We negate; resolved: The benefits of domestic surveillance by the NSA outweigh the harms.

Contention One: Surveillance undermines trust.

Sub-point A: The people.

First, trust is lost between the general population and the government. **The International Journal of Law, Crime and Justice shows**

Trust is based on how another individual will perform on some future occasion, as a function of that individual's (or in this case, government's) current and previous claims, as to how they will behave (Good, 1988: 33). Generally, objections to surveillance do not arise when others are the subject of surveillance. On the contrary, **objections are usually raised when the individuals** themselves are subject; especially if they **see themselves as law-abiding citizens in which case surveillance of their activities would seem unnecessarily intrusive.** Concerns have been raised that authorities may use private information to investigate and prosecute activities beyond the scope of the original intent of surveillance. **The result will be a loss of public trust in the government because while it reassured its citizens that counterterrorism measures would not apply to them, recent extensions of these measures proved otherwise.** For example, in the United States, when the [P]resident introduced the concept of military justice with his military tribunal order in November.he reassured Americans that it would not apply to them but only to noncitizens. Yet now the administration has crossed that line and asserted the same authority with respect to the two US citizens, Hamdi and Padilla, that it asserts with respect to the foreign citizens held at Guantanamo (Cole, 2002/2003: 12).

Next, it shows that governments don't trust the people. **The International Journal of Law, Crime and Justice continues**

Governments' over-reliance on surveillance processes and practices sends the message to citizens within the particular setting where surveillance is taking place that they cannot be trusted. Constant surveillance, which minimizes the possibility of undetected default, negates trust because there can be no trust when there is no possibility of error (Fried, 1984: 212 and 216). Therefore, trust specifically relates to a lack of transparency because total transparency would not be necessary if there was trust. **With measures requiring mass data retention, everyone is considered as a 'risk' and not to be trusted.** Yet, trust is a crucial dimension in the relationships between citizens and their governments. **Since trust is reciprocal, citizens will trust the government to the extent that they believe that it trusts them**, that it is acting in their interests and that its procedures are fair. Mass surveillance not only fosters suspicion as to why information was retained in the first place (seeing as how it falls on suspects and non-suspects alike), but also in terms of how this information will inevitably be used. What other adverse social consequences might be observed by the creation of the database and its use?

Trust is essential to good governance and well-being. **Eric Uslaner from the University of Maryland explains**

I shall argue for the cultural roots of trust in this papser–but trust also reflects an optimstic view of the world. This worldview in turn is based upon real economic circumstances. Societies with more equal distributions of wealth are more trusting. And **societies with higher levels of trust in turn have institutions that function better. Trust leads to better institutions–not the other way around. It also produces higher spending for the sorts of policies that foster equality** (more redistribution, more funding for education). So the countries with the lowest levels of trust will are those with the most unequal distributions of wealth. But they are also the countries that are least likely to redistribute wealth to create the sort of trust that will breed institutions that function better.

Sub-point B: Businesses.

Forbes warrants

We are told we live in a digital world and the future is bright for tech startups as costs of launching new products and services plummet and global markets open up to the smallest vendor. Yet, **there is a worldwide perception that any data that is stored or even routed through the United States is sucked into cavernous NSA data centers for analysis and cataloging.** That perception was solidified in 2006 when former AT&T technician Mark Klein blew the whistle on the fiber tap that ATT had provided to the NSA in some of its data centers. **Those**

perceptions have had real consequences for US tech firms seeking to offer global services. Email archiving services such as ProofPoint could not sell to even Canadian customers without building local infrastructure. **Even establishing separate data centers in Canada and Europe is not enough to assure customers that their data would forever stay out of the grasp of US intelligence services.**

The Information Technology and Innovation Foundation furthers

What is the basis for these assumptions? The data are still thin—clearly this is a developing story and perceptions will likely evolve—but in June and July of 2013, the Cloud Security Alliance surveyed its members, who are industry practitioners, companies, and other cloud computing stakeholders, about their reactions to the NSA leaks.16 **For non-U.S. residents, 10 percent of respondents indicated that they had cancelled a project with a U.S.-based cloud computing provider; 56 percent said that they would be less likely to use a U.S.- based cloud computing service.** For U.S. residents, slightly more than a third (36 percent) indicated that the NSA leaks made it more difficult for them to do business outside of the United States.

On the low end, **U.S. cloud computing providers might lose $21.5 billion [to $35.0 billion] over the next three years.** This estimate assumes the U.S. eventually loses about 10 percent of foreign market to European or Asian competitors and retains its currently projected market share for the domestic market. On the high end, U.S. cloud computing providers might lose $35.0 billion by 2016. This assumes the U.S. eventually loses 20 percent of the foreign market to competitors and retains its current domestic market share. (See Appendix A for details.)

Sub-point C: Foreign countries.

The Russian Times reports

Before treaty procedures move forward, **the EU will want more transparency from the US. Other EU officials felt vulnerable heading into diplomatic negotiations** with a party that has listened in on classified information beforehand. The agreement would be a "once in a generation prize," which could add as much as $157 billion to the EU economy, over $125 billion to the US economy and as much as around $133 billion to the rest of the word, British Prime Minister David Cameron said at the summit, adding it could add two million extra jobs, more choices and lower consumer prices. **Lode Vanoost, former deputy speaker of the Belgian parliament, believes the main purpose of the US surveillance program was "economic spying" on the EU**, seeing a connection between economic decline and the need to spy. "One consequence [of the Snowden leak] for sure is that people will ask, 'Does it make sense to negotiate a free-trade agreement without clear rules about data protection and control?'" European Parliament President Martin Schulz told reporters in Brussels.

The Wall Street Journal corroborates

France and Germany demanded that Washington respond to reports that the National Security Agency spied on European institutions, in the latest diplomatic eruption to follow the revelations by rogue contractor Edward Snowden. **French President François Hollande**, abandoning the usual niceties of trans-Atlantic dialogue, told the U.S. to stop spying on European diplomatic outposts and **suggested that coming free-trade talks between the EU and U.S. now hang in the balance.**

Contention Two: NSA surveillance splinters the Internet.

There are two reasons why this is true.

First, EU companies are decreasing the amount of data sent to US databases. **The Guardian explains**

Parallel to the proposed data privacy rules, there are various other transatlantic arrangements in place regulating European supply to the Americans of air passenger data, financial transactions and banking information aimed at suppressing terrorism funding and **the so-called Safe Harbour accord [allows]** allowing **companies in Europe to send data to companies in the US where, as a result of Snowden, it is clear that that data can then be tapped by the NSA.**

"**The Safe Harbour** may not be so safe after all. It could be a loophole because it **allows data transfers from EU to US companies**, although US data protection standards are lower than our European ones," said Reding. "Safe Harbour is based on self-regulation and codes of conduct. In the light of the recent revelations, I am not convinced that relying on codes of conduct and self-regulation that are not policed in a strict manner offer the best way of protecting our citizens."

Second, the US is being hypocritical with its own policies. **Slate furthers**

Rousseff's move could lead to a powerful chorus—one that would transform the Internet of the future from a global commons to a fractured patchwork severely limited by the political boundaries on a map. Brazil is one of a handful of **countries**—including Indonesia, Turkey, and India—that **have wavered in the debate over whether to develop an international framework to govern the Internet, one that would replace the role that the United States has played as chief Internet steward. Traditionally, that debate has featured America in the role as champion of a free and open Internet, one that guarantees the right of all people to freely express themselves.** Arguing against that ideal: repressive regimes that have sought to limit connectivity and access to information. **The NSA's actions have shifted that debate, alienating key Internet-freedom allies** and emboldening some of the most repressive regimes on the planet. Think of it as **an emerging coalition between countries** that **object to how the United States is going about upholding its avowed principles for a free Internet**, and countries that have objected to those avowed principles all along.

The problem is a unified Internet is essential.

First, it's key to cybersecurity. **The Georgetown Journal of International Affairs impacts**

Third, in an increasingly interconnected world, we must realize that norms, national policies, and national frameworks for cyber defense are necessary, but not sufficient. **We must go to the next level by linking national plans to coalition planning, exercises, and greater understanding of coordinated security in cyberspace. These efforts must leverage political and military alliances as well as international organizations** (governmental ones and non-governmental ones). They may include activities focused on military, legal, political, economic, and technical aspects of cyber security. **We will draw new lessons from these actions that will enhance our ability to share information and act in a coordinated manner at the coalition level while fostering further development of policy and capability delivery within our respective nations.** This will begin to change the cyber playing field from one dominated by offensive-minded adversaries to one based on mutually assured defenses.

Second, it harms the economy. **The Information Technology Industry Council details**

The other point that Friedman makes (one that has been set aside too often in this debate) is the genuine risk the surveillance storyline poses to the global digital economy. Some countries are considering laws to mandate in-country Internet services. Others are looking at the feasibility of building their own Internet infrastructure, complete with cables running across the oceans to connect continents while avoiding connection to the U.S. Some nations are giving serious consideration to proposals that would force technology services and products to be housed, built, and tested within their borders, which could permanently fragment the Internet. The result of these policies: good bye, information superhighway; hello, potholed digital gravel roads. Friedman writes: **Just as countries around the world have grown more dependent on information systems for their stability and quality of life, they have also grown dependent on the trade that supports IT access and innovation.** Threats to IT systems have spurred governments to think about regulatory solutions, but care must be taken not to disrupt the parallel system of trade that undergirds the IT ecosystem.