Last week, we discussed the PRO side of the current Public Forum resolution, **Resolved: The benefits of domestic surveillance by the NSA outweigh the harms**. The reasons, including national security and relative risk, cast an important light on this recent controversy. Today, we're providing a fuller picture by supplementing our initial analysis with a survey of probable CON arguments. We'll begin by defining the scope of current domestic surveillance,

Schoen, 2013 ["The Threat At Home -- The NSA And The "Golden Age of Spying"," Doug, Forbes Contributor and political strategist, Forbes.]
This is surely troubling. But newly disclosed documents ring perhaps even greater alarm bells. These documents reveal that NSA is guilty of extreme hacking themselves. The NSA is winning its long running war on encryption: it has circumvented or cracked majority of the digital scrambling that guards global commerce and banking systems. This includes data like trade secrets, medical records, emails, telephone conversations and online chats. The highly classified program, Bullrun, is one of the NSA's closest guarded secrets – or was until Edward Snowden leaked details of NSA programs that majority of Americans, as well as Congressional representatives, had no idea were in effect. According to the NY Times, the NSA hacked into target computers to snare encrypted messages before they were encrypted. And in some cases, companies have reported that the government coerced them into handing over their master encryption keys or building in a back door. "For the past decade, N.S.A. has led an aggressive, multipronged effort to break widely used Internet encryption technologies," said a 2010 memo describing a briefing about N.S.A. accomplishments for employees of its British counterpart. "Cryptanalytic capabilities are now coming online. Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable." Exploitable? While I understand the meaning in the memo, the use of the word "exploit" is all too apt for how I, and majority of Americans, feel about the NSA's overreaching and clear breaches of our Fourth Amendment rights. There is little doubt that there is more to this story and that Snowden's leak will be a slow drip that will continue to shed light on the true nature of the NSA and, indeed, the Obama administration that supports them in their endeavors. The President has his hands full with the impending conflict in Syria, the G-20 in Russia and his usual duties both domestic and international. But **it is crucial that he take this crisis with the NSA seriously. Their practices are truly un-American**. This hasn't gone unnoticed. Congressman Rush D. Holt, a New Jersey Democrat, has proposed legislation that would prohibit the NSA from installing "back doors" into encryption – a step in the right direction. Paul Kocher, a leading cryptographer, commented that, "the intelligence community has worried about 'going dark' forever, but today they are conducting instant, total invasion of privacy with limited effort. This is the golden age of spying."

Schoen paints a very different picture from many of the pro authors we surveyed last Thursday. By going into great detail about the extent of Bullrun, the previously-classified surveillance program that allows the NSA to monitor almost all domestic communication, he emphasizes the sheer size and extent of the incursion into Americans' privacy. He points out a few important aspects of the program, including the NSA's proclivity for pressuring companies into building backdoors into their code that the NSA can hack them (with what amounts to permission).

Schoen mentions that this trend is worrying because so many of us have long trusted companies with our material – in fact, many of these companies marketed how safe, secure, and private their networks were. The loss of that sense of security is more than uncomfortable – it raises concerns for the future of the 4th amendment to the Constitution and questions about whether a spying agency like the NSA can ever be trusted to be a benevolent force.

In our PRO analysis, however, we minimized this concern by mentioning that the NSA may collect information but much of it is of questionable use and very generic. Elizabeth Goitein argues that this is not so:

Goitein, 2013 ["The danger of American apathy on NSA surveillance," Elizabeth, codirector of the Liberty and National Security program at the Brennan Center for Justice at New York University School of Law, July 13, Christian Science Monitor.]
The programs also threaten Americans' privacy. It is disingenuous for officials to characterize the "metadata" being collected as mere phone numbers. Sophisticated computer programs can glean volumes of sensitive information from this metadata about people's relationships, activities, and even beliefs. The government knows very well how revealing call records can be; **that is why it considers the program so valuable**.

In essence, if these programs told the NSA nothing, they wouldn't bother with the time and expense of having them. This is a good rhetorical move for a CON speech – articulating that the more useful the PRO proves these programs are in finding information, the more intrusive they must be. The fact is, even generic data can tell the government an awful lot about people in this increasingly connected age – where they live, who they hang out with, what they do, and what they think. This information is more than the PRO would have you believe and arguably more worrisome.

Still, many argue that these programs are but a drop in the bucket – that is, despite domestic surveillance, America remains remarkably free in context. Goitein continues, questioning the veracity of this claim:

Goitein, 2013 ["The danger of American apathy on NSA surveillance," Elizabeth, codirector of the Liberty and National Security program at the Brennan Center for Justice at New York University School of Law, July 13, Christian Science Monitor.]
Serious as they are, these concerns fail to explain fully why Americans should care. After all, this remains a remarkably free country. There are exceptions. Muslim Americans, who are singled out for scrutiny by some law enforcement agencies, have reported harassment by customs officials as well as a chilling of political and religious activity. Outside of these communities, though, few Americans feel any tangible effects from increased surveillance. The vast majority of law-abiding citizens go about their lives without fear of government persecution. And that may be the problem. **Free societies tend to take their freedom for granted. But our liberties do not derive from the innate trustworthiness of our elected representatives**. They derive from laws and institutions put in place for the preservation of liberty. These laws and institutions, some version of which can be found in all democratic societies, are relatively recent innovations in human history. Before their advent, tyrannies and dictatorships were the norm. Even today, in countries without this framework, people are not free. Since 9/11, the laws and

institutions created to ensure Americans' freedom have been weakened – sometimes incrementally, **sometimes significantly** – at a rapid pace. This is particularly true for limitations on surveillance, a power that carries tremendous potential for abuse. National Security Letters, a form of administrative subpoena, are now available to collect any information "relevant" to a terrorism investigation, not just information about potential suspects. Customs agents no longer need reasonable suspicion of wrongdoing to search citizens' laptops at the border. Americans' international communications are now subject to wiretapping without an individualized court order. The list goes on. In any given instance, the government can make the case that the change is small, or that it is justified by increased security. In some cases, the argument may be persuasive. It is the trend, however, that should concern us. Twelve years after 9/11, as the nation approaches the date for withdrawing troops from Afghanistan, the quiet erosion of Americans' civil liberties continues. That doesn't mean the US government should never expand surveillance authorities, or that Americans should resolve all trade-offs between liberty and security in favor of liberty. After all, the United States is a long way from a dictatorship. But given the post-9/11 trend of diminishing legal protections, Americans should not make these choices lightly. And each additional **broadening of the government's powers must be a matter of choice – not passive acquiescence to a secret expansion. When that choice is taken from the citizenry, it is no occasion to "calm down" and look the other way**.

A few arguments here that you can you can use to answer PRO arguments that minimize the impact of NSA spying – including framework justifications.

1. **The insistence on how "free" we are even in the face of evidence to the contrary breeds complacency.** When we remind each other how "free" Americans are in other areas, Goitein argues, what we're really saying is that we shouldn't care about things like the NSA's domestic spying program because they could be much worse. This attitude is self-defeating and dangerous because it encourages us to turn our focus from ensuring we remain free to passively accepting policies that blatantly change that. This can pave the way for worse abuses in the future by fomenting a general climate of apathy toward expansive government. For debate context, voting for the PRO is much like this – saying that other concerns outweigh our freedom in even a single instance necessarily gives credibility to the idea that freedom can be bought or diminished without a cause for concern – which makes that opinion credible in the future.

2. **Liberty derives from hard-fought battles and is not freely given.** Our form of government, complete with its respect for individual freedom, is not the natural or original state of politics but rather the result of a long and rocky struggle for more and more liberty. Throughout history, abuses of power have been rampant and the impulse to extinguish them has not come without its costs – entire revolutions have been fought over things like these. Goitein's argument is that the existence of liberties is precarious (that is, people will always have an incentive to take it away from us and impose their will). Although the threats to liberty seem less credible now, not taking them seriously may jeopardize our progress in advancing and maintaining a free society. You can use this evidence to urge the judge to take the long view and argue that a large part of maintaining a free society is insisting, at every opportunity (including the debate round you're in) that liberty is important.

In essence, tolerance for even small incursions of liberty adds up. You should make a framing argument that the role of the judge is to reject every incursion on liberty because that is the only way to ensure the continued survival of s free society.

As Schneier points out,

Schneier, 2013 ["The NSA-Reform Paradox: Stop Domestic Spying, Get More Security," Bruce, Security and Technology correspondent for The Atlantic, September 11, The Atlantic.]
Regardless of how we got here, the NSA can't reform itself. Change cannot come from within; it has to come from above. It's the job of government: of Congress, of the courts, and of the president. These are the people who have the ability to investigate how things became so bad, rein in the rogue agency, and establish new systems of transparency, oversight, and accountability. Any solution we devise will make the NSA less efficient at its eavesdropping job. That's a trade-off we should be willing to make, just as we accept reduced police efficiency caused by requiring warrants for searches and warning suspects that they have the right to an attorney before answering police questions. We do this because we realize that a too-powerful police force is itself a danger, and we need to balance our need for public safety with our aversion of a police state. The same reasoning needs to apply to the NSA. We want it to eavesdrop on our enemies, but it needs to do so in a way that doesn't trample on the constitutional rights of Americans, or fundamentally jeopardize their privacy or security. This means that sometimes the NSA won't get to eavesdrop, just as the protections we put in place to restrain police sometimes result in a criminal getting away. **This is a trade-off we need to make willingly and openly, because overall we are safer that way**. Once we do this, there needs to be a cultural change within the NSA. Like at the FBI and CIA after past abuses, the NSA needs new leadership committed to changing its culture. And giving up power. **Our society can handle the occasional terrorist act; we're resilient, and -- if we decided to act that way -- indomitable**. But a government agency that is above the law ... **it's hard to see how America and its freedoms can survive that**.

Expanding on Goitein's analysis, Schneier makes some more important points about the stakes of liberty and security in the face of domestic surveillance:

1. **The NSA can't police itself.** The NSA's situation is unique in that checks and balances are automatically less effective. When a program is confidential, only a small circle of individuals can know what they do or be in a position to stop them. The NSA is in a position where, due to the nature of its activities and its overall function, it essentially must be trusted to police itself. That's concerning because accountability works best when there is an outside entity with the ability to impose penalties.

   Consider: You resolve to do better in school for a variety of reasons, some personal and some external. You struggle with this because you're busy but ultimately succeed in managing your time so your schoolwork gets done. **Let's say you were told that, from here on out, you would be the one to decide the consequences if you did poorly in school**. Even if you genuinely want to succeed, it would be hard for you to decide to kick yourself out of school for failing because you have a stronger incentive to succeed in your primary mission (getting ahead in life) than your secondary mission (getting good grades).

The same is true for the NSA. Just as you aren't an inherently bad person in the example above, you don't have to win that the NSA is an inherently bad agency to see why the policy of allowing them to self-police these programs is ultimately ineffective. They have a mission (keep America safe) which is at odds with policies of restraint in surveillance. Resolving this tension internally is too much to ask – just like (hypothetical) you in the example above, their overwhelming bias is to succeed in their primary mission and so imposing consequences that constrain that, even when it's the right thing to do, is difficult. Goitein echoes these claims, outlining the ineffective and toothless checks and balances in place that have allowed the NSA to spy illegally,

Goitein, 2013 ["The danger of American apathy on NSA surveillance," Elizabeth, codirector of the Liberty and National Security program at the Brennan Center for Justice at New York University School of Law, July 13, Christian Science Monitor.]
Among this latter group, there is a sense that privacy advocates are making much ado about nothing. The NSA's data collection programs were approved by federal judges; Congress knew about them; they're used only to identify terrorists. What, exactly, is the big deal? The most obvious answer is that these programs **may be illegal**. The government admits it obtains Americans' telephone records in bulk, but claims officials do not examine them unless there is reason to suspect a terrorist link. Section 215 of the Patriot Act, however, requires the government to establish a record's investigative relevance before obtaining it – not after. The PRISM program, which collects information from Internet service providers, is ostensibly legal because it "targets" foreigners. But the program tolerates extensive "inadvertent" and "incidental" collection of Americans' information – including information the government needs a warrant to obtain under the Fourth Amendment. Yes, a secret court approved these programs. That should not start and end the discussion about their legality. Judges make mistakes, and – as recent reporting on the secret Foreign Intelligence Service Act (FISA) Court has underscored – they are far more likely to do so when they hear only the facts and arguments that one side chooses to present. When citizens have gone to the regular courts to challenge government surveillance, the government has successfully argued that the courts cannot even consider their claims.

2. **All the rights of the accused require a similar acceptance that we might not catch all criminals.** One of the foundations of our free society is that we all have certain rights in relation to the judicial system – the right to an attorney, the right to face your accuser, the right to not be unreasonably searched by police, the right to be presumed innocent until proven guilty, the right to a trial. All of these rights are necessary to ensure fairness in our judicial process and to protect people from unchecked state power. They help us be certain that our police are behaving responsibly. Each of these rights, however, arguably makes it harder to arrest people and, in some cases, to arrest criminals. If the police could question suspects without attorneys present, make them talk, search their belongings without cause, etc. then it's likely that they would catch many more criminals in the process of violating these fundamental rights.

   Why don't we let them do that? **We have decided we would rather risk letting some criminals go free than live in a society with no privacy where everyone is at the mercy of the law and has no protection.**

You can use this in a debate to make a rhetorical point: Just as a judge would not object to the right to a trial or the right to an attorney, he or she should not object to the right to be free from domestic surveillance by the NSA without a warrant. All of these things make it harder to catch criminals but are worthwhile to keep our system from being at the mercy of the overzealous whims of those who value security before all else.

3. **A police state would be worse for our safety and security.** The concept of security does not only imply that one is safe from attack by terrorists or outside entities. To be truly secure, one must be confident that they are safe from abuse at the hands of their government. We tend to assume that the only sources of danger are external because, in many of our lifetimes, they have been. That said, a police state is nothing to take lightly – absolute power in the hands of authorities is dangerous and allows them to use force to harm political enemies, to force citizens to do things that are dangerous or unseemly, and to take money or property from citizens. You need to paint a good picture of why a police state is every bit as dangerous as a terrorist attack because the PRO has the advantage of being able to point to something most people know and remember whereas you do not.

4. **Liberty is more fragile than security.** Finally, Schneier argues that, when choosing between liberty and security, we should always choose liberty. This is because, while the American people are resilient enough to rebuild after terrorist attacks and the like, once liberty is lost it's very very hard to get it back. For example, the TSA programs that many analysts consider to be unhelpful and intrusive remain in place because the government would have an irrationally difficult time defending a decision to get rid of them and we've all become numb to the impact. Use this as a tie-breaker argument – that while we can always recover from security breaches, we have a much harder time reversing losses on the liberty front.

Now that we have some context, let's look at some specific harms. We'll start with free speech and association:

Goitein, last modified 2013 ["3 views on NSA reform after Snowden leaks," Elizabeth, codirector of the Liberty and National Security program at the Brennan Center for Justice at New York University School of Law, Christian Science Monitor.]
Collecting foreign intelligence is the National Security Agency's job, and that sometimes requires eavesdropping on Americans. Before 9/11, however, the NSA could collect an American's information only if he or she was acting on behalf of foreign interests. Congress amended the law after 9/11 to eliminate this limitation. Today, the NSA doesn't even need an individualized court order to wiretap Americans' international communications, and it may collect their phone records if they are deemed "relevant" to an authorized investigation. These developments are worrisome in their own right. The government has a history of using domestic surveillance to harass political enemies (Martin Luther King Jr.) and disrupt social justice movements (anti-Vietnam war protesters). Legal limits on the government's ability to spy on Americans were established after Watergate to stem such practices. These limits are being eroded.

As Goitein points out, many social justice movements are meant to disrupt the status quo. The government often has an interest, for a variety of reasons, in maintaining the status quo. That can often mean disrupting social justice movements by making it harder for them to assemble or disseminate their speech. The freedom to spy on citizens without cause makes their associations and statements subject to government monitoring, giving authorities the tools to disable those movements. This argument shows how violations of some rights may spill over into violations of other rights – particularly with surveillance. In some cases, surely the government does not pursue abuses of its power (detaining human rights leaders, etc.) merely because it lacks the information to do so. By removing that barrier, the government has the information to conduct other abuses, as proven empirically by the civil rights movement.

Moreover, even if power is not abused, individuals may become more conscious of their speech and less likely to speak out against the government because they know their statements will be tied to them directly. This disables dissent and has a chilling effect on robust democracy because people will start to police what they say simply by virtue of being watched.

It also harms the public,

Meyer, 2013 ["Dear NSA, Thanks for Making Us All Insecure," David, Bloomberg Businessweek Contributor, September 6, Bloomberg Businessweek.]
However, you've not stopped at code breaking—you have also made sure that vulnerabilities have been inserted into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets. Here's where the stupidity creeps in: You actively work to influence policies, standards, and specifications for commercial public key technologies and shape the worldwide commercial cryptography marketplace to make it more tractable to advanced cryptanalytic capabilities being developed by yourself. In other words, **instead of just building a better lock pick, you are trying to make sure that all locks are faulty by design**. What is so jaw-droppingly idiotic about your actions is that you have not only subverted key elements of modern cryptography, but you have also appointed yourself as the guardian of the knowledge that the resulting vulnerabilities exist. And if your own security systems were up to the task, then those secrets wouldn't be sitting in the offices of the New York Times and ProPublica. One must possess a Panglossian view on things to assume that Edward Snowden was the first person out of the many thousands in his position to make away with such material. He brought it to the public, and without that move there's a good chance you wouldn't have even known he took it. So who else has it? Bet you have no idea. So well done; you've probably put your own citizens at risk.

As Meyer explains, the NSA's domestic spying program has been built on pressuring entities who hold information (phone companies, etc.) to build "backdoors" into their systems so that the NSA can get into them at will, without needing a warrant or proving that they have cause to search. The unintended consequences, however, are extreme. The NSA's insistence has made it such that all systems are always already faulty. The lack of a truly secure system is troubling, even if the NSA is the only organization who knows the way in. Why? Simply put: if someone compromises the NSA or turns against them (which we already know is possible) they have a skeleton key to almost all the major systems in the world. That

would be disastrous and would eliminate all fail-safes and redundancies. It's a sobering thought but not at all outside the realm of possibility.

That same problem can harm the economy as well,

Meyer, 2013 ["Dear NSA, Thanks for Making Us All Insecure," David, Bloomberg Businessweek Contributor, September 6, Bloomberg Businessweek.]
But let's ignore that distinct likelihood for a moment, and concentrate on the aftermath of Snowden's revelations. If the first tranche of those revelations will hit the U.S. Web services and cloud economy hard—estimates vary as to how hard, and only time will tell—then the crypto scandal is going to do the same to the U.S. security industry. In fact, it's probably going to hurt more. Most people have too much invested in American Web services to pull out on short notice; it's relatively trivial in many cases to switch security services. Of course, the implications aren't only glum for U.S. firms. There are enough hints in your leaked documents to suggest that you got to some foreign firms, too. And as you seem to have influenced the standards-setting process (sometimes cackhandedly) the global security industry must now think about starting from scratch.

Widespread domestic spying isn't just bad for American citizens' privacy. It's also not great for their businesses. Both the web industry and the security industry now operate under a haze of doubt and people will likely be hesitant to use U.S.-based companies in the future if they fear that their data may be compromised. This damages these industries and the consumers, businesses, etc. that depend on them, which is terrible for the economy.

The pro will argue that all of this is worth a bit more security, but Noble argues:

Noble, 2013 ["U.S. debates security vs. privacy 12 years after 9/11," Jason, Staff Writer at the Des Moines Register, September 11, USA Today.]
But John Mueller, a senior fellow at the libertarian Cato Institute and researcher at the Mershon Center for International Security Studies at Ohio State University, worried that when it comes to national security, it's not always realistic to count on the political process to change course and restore civil liberties. The NSA programs revealed this year exemplify an unaccountable security state, he said. The immediate fear and anger generated after the attacks allowed the construction of a surveillance system that has remained mostly hidden from public scrutiny and public opinion. As long as the programs remain secret, they continue to grow, he said. In his research, Mueller has calculated the increased cost of domestic security operations at more than $1 trillion since Sept. 11, with little scrutiny, oversight or evaluation to determine whether they're actually making Americans safer. "The real question should be: **How safe are we?" Mueller said. "But that question is essentially never asked**." Mueller attempted to provide an answer by saying that the chances of an American being killed by a terrorist in a given year were one in 3.5 million. National media, including The Washington Post and Reason Magazine, have cited a one-in-20 million figure. The National Safety Council, which puts out a chart each year on the odds of dying from one of dozens of causes, has declined to provide a figure for terrorism in recent years because there haven't been enough deaths from which to draw reliable estimates. "Virtually no one ever says that your chance of being killed (by a terrorist) is one in 3.5 million," Mueller said. "**Should we**

consider that to already be pretty safe, or are we going to spend a lot of money to become even safer?"

Noble makes an important point about costs and benefits. He agrees that we shouldn't take unnecessary risks and should maintain a certain baseline of security that keeps us safe. After a certain point, however, the costs swamp the benefits and are no longer worth it. Consider the following example:

You're starving. Someone offers you a pizza for 10 dollars. You gladly pay it and eat the entire pizza because it solves your hunger problem. Someone then offers you more pizzas for 5 dollars apiece. You don't want to pay for them, even though they're cheaper, because you have just eaten an entire pizza. The marginal cost of more pizza outweighs the marginal benefit of getting to eat it.

In this case, safety is the pizza and the money is the freedom we give up to get the safety. The NSA already has the capability to keep us pretty safe without domestic surveillance – so safe that in decades your statistical odds of being harmed in a terror attack are **literally so low as to be insignificant**. Put simply, the NSA has no reason to be hungry for more pizza and would be wasting liberty and resources for something that no longer satisfies an important need but rather is, essentially, overkill – a waste of valuable liberty for a modest or non-existent return in how safe we are from harm.

Healy continues,

Healy, 2013 ["Be Afraid of NSA Spying," Gene, senior editor at the Cato Institute, September 24, Reason.]
The "Dear Family" letter repeats what the agency told Congress this summer that NSA has kept "the nation and its allies safe from 54 different terrorist plots ... just part of the great work that your family members are doing every day." But as Gosztola points out, pressed on that claim by Sen. Patrick Leahy, D-Vt., back in August, Inglis retreated, conceding that the secret programs were instrumental in only one case, a 2009 New York subway bombing plot. Even there, the program in question (PRISM, an email and web-traffic monitoring tool) was unnecessary, since the FBI already had ample justification for a warrant. When it comes to the call-records dragnet, the Washington Post reports, "The case that the NSA points to as its primary example of the program's usefulness" wasn't an interdicted terror plot -- it involved a Somalia-born San Diego cabbie who sent $8,500 to a terrorist group in his home country. The NSA hoovered up every American's calling records and **all we got was one lousy cabdriver**.

This data supports the diminishing returns claim by calling the statistics underlying the claim that enhanced surveillance makes us safer into question. In this case, the data supports that conventional methods (waiting to get a search warrant, etc.) were enough to keep us safe.

That's all for today! Keep reading, and good luck this weekend!