soon be under assault. Rather than railing against technological intrusions on privacy, Mr Barr should recognise that these same technologies may, in the end, reinforce privacy in the modern world. In other words, by contributing to the security of modern societies, new information and surveillance technologies may actually do more to promote privacy than to diminish it.

The above card establishes that, especially in the context of terrorists capable of wreaking great devastation on society, security is a prerequisite to privacy:

- First, because people are not inclined to care about their privacy when their lives are imminently threatened.
- Second, because governments do a poor job of protecting civil liberties during environments of crisis.
- Third, because a successful terrorist attack would likely create a backlash that would crack down on privacy even more (the passage of the PATRIOT Act is a good empirical example here).
- Finally, because the widespread usage of digital surveillance technologies may actually free us from the necessity of other, more intrusive forms of surveillance, such as the monitoring of our physical person.

Each of these points represents a strategically useful piece of defense against common negative arguments.

Here's yet more **evidence** supporting that idea that eliminating digital surveillance would lead to terrorist attacks and worse invasions of privacy:

> *(Marshall Honoroff, contributing writer, Tom's Guide, "How the NSA's spying keeps you safe," http://www.tomsguide.com/us/nsa-spying-keeps-safe,review-1899.html, September 12 2013)*
>
> While this anger is both understandable and justifiable, relatively few people have stopped to consider the other side of the coin. You can have total privacy or total national security, but you cannot have both. A modern democratic society requires a compromise between the two extremes. The most important thing to keep in mind is that there is, at present, absolutely no indication that the NSA has done anything illegal or outside the parameters of its mission statement. The NSA monitors external threats to the U.S., and, in theory, does not turn its attention to American citizens without probable cause. There is no evidence to the contrary among the documents that Edward Snowden leaked. Terrorist threats "How do we protect our nation? How do we defend it?" asked Gen. Keith Alexander, the NSA's director, at the Black Hat 2013 security conference, held in Las Vegas in July. "[This information] is not classified to keep it from you: a good person. It's classified because sitting among you are people who wish us harm." While the thought of the NSA controlling every bit of information that the average

> American citizen posts online is disconcerting, Alexander maintained that a terrorist attack is even worse for a country's basic freedoms. "What we're talking about is future terrorist attacks," Alexander said, discussing a number of planned attacks that the NSA foiled over the last 10 years. "It is worth considering what would have happened in the world if those attacks — 42 of those 54 were terrorist plots — if they were successfully executed. What would that mean to our civil liberties and privacy?" James Lewis, a researcher at the Center for Strategic and International Studies, agrees. "The NSA said there were 54 cases where they were able to detect plans and stop them, and 50 of them led to arrests," Lewis told Tom's Guide. "Fifty doesn't sound like a lot compared to the number of records [the NSA collected], but would you have preferred to have 50 more Boston bombings?"

The above evidence also contains the claim that the NSA's actions are legal and without the bounds of their mission statement. Again, you may or may not choose to defend the NSA's specific programs. You always have the option to say "even if they win that [specific program] is ineffective/illegal/bad, I will still win that national security in general is more important than digital privacy." If you do want to defend PRISM or other programs, though, you will want to familiarize yourself with the legislation and judicial rulings which determined these programs were legal. Make sure you do your research!

Another defensive argument you may want to advance against neg privacy impacts is that **people choose to post personal data all over the internet anyway**. This argument corresponds to the reality most of us experience every day. People post detailed personal information all over Facebook, Twitter, Tumblr, etc. They constantly and publically share what products, services, and ideas they like or dislike across a variety of platforms. They agree to sign into a multitude of services using Facebook, indicating they are ok with entities storing and accessing enormous stores of detailed data about them, linked to a personal profile. Most of this information is more personal than the metadata collected by surveillance programs. Moreover, it's generally posted totally voluntarily, and becomes completely public, accessible by anyone. You can argue that it makes no sense to be ok with this, but scandalized by the NSA being able to look at who you called and when.

You should also be prepared for the possibility that you will need to **answer a security kritik** (a criticism of the concept of national security). The specifics of how you combat this position will depend upon the

exact arguments made by the negative as well as content of your case, but, on a basic level, you will want to win that A) threats are real and B) we ought to attempt to prevent them. If you have built a strong case, your value and criterion should be set up to help you with this. For example, you may have already built up arguments encouraging the judge to evaluate the round through consequentialism, with protecting human life as the most important measure of success. However, keep in mind that many security K positions will say that threat construction is a self-fulfilling prophecy. In other words, they'll argue that the only reason we experience threats is because we establish the conditions for them through our obsession with national security (for example, by engaging in preemptive warfare, which angers others). You can answer this in a variety of ways; one good argument is that concern with self-preservation is inevitable, and digital surveillance is less intrusive and therefore less likely to provoke backlash than other possibilities for combatting terrorism/other threats. This is supported by the cards above. You may also want to grab some cards from the security K answers files on the Open Evidence Project.

One last thing: as you've probably already figured out, this topic is extremely similar to the November 2013 Public Forum topic. Although they demand slightly different focuses, you may still find our guides to the NSA surveillance PF resolution helpful. Check them out: pro and con.

Of course, you should not feel confined to what is written here. Get creative! There are a tremendous amount of tricky, interesting arguments out there for you to explore. This is only meant as an introduction to help you find your "sea legs" on this topic.

Now you should be ready to go to go toe-to-toe with top debaters from around the country. Don't forget to thank Debate Central in your acceptance speech when you win Nationals! ;)

As always, you can email completed cases to **Rachel.Stevens@NCPA.org** for a free case critique. You can also join the discussion in the comments below. Good luck!