Leads Act Counterplan — GFCA Novice Packet

Explanation

Negative

1NC

2NC/1NR

Affirmative

2AC

1AR

File Description and General Tips

This file contains a counterplan that can be read against both the Surveillance State Repeal Act affirmative and the Secure Data Act affirmative. It contains materials for both the negative and the affirmative.

A counterplan is a type of negative argument that proposes a different policy than the plan. It is introduced as an off-case position in the 1NC. The 1NC shell for the counterplan is included in this file. To extend the counterplan in the negative block, the negative should prepare blocks to each affirmative response. When doing so, the negative can make use of the backline evidence contained in this file. Students should carefully choose which extension evidence to read; it is very unlikely that students will be able to read *all* extension cards in any 2NC or 1NR.

When answering this counterplan, the affirmative should use the materials in this file to construct a 2AC frontline. Students should include the appropriate solvency deficit arguments in the frontline based on the case and advantages being debated. For some of the 2AC arguments, the affirmative is provided with additional extension cards that could be useful for the 1AR. Due to the intense time constraints of that speech, students should carefully choose which (if any) extension evidence to read.

When reading this counterplan, the negative should also read the Terrorism DA and/or the Presidential War Powers DA in the 1NC. These disadvantages are net-benefits to the counterplan; the EU Tech Sector DA is not a net-benefit to this counterplan.

Explanation of the Negative

The LEADS Act counterplan proposes that the United States federal government enact the Law Enforcement Access to Data Stored Abroad (or LEADS) Act. This legislation would update the Electronic Communications Privacy Act (passed in 1986) to require law enforcement agencies to obtain a judicial warrant in order to access U.S. persons' data stored in the cloud. Currently, no warrant is required. The LEADS Act would allow law enforcement agencies with a proper warrant to access U.S. persons' cloud data even if it is stored overseas, something that has been controversial (see the *In Re Microsoft* case). For non-U.S. persons, it would require law enforcement agencies to comply with the relevant laws of the foreign country where the data is stored. Finally, the Act would make a series of improvements to the Mutual Legal Assistance Treaty Process to facilitate improved cooperation between international law enforcement agencies. The idea is that instead of directly subpoenaing a foreign company, a law enforcement agency should go through the MLAT process to request that the data be subpoenaed by that nation and then shared with the nation doing the investigation.

The negative argues that the LEADS Act solves the affirmative's advantages:

1. Privacy — the LEADS Act requires law enforcement agencies to obtain a warrant before searching or seizing a U.S. person's data stored in the cloud. This is a big privacy improvement.

2. Tech Competitiveness — the LEADS Act resolves one of the biggest concerns of foreign customers by clarifying that data stored by U.S. cloud providers cannot be accessed without a warrant. This helps rebuild trust in U.S. tech companies.

3. Investigative Journalism — the LEADS Act reassures journalists that their cloud data is protected from law enforcement agencies. This enables media organizations to make better use of the cloud, cutting down on operational costs.

4. Cybersecurity — the LEADS Act reforms the MLAT process to facilitate improved global law enforcement cooperation. Because cyber threats are almost always transnational, this cooperation is vital to effectively combat them.

The 1NC shell includes a general solvency card and an internal transnational organized crime net-benefit. The negative should also read the Terrorism DA and/or the Presidential War Powers DA in the 1NC. In the 2NC/1NR, the negative should use the backline evidence in this file to respond to the affirmative's arguments. Students are encouraged to construct blocks to answer each potential affirmative response.

Explanation of the Affirmative

The affirmative argues that the plan is vital to solve the advantages because it curtails surveillance done by the National Security Agency. The counterplan only affects law enforcement agencies, not intelligence agencies. The affirmative materials include a general solvency argument (supported by evidence) as well as specific solvency arguments for each advantage (supported by analysis based on the relevant 1AC evidence).

In addition to solvency arguments, the affirmative will argue that the counterplan and plan can be done simultaneously ("permutation"). The affirmative should argue that the "do both" permutation resolves the internal net-benefit about transnational organized crime.

The affirmative also argues that the counterplan results in data localization that threatens Internet Freedom and global human rights. This is both a disadvantage to the counterplan and an add-on advantage to the plan. Data localization can be impacted not only to human rights but also to the 1AC's impacts.

When answering the counterplan, the affirmative should remember that any offense they have against one of the net-benefits (Terrorism DA and/or Presidential War Powers DA) is a reason to prefer the plan to the counterplan. Instead of attempting to generate offense against the counterplan by reading the Data Localization DA, the affirmative could choose to read the data overload link turn to the Terrorism DA or the presidential powers bad impact turn to the War Powers DA.

Explanation of Conditionality

This file includes conditionality arguments for both sides. Conditionality refers to the "status" or "disposition" of the counterplan: is the negative defending only the counterplan or can they "kick" the counterplan at any time and revert to defending the status quo? When the negative defends a counterplan but reserves the right to revert to defending the status quo, they are defending the counterplan conditionally. In response, the affirmative can argue that conditionality should not be allowed. When the affirmative makes this argument, the negative must respond by defending the desirability of conditionality. This is called a theory argument.

1NC — LEADS Act CP

The first/next off-case position is the LEADS Act counterplan.

The United States federal government should enact the Law Enforcement Access to Data Stored Abroad Act.

First, the counterplan solves the case without jeopardizing national security — it avoids our [Terrorism DA and/or Presidential War Powers DA] and strengthens global law enforcement cooperation.

Evans 15 — Karen S. Evans, Partner at KE&T Partners, LLC—an IT management consulting firm, National Director of The US Cyber Challenge—a nationwide talent search and skills development program focused specifically on the cyber workforce, former Administrator of the Office of Electronic Government and Information Technology at the Office of Management and Budget—the de facto Chief Information Officer for the U.S. government before that position was formally created in 2009, former Chief Information Officer for the United States Department of Energy, former Director of the Information Resources Management Division in the Office of Justice Programs in the United States Department of Justice, holds an M.B.A. from West Virginia University, 2015 ("LEADS Act is logical path toward much-needed ECPA reform," *The Hill*, March 13th, Available Online at http://thehill.com/blogs/congress-blog/technology/235582-leads-act-is-logical-path-toward-much-needed-ecpa-reform, Accessed 10-27-2015)

The necessity of reforming the Electronic Communications Privacy Act (**ECPA**) **has long been talked about in Congress, and it is time to take action. A sensible and bipartisan bill has been introduced that gives us a realistic path to reform. That bill is the** Law Enforcement Access to Data Stored Abroad (**LEADS**) **Act** – we should examine it seriously. In today's Digital Age, we store incalculable quantities of personal information on cloud servers which may be located anywhere in the world, something 1980s-era ECPA never anticipated. **It's time to modernize the way we conduct digital trade and the legal framework that controls how law enforcement agencies interact with this data**.

With little fanfare, this bipartisan bill was recently reintroduced by Sens. Orrin Hatch (R-Utah), Dean Heller (R-Nev.) and Chris Coons (D-Del.) last month (a companion bill was also introduced in the House). The bill will help achieve several important outcomes. **LEADS will improve data privacy protections for U.S. citizens and residents while strengthening law enforcement cooperation with other nations. The bill** also **preserves the essential balance between security and privacy**. At the same time, **it will signal to our foreign partners that we are serious about improving law enforcement cooperation with them**. In these times, **such improvements are vital to ensuring effective functioning of our law enforcement agencies while maintaining the privacy rights of our citizens**.

We have all come to expect a certain level of privacy in our personal communications. Our law enforcement agencies must follow procedures established by Congress and the courts to gain access to personal correspondence and data files. These rules also govern access to information held overseas and controlled by long-standing mutual legal assistance treaties (MLATs). But these clear principles have been partly obscured by the digital nature of today's communications. Today many data centers operated by American companies are located in foreign countries and their electronic footprints cross numerous jurisdictions. In these changing conditions, U.S. courts are now serving warrants to American technology companies demanding access to customer data stored overseas.

[Evidence Continues — No Text Removed]

1NC — LEADS Act CP

[Continued from Previous Page]

We must bring greater clarity to these procedures **by updating our laws to reflect today's circumstances. The LEADS Act is an ideal opportunity to do this. It removes the gaps in ECPA by specifying that U.S. warrants apply to data stored abroad only when the owners are U.S. persons** (citizens or residents) **and only when execution of the warrants does not violate foreign laws. The bill also requires that the U.S. improve its MLAT procedures**, which are the primary alternative mechanism to warrants in these situations. **These clarifications to ECPA can only enhance U.S. cooperation with other governments. Strong relationships of mutual confidence with these governments are vital to the ability of our law enforcement agencies and courts to carry out their missions effectively**.

There are many examples from my service in government that illustrate the importance of U.S. cooperation with other countries as it relates to effective policy implementation, and I'd like to highlight two of them.

Established in 2002 by Congress, transportation worker identification cards (TWIC) are intended to minimize the risk of bad actors accessing key aspects of the maritime transportation system. Effective policy implementation meant the U.S., Canada and Mexico had to work together to make technical requirements interoperable. Treaties governed the intergovernmental work. Policy guidelines set the technical implementations in motion in each participating country.

In addition, a consortium of countries composed of Australia, New Zealand, Canada, the U.K. and the U.S. met regularly to share best practices for expanding e-government to improve services to the citizen, which included information sharing across law enforcement agencies. Each country used this information and implemented new approaches to bolster law enforcement cooperation without harming constituent services.

Without trust, reciprocity and shared information, these efforts will be futile. **Only by respecting the Golden Rule when cooperating with other countries can we hope to produce real results. The LEADS Act will strengthen our ability to maintain these productive relationships with international partners to the real benefit of American citizens**.

It is **legislation like LEADS** that **will help the U.S. achieve broader, much-needed ECPA reform**. The goal is clear – **the laws should ensure that data stored in the cloud receives the same legal protections as data stored in our homes and at work**. Senators and representatives have the opportunity to act on the legislation to ensure we do unto others as we would have them do unto us. **It's time to provide better data privacy protections for our citizens while preserving U.S. relationships abroad. I encourage Congress to take up The LEADS Act** this session **and strengthen America's leadership in preserving the balance between security and privacy**.

1NC — LEADS Act CP

Second, strengthening the Mutual Legal Assistance Treaty (or MLAT) process is vital to effective law enforcement — this prevents terrorism and organized crime.

Cunningham 15 — Bryan Cunningham, Senior Advisor specializing in Cybersecurity and Data Privacy at The Chertoff Group—a private security and risk management consulting company, Member of the Cyber Security Task Force at the Bipartisan Policy Center, Principal at Cunningham Levy LLP—a law firm, served as Deputy Legal Advisor to National Security Advisor Condoleezza Rice, holds a J.D. from the University of Virginia, 2015 ("Why State and Local Law Enforcement Should Be Part of the MLAT Reform Process," *Government Executive*, March 25th, Available Online at http://www.govexec.com/state-local/2015/03/mlat-reform-state-local-law-enforcement/108427/, Accessed 11-02-2015)

French President François Hollande went further, warning "American web giants" that if such companies "are serious about not becoming accomplices of evil, they've got to help us."

Hollande's comments bring into sharp relief the simple truth that, **in the age of instantaneous communication and routine overseas storage or massive amounts of data, the current MLAT process can be inefficient, ineffective and, where speed is decisive, futile**. In short, **MLAT is broken**.

MLATs are formal agreements between countries establishing procedures for requesting evidence stored outside the requesting country's jurisdiction. Historically, in many time-sensitive cases, law enforcement agencies officials exchanged information informally and private companies cooperated without formal legal process. But with increasing overseas attention to privacy rights and concerns about secret, unilateral data collection by national governments against other countries' citizens, companies increasingly are refusing to cooperate informally and governments are retaliating for unfair "spying" on their citizens.

State and local law enforcement agencies (LEAs) **should care about this problem not only because of its potential impact on the general ability of the U.S. to take down international terror and other criminal organizations, but because, in our increasingly interconnected world, what once could have been treated largely as "local" cases, such as cyber fraud and child pornography now require retrieval of evidence from overseas, and even basic crimes without any obvious cyber component will require evidence stored overseas**.

The problem will get worse as cloud storage providers increasingly globalize data storage, in order to: store data close to the account holder for faster service; take advantage of excess capacity; and/or save on infrastructure costs or tax burdens.

There is broad agreement that the current MLAT system has not kept pace with technology and must be reformed to support fast and effective global law enforcement and many countries, especially in Europe, are threatening to cut off U.S. LEAs from some data altogether in retaliation for perceived spying abuses. Unchecked, both trends threaten to damage the ability of state and local LEAs to prosecute many types of crimes. But U.S.-led MLAT reform can stem this dangerous tide. What should state and local law enforcement leaders do about it?

First, stay informed. **The** Law Enforcement Data Stored Abroad (**LEADS**) **Act**, currently under debate in the United States Senate, and a similar measure in the House, **aim to begin the process of MLAT reform**. A number of law enforcement and civil liberties advocacy groups are tracking such legislation.

Second, be heard. Particular facets of legislation may be more or less acceptable to individual state and local law enforcement agencies but such LEAs shouldn't let the federal government be the only law enforcement voice in the debate.

[Evidence Continues — No Text Removed]

1NC — LEADS Act CP

[Continued from Previous Page]

Finally, think through the issues carefully. The immediate reaction of many LEAs may be to oppose any congressional "meddling" with the current system, particularly if an LEA has not itself experienced problems. But **efforts to streamline and improve U.S. MLAT processing, as the LEADS Act**, for example, **can benefit state and local LEAs both because such agencies must go through the U.S. government to request foreign-stored evidence and because U.S. efforts may prompt improvement abroad**.

Further, **shows of U.S. "good faith" may forestall new foreign restrictions on U.S. LEAs access to data stored in their countries**.

1NC — LEADS Act CP

Third, transnational organized crime poses the gravest risk to global peace and stability. It is the root cause of many conflicts.

France 15 — The Permanent Mission of France to the United Nations in New York, 2015 ("Transnational threats to international peace and security," March 11th, Available Online at http://www.franceonu.org/Transnational-threats-to-8739, Accessed 11-02-2015)

The Security Council has several times noted with concern the consequences of transnational threats, such as organized crime and drug trafficking, on international peace and security.

It repeatedly noted the role played by drug trafficking and organized crime in the emergence of conflicts in places such as Afghanistan (Resolution 1817/2008 and Resolution 1890/2009), **Haiti** (Resolution 1892/2009) **and Guinea Bissau** (PRST of 15 October 2008 and 5 November 2009).

It also considered the issue on a more general point of view in Resolution 1373/2001 on Threats to international peace and security caused by terrorist acts (**the Council** "**[noted] with concern the close connection between international terrorism and transnational organized crime, illicit drugs, money-laundering, illegal arms-trafficking, and illegal movement of nuclear, chemical, biological and other potentially deadly material**") and in PRST/2009/32 on Peace and Security in Africa ("the Council notes with concern the serious threats posed in some cases by drug trafficking and related transnational organized crime to international security in different regions of the world, including in Africa").

A threat to security

Transnational threats create roots for the development of regional and global tensions. Drug trafficking and related transnational organized crime encourage money laundering and makes possible the financing of non-governmental armed groups. Organized crime networks threaten effective state control on borders and territories. They undermine the authority of states, spread corruption and weaken economic development. Therefore, they pave the way for radicalisation processes that can lead to violent extremism and terrorism. Insurgents and criminals develop close ties to profit from this instability and in some cases create the conditions for such instability.

As a matter of fact, **transnational threats are a destabilizing factor in every crisis where the U**nited **N**ations **operates. They take advantage of the weakness of states in conflict situations and make the return to peace and economic development a more protracted and more difficult process for those states**.

A growing challenge

The international community adopted several conventions in order to counter transnational threats in a comprehensive approach:

— the Single Convention on Narcotic Drugs of 1961,

— the Convention on Psychotropic Substances of 1971,

— the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 1988,

— the United Nations Convention against Transnational Organized Crime of 2000,

— the United Nations Convention against Corruption of 2003.

However, **in the last decades, advances in technology, open borders and open markets created greater cross-border opportunities for criminal groups. As a result, organized crime has diversified, gone global, and has reached macro-economic proportions. It developed even closer links with drug trafficking, corruption and terrorism. It poses a great**er **threat to national and global security** than when the Convention against Transnational Organized Crime was adopted. **No part of the world is immune**. Particularly vulnerable are post-conflict regions, areas where the rule of law is weak and countries that suffer from under-development.

Counterplan Explanation/Overview

Instead of enacting the plan, the counterplan enacts the Law Enforcement Access to Data Stored Abroad (or LEADS) Act. This bill updates the Electronic Communications Privacy Act to require law enforcement agencies to get a warrant in order to search information stored by U.S. citizens in the cloud. It also streamlines the process by which U.S. law enforcement agencies cooperate with foreign law enforcement agencies by upgrading the Mutual Legal Assistance Treaty (or MLAT) process. This solves most of the case without jeopardizing national security: the LEADS Act maintains the essential NSA authorities crucial to (the war on terrorism and/or presidential war powers) — that's Evans. This outweighs the risk of a solvency deficit — the counterplan solves well enough to minimize the case's impact.

The counterplan also prevents transnational organized crime by facilitating improved global law enforcement cooperation. Absent reform, foreign agencies will stop working with the U.S. — that's Cunningham. Organized crime is the root cause of most global conflicts because it creates the conditions for instability — that's France.

They Say: "Permute – Do Both" (vs. SSRA/Upstream)

( ) Links to Terrorism DA — maintaining NSA surveillance is crucial to counterterrorism because it provides proactive intelligence that can uncover plots before they happen. The counterplan *alone* maintains these capabilities, preventing attacks.

( ) Links to Presidential War Power DA — intelligence gathering authority is vital to the President's ability to exercise his commander-in-chief powers during the war on terrorism. Intelligence capabilities eliminated by the plan — not law enforcement capabilities — are key to presidential power. The counterplan *alone* preserves the executive flexibility needed to prevent WMD proliferation.

( ) Our Links Are Linear — we don't have to win that the counterplan doesn't link *at all*. As long as the counterplan links *less than the plan*, our net-benefits outweigh — the counterplan solved enough of the case to minimize the impact of a solvency deficit.

They Say: "Permute – Do Both" (vs. SDA/Encryption)

( ) Links to Terrorism DA — encryption that NSA can't break makes it impossible to obtain proactive intelligence that uncovers plots before they happen. The counterplan *alone* preserves NSA's backdoor access to encrypted communications, preventing attacks.

( ) Links to Presidential War Power DA — intelligence gathering authority is vital to the President's ability to exercise his commander-in-chief powers during the war on terrorism. Intelligence capabilities eliminated by the plan — not law enforcement capabilities — are key to presidential power. The counterplan *alone* preserves the executive flexibility needed to prevent WMD proliferation.

( ) Our Links Are Linear — we don't have to win that the counterplan doesn't link *at all*. As long as the counterplan links *less than the plan*, our net-benefits outweigh — the counterplan solved enough of the case to minimize the impact of a solvency deficit.

They Say: "CP Doesn't Solve Constitutional Privacy"

The counterplan solves their privacy advantage — it extends Fourth Amendment protection to data stored in the cloud.

Rogers 15 — Jerry Rogers, President of Capitol Allies and Founder of its Six Degrees Project—an independent, nonpartisan effort that promotes entrepreneurship, economic growth, and free market ideals, former Director of External Affairs at The Manhattan Institute for Policy Research, former Director of Development for the Competitive Enterprise Institute, 2015 ("Congress LEADS Privacy Rights into the 21st Century," *Townhall*, May 13th, Available Online at http://townhall.com/columnists/jerryrogers/2015/05/13/congress-leads-privacy-rights-into-the-21st-century-n1998505/page/full, Accessed 10-28-2015)

Bipartisan legislation, introduced in both Houses of Congress, seeks to modernize the wholly inadequate and outdated Electronic Communications Privacy Act (ECPA). **The rules regulating government surveillance and information gathering are obsolete and in dire need of reform. Americans believe—rightly—their privacy rights are not properly protected from government infringement**.

Enacted in 1986, the ECPA is the major federal statute that regulates electronic surveillance and data gathering, and it **does not sufficiently address the challenges presented by modern day computing**. The ECPA was designed to protect the privacy of electronic communications, and in the mid-1980s, many of the issues of today's interconnected world could not have been anticipated.

The Law Enforcement Access to Data Stored Abroad (**LEADS**) **Act amends the ECPA by bringing into the Twenty-first Century the rules determining how U.S. authorities can gain access to electronic data**. On the international level, LEADS mandates that U.S. agencies cannot use search-warrants to compel the disclosure of an individual's content stored outside the United States unless the account holder is an American citizen (or U.S. person). It clarifies how U.S. authorities can access data held overseas by settling questions of jurisdiction and transparency. What's more, the reform legislation will make stronger the international process of MLATs (Mutual Legal Assistance Treaties) through which governments obtain evidence in criminal investigations. Simply, LEADS will thwart government overreach into personal data stored on U.S.-corporation servers abroad.

On the national level, the LEADS Act would make documents and material stored in the cloud subject to the same search-warrant requirements as a user's personal property. LEADS is a significant step toward protecting due process and privacy rights by extending Fourth Amendment protections to data stored by commercial services (or cloud storage).

They Say: "CP Doesn't Solve Constitutional Privacy"

Even if the counterplan doesn't solve all privacy intrusions, it is an important step — it solves *enough* of the advantage.

Smith 15 — Brad Smith, General Counsel and Executive Vice President of Legal and Corporate Affairs at Microsoft, 2015 ("The LEADS Act: A common sense reform of our outdated privacy laws," *Microsoft on the Issues*, February 12th, Available Online at https://blogs.microsoft.com/on-the-issues/2015/02/12/leads-act-common-sense-reform-outdated-privacy-laws/, Accessed 10-28-2015)

Today's bipartisan introduction of **the** Law Enforcement Access to Data Stored Abroad (**LEADS**) **Act** of 2015 **is an important step to reform our outdated privacy laws**. We commend the sponsors – Senators Hatch, Coons and Heller – for introducing this critical legislation in the United States Senate.

Microsoft supports the LEADS Act for its common sense reforms. The LEADS Act is a real solution to a real problem.

For the last 18 months there has been a vibrant debate about how to balance personal privacy and public safety. It's clear that there is an urgent need to move past debate and take action. **Citizens around the world don't believe their privacy rights are sufficiently protected, while law enforcement officials express concerns about their ability to do their jobs**.

It's clear that 2015 needs to be a year for solutions.

Any solution starts with updating our outdated laws so that they reflect the technology of today and not that of **thirty years ago. We need to ensure that law enforcement can access the information it needs while people benefit from the privacy they deserve, all pursuant to proper legal process and the rule of law. We need to protect the global nature of modern technology, while preserving the role that governments play in protecting the privacy of their citizens. To do this, governments must respect each other's borders and national sovereignty, while also enabling law enforcement cooperation across borders at Internet speed under new international rules**.

The bill introduced today **strengthens the protection of Constitutional due process rights and limits the extraterritorial reach of search warrants. It also proposes a more principled legal blueprint for balancing law enforcement needs with consumer privacy rights. It creates an important model that will help advance the international conversation that is so critically needed**. Further, the LEADs Act is consistent with ongoing ECPA reform efforts supported by Microsoft.

We're joining a broad coalition of companies and associations in the technology, telecommunications, manufacturing and cloud computing sectors to advocate for passage of the LEADS Act.

Passage of the LEADS Act would be a very important step, but there is more to do to ensure that 2015 becomes a year for solutions that promote personal privacy and protect public safety.

They Say: "CP Doesn't Solve Constitutional Privacy"

The counterplan is essential to protect cloud privacy.

Chambers 15 — Dean Chambers, independent journalist and blogger, 2015 ("The LEADS Act Necessary to Protect Internet Privacy," *Patriot Update*, August 7th, Available Online at http://patriotupdate.com/the-leads-act-necessary-to-protect-internet-privacy/, Accessed 11-03-2015)

Privacy has become the dividing line in American policy between those who believe America has become vulnerable to its enemies and those who believe, that in the quest to protect the nation, the **government has gone too far to trample on basic constitutional rights and privacy**. There is often little middle ground in the debate — until now.

When the Department of Justice suspected an Irish citizen of storing material on a cloud computing system of an Irish company that happened to be a subsidiary of Microsoft, it served to Seattle-based company a warrant, despite the clear lack of jurisdiction on the materials in question. If the material in question was a piece of paper, the DOJ would be forced by treaty obligations to abide by Irish law and request the Irish government serve a warrant for the material in question. But being on the Internet, Eric Holder's Justice Department has declared the power the grab the material, by passing the Irish government altogether.

Sen. Orrin **Hatch** (R-UT), along with Senators Chris **Coons** (D-DE) **and** Dean **Heller** (R0NV) **have proposed the LEADS Act** (Law Enforcement Access to Data Stored Abroad) **to protect internet privacy while assuring the ability to laws enforcement to legally obtain information when needed**.

Printed information held by Microsoft's subsidiary in Ireland could only be legally obtained by the Dept. of Justice if it had asked the Irish government to serve a warrant and obtain the information in question. Since this information was located on a private cloud server on the internet owned by the Microsoft subsidiary, Attorney General Eric Holders Justice Department asserted authority request the information without seeking it through under Irish law.

Microsoft, determined to fight on principle, has refused to abide by the warrant and argues that the government's Mutual Legal Assistance Treaty (MLAT) between Ireland and the United States must be followed. So far, not to the shock of many legal observers who note the judiciary's frequent refusal to reign in abuse by the Obama administration, the courts have been unwilling to stand up to the DOJ. A lower court sided with the government, as did a federal court of appeals. Unless the Supreme Court accepts the case or the Congress intervenes, privacy rights for those who use the Internet will be weakened.

"Currently, the U.S. government takes the position that it can compel a technology company to turn over data stored anywhere in the world, belonging to a citizen of any country, so long as the data can be accessed in the United States," Sen. Hatch wrote in a statement on the LEADS Act.

The LEADS act would protect the privacy rights of individuals and businesses they affiliate with to store information on the internet, such as through "cloud" servers and other means of data storage, while recognizing that law enforcement can obtain information by abiding by the laws of the country where the data is stored.

They Say: "CP Doesn't Solve Tech Competitiveness"

The counterplan solves their tech competitiveness advantage — the industry can't survive without it.

Versace 15 — Chris Versace, Columnist for *Fox Business*, Portfolio Manager for Fabian Wealth Strategies, Assistant Professor at the New Jersey City University School of Business, holds an M.B.A. in Finance from the Fordham Gabelli School of Business, 2015 ("LEADS Act Can Save U.S. Innovation," *Fox Business*, February 15th, Available Online at http://www.foxbusiness.com/technology/2015/02/23/opinion-leads-act-can-save-us-innovation/, Accessed 10-27-2015)

In an era of cloud computing, jurisdictional overreach on the part of any government is likely to prevent its citizens trading abroad. If left unchecked, it could even lead to companies re-incorporating abroad. With an $18 trillion national debt, the last thing the country needs is to allow the Justice Department to skirt international protocols, while endangering the private sector's ability to compete and proactively shrinking the domestic tax base.

Realizing the short and long-term stakes, including how international business could become impossible for American companies if the U.S. government is allowed to demand U.S. businesses treat all data everywhere as if it fell under U.S. domestic jurisdiction, Senators Hatch, Coons and Heller introduced the Law Enforcement Access to Data Stored Abroad (**LEADS**) **Act. The legislation looks to safeguards Americans' electronic data stored abroad and establish a balanced process for how U.S. law enforcement can obtain this data while respecting the sovereign rights of other countries**. Among the finer points, the LEADS Act:

- Requires a warrant to access stored content irrespective of how old the content is;
- Confirms that warrants under the Electronic Communications Privacy Act (ECPA) do not reach extraterritorially;
- Creates an exception that would allow extraterritorial warrants for content of U.S. persons (citizens and residents) stored outside of the U.S.;
- Proposes several reforms designed to improve and facilitate the Mutual Legal Assistance Treaty (MLAT) process; and
- Expresses the sense of Congress that countries should not impose data localization requirements.

The response from technology companies and associations such as Apple (AAPL), IBM (IBM), Cisco Systems, Internet Infrastructure Coalition (i2 Coalition), BSA - The Software Alliance, ACT - The App Association, Entertainment Software Association (ESA), Information Technology & Innovation Foundation (ITIF), Information Technology Industry Council (ITI), TechNet, National Association of Manufacturers (NAM), Telecommunications Industry Association (TIA), and the American Consumer Institute (ACI) **has been one of positive support for the LEADS Act**.

With the situation locked and loaded, and the ability of American companies to compete on the world stage hanging in the balance, Congress needs no greater call to act. For those supporters of the Justice Department's tactics, what would they say if Russia, China or North Korea requested similar information from an American company?

They Say: "CP Doesn't Solve Tech Competitiveness"

Even if the counterplan doesn't eliminate all surveillance programs, it rebuilds foreign confidence in U.S. tech companies.

Maines 15 — Patrick Maines, President of the Media Institute—a nonprofit research foundation specializing in communications policy issues, 2015 ("The LEADS Act and cloud computing," *The Hill*, March 30th, Available Online at http://thehill.com/blogs/pundits-blog/technology/237328-the-leads-act-and-cloud-computing, Accessed 10-27-2015)

The larger issue in the Microsoft case, and as **addressed by** the **LEADS** legislation, **is the fear, especially since the** Edward **Snowden revelations, that foreigners will lose confidence that the content of their email on U.S. servers will be open to government inspection, and go elsewhere for the purpose**.

Organizations like Forrester Research and the Information **T**echnology and **I**nnovation **F**oundation **have attempted to put a price tag on the cost to the U.S. cloud computing industry of** what is called the **PRISM** project, an outgrowth of the Protect America Act which authorizes the NSA to conduct metadata searches of email. **Those estimates are uneven, and evolving, but all the figures reported are in the billions of dollars. And while PRISM operates on a different legal foundation than the one**, ECPA, **that is the subject of the LEADS Act, there can be no question that** if Microsoft were to lose its case, and **in the absence of the passage of the LEADS Act, U.S. cloud providers will suffer**.

They Say: "CP Doesn't Solve Tech Competitiveness"

The counterplan is vital to rebuild trust in U.S. tech companies after the Snowden revelations.

Christenson 14 — Zack Christenson, Research Fellow for the American Consumer Institute Center for Citizen Research—a nonprofit educational and research institute, 2014 ("Can The DOJ Seize Emails From American Companies Stored Anywhere On Earth?," *The Daily Caller*, September 19th, Available Online at http://dailycaller.com/2014/09/19/can-the-doj-request-emails-from-american-companies-stored-anywhere-on-earth/, Accessed 10-28-2015)

Many foreigners are already wary of the U.S. government's power over U.S.-based tech companies. With the NSA's PRISM scandal and many stories of tech companies cooperating with the NSA, many foreigners already look at tech companies with a cautious eye.

The European Commission, along with most European countries, already have stringent privacy laws, and **putting U.S. companies in a position of violating local laws greatly harms their ability to do business overseas**.

The economic ramifications are large as well. According to the latest ACI ConsumerGram, high-tech services and applications are valued at $2 trillion per year, with the U.S. exporting technical equipment valued at $76 billion every year. The cloud services, like the one that Microsoft operates, are a $174 billion business. But the industry is more than just Microsoft. Other U.S. cloud businesses included Amazon, Salesforce, Google, IBM, Rackspace and many other giants. **If European regulators or consumers feel threatened, it could do major damage to the U.S. tech industry by imposing sanctions and not inviting U.S. firms to bid on contracts**.

One study, by the Information Technology and Innovation Foundation, found that a privacy backlash could spark a $35 billion dollar loss in the cloud industry, and Forrester Research estimated that the financial losses spilling into other sectors becoming as high as $180 billion. Using Bureau of Economic Analysis numbers, the financial losses could result in 2 million lost US jobs. As the ACI ConsumerGram points out, we've already started to see some backlash to the NSA scandal — many large U.S. tech companies, like IBM and Verizon Communications, were shut out from bidding on international contracts. Alternatively, foreign governments could compel foreign companies operating in the U.S. to collect send personal information on U.S. citizens and send it back overseas.

Last Thursday, **Senators Hatch, Coons and Heller introduced the L**aw **E**nforcement **A**ccess to **D**ata **S**tored Abroad **Act to address this issue by limiting the reach of warrant to U.S. citizens and companies, as well as keeping some conformity with foreign treaties and laws. Congress should give this bill its full and immediate consideration before the negative economic consequences of the DOJ's actions harm U.S. interests abroad**.

If the U.S. wants to maintain its tech dominance, both American and foreign consumers need to have peace of mind that there are some limits to the U.S. government's intrusions on the privacy of consumers living overseas. American and foreign consumers need to have trust in U.S. tech companies, otherwise it could spell disaster for the sector both at home and abroad.

They Say: "CP Doesn't Solve Investigative Journalism"

The counterplan solves their journalism advantage — it allows media companies to make better use of the cloud, improving efficiency and effectiveness.

Wimmer 15 — Kurt Wimmer, U.S. Chair of the Privacy and Data Security Practice of Covington & Burling LLP—an international law firm, Member of the Board of Trustees and Chair of the First Amendment Advisory Council at The Media Institute—a nonprofit research foundation specializing in communications policy issues, holds a J.D. and an M.A. in Communication from Syracuse University, 2015 ("Updating The Electronic Communications Privacy Act: An Essential Legislative Goal For Media Companies And The Public They Serve," *Policy Views*—a publication of The Media Institute, Available Online at http://www.mediainstitute.org/PDFs/Policy%20Views%206%20LEADS%2031815.pdf, Accessed 10-28-2015, p. 5-6)

From the perspective of the media, the LEADS Act is long overdue. Concerns about the security of confidential-source information that may be stored in the cloud, particularly on an international basis, may be holding back the media's use of the most efficient and effective technologies. Clarifying that the data in the cloud can be as secure [end page 5] **as data held on local servers would permit media companies**, and the economy as a whole, **to rely on cloud-based technologies that exist today, and that will be developed in the future. This issue and this Act are bi-partisan, common-sense, and workable solutions that Congress should embrace and pass as soon as possible**.

They Say: "CP Doesn't Solve Investigative Journalism"

Cloud services are key to overcome tight journalism budgets — the counterplan is vital to cloud adoption.

Maines 15 — Patrick Maines, President of the Media Institute—a nonprofit research foundation specializing in communications policy issues, 2015 ("The LEADS Act and cloud computing," *The Hill*, March 30th, Available Online at http://thehill.com/blogs/pundits-blog/technology/237328-the-leads-act-and-cloud-computing, Accessed 10-27-2015)

Nor is the suffering to be endured just by cloud computing companies. As published in a paper by the Media Institute, media and privacy lawyer Kurt Wimmer makes a compelling case that **media companies may be especially sensitive to issues like those addressed by** the Microsoft case and **the LEADS Act legislation:**

> **In an era of tight budgets for newsrooms and infrastructure, cloud computing has helped many media companies reduce costs and make their newsgathering operations more efficient and effective. It can be much more efficient for a newsgathering and publishing operation to purchase a package of cloud-based services** (e.g., word processing, photography, publishing, storage) **rather than maintain its own IT department, servers, and software**.
>
> **Although there are substantial advantages for media companies in adopting cloud-based technologies, there are also risks. Newsgathering operations routinely handle highly sensitive information, and they rely on a foundation of trust between reporters and their confidential sources. If a media organization concludes that entrusting its data with a cloud service provider will result in that data being less private or secure, then the organization is less likely to embrace cloud technologies**. …
>
> **This concern has been accentuated by the controversy surrounding** Edward **Snowden's disclosures** in 2013 **regarding government surveillance. Particularly for media organizations with headquarters or operations outside the U**nited **S**tates, **the Snowden disclosures increased concern that if the companies entrusted their data to a U.S. cloud provider, that would make it easier for U.S. law enforcement to obtain their data**.

For media companies, these are not abstract questions. As the Department of Justice (DOJ) recognized in updating its rules regarding subpoenas to reporters, **maintaining the confidentiality of the newsgathering process is essential to both a free press and a working democracy**. The DOJ now has strong guidelines governing the considerations that will be considered before subpoenas will be directed to reporters, but these are only internal guidelines and they only apply to the DOJ. **The bipartisan LEADS Act provides a path forward to update the law to permit the cloud to be more meaningful and useful to media companies — and to others concerned about the privacy and security of their data. And by doing so, Congress can bolster the competitiveness of an emerging and important area of our information economy**.

They Say: "CP Doesn't Solve Investigative Journalism"

Only the counterplan prevents foreign governments from accessing data from U.S. journalists.

Hatch 15 — Orrin G. Hatch, United States Senator (R-UT), currently serves as President pro tempore of the United States Senate, 2015 (Statement to The Media Institute Regarding the Law Enforcement Access to Data Stored Abroad Act, September 16th, Available Online at http://www.mediainstitute.org/PDFs/luncheonspeeches/Media%20Institute%20Speech%20on%20LEADS%20Act,%20September%2016,%202015.pdf, Accessed 10-28-2015, p. 2-3)

The government's position presents unique challenges for a number of industries, which increasingly face a conflict between American law and the laws of other countries. For example, **when tech**nology **companies receive demands from U.S. law enforcement to turn over data on behalf of foreign customers, they are forced to make a difficult decision: either comply with the demand and satisfy U.S. law or risk violating the privacy laws of the host country**.

No one should be placed in this untenable situation.

Moreover, **if federal officials can obtain e-mails stored anywhere in the world simply by serving a warrant on a provider subject to U.S. process, nothing stops governments in other countries**—including China and Russia—**from seeking e-mails of Americans stored in the U.S. from providers subject to Chinese and Russian process**.

Lest you think there are no reciprocal or far-reaching consequences, **imagine a scenario where China wants to access e-mails stored in the U**nited **S**tates. **Instead of going through established diplomatic channels or international treaties** to obtain those e-mails, **Chinese officials could go to a China-based company**, like Ali Baba, **and demand that it retrieve e-mails from its U.S. servers and turn them over**.

This disturbing hypothetical could well **become a reality because of our government's position on the extraterritorial reach of U.S. warrants**. In fact, the lawyer who is litigating the Microsoft case on behalf of the government acknowledged last week that the ability for a foreign government to require disclosures of a U.S. provider "should be of some concern." [end page 2]

As media organizations, you are particularly sensitive to these issues. Here **in the U**nited **S**tates **we respect free speech and media independence. Your newsrooms are free from government search or censure. Yet, because of this Administration's position on the extraterritorial reach of warrants, your rights could be circumvented by foreign law enforcement agencies seeking to access your confidential information—even if it is stored in the U**nited **S**tates.

Recognizing the dangerous precedent our government's position could set, a group of media organizations filed an amicus brief in the Second Circuit case.

Let me read an excerpt from their brief: "**[F]or those countries that are already taking extra-legal measures to try to penetrate and monitor journalists' e-mails, the government's position offers a far easier approach: simply raid the local office of a service provider and demand that a local employee retrieve the desired information remotely from U.S.-based accounts. This scenario would cause certain outrage in the U**nited **S**tates**—and rightly so**."

Without an appropriate legal framework, the current state of affairs regarding extraterritorial use of warrants puts the privacy of American citizens at risk.

That is why I introduced the LEADS Act: to promote international comity and law enforcement cooperation. To date, the bill has received broad bipartisan support in both the Senate and the House of Representatives and from trade associations and the business community.

The proposed legislation would clarify ECPA by stating that the U.S. government cannot compel the disclosure of data from U.S. providers stored abroad if (1) **accessing that data would violate the laws of the country where it is stored or** (2) **the data is not associated with a U.S. person**— that is, a citizen or lawful permanent resident of the United States, or a company incorporated in the United States.

They Say: "CP Doesn't Solve Cybersecurity"

The counterplan solves their cybersecurity advantage — MLAT reform is key to effective cyber investigations.

Fidler 15 — Mailyn Fidler, Marshall Scholar and M.Phil. Candidate in International Relations at Oxford University, Research Fellow at the Center for Applied Cybersecurity Research at Indiana University Bloomington, former Policy Consultant for Google, holds a B.A. in Science, Technology, Society from Stanford University, 2015 ("MLAT Reform: Some Thoughts from Civil Society," *Lawfare*—a scholarly blog curated by the Brookings Institution, September 11th, Available Online at https://www.lawfareblog.com/mlat-reform-some-thoughts-civil-society, Accessed 11-02-2015)

Security Implications of MLATs

MLA processes most immediately have implications for law enforcement and companies (including the future of data localization) **but also for national and cyber security. As encryption adoption increases, MLATs will become more important. When interception becomes less useful because of encryption adoption, two options usually remain: hacking or legal requests for data sharing. The spectre of local law enforcement hacking across borders encourages the development of a workable MLA process. Such hacking**—and other workarounds, such as calling foreign companies before local courts or laws mandating data access—also **raises concerns about comity. Workable MLATs may help ensure national sovereignty remains unruffled by normal criminal investigations**.

They Say: "CP Doesn't Solve Cybersecurity"

MLAT reform is vital to cybersecurity — nearly all attacks are transnational.

Swire and Hemmings 15 — Peter Swire, Nancy J. and Lawrence P. Huang Professor of Law and Ethics at the Georgia Institute of Technology, Senior Counsel with Alston & Bird LLP—an international law firm, Senior Fellow with the Future of Privacy Forum, Policy Fellow with the Center for Democracy and Technology, served on President Obama's Review Group on Intelligence and Communications Technology, served as President Obama's Special Assistant to the President for Economic Policy, served as Chief Counselor for Privacy in the U.S. Office of Management and Budget during the Clinton Administration, recipient of the Privacy Leadership Award from the International Association of Privacy Professionals, holds a J.D. from Yale Law School, and Justin D. Hemmings, Research associate at the Georgia Institute of Technology, Policy Analyst at Alston & Bird LLP—an international law firm, holds a J.D. from the Washington College of Law at American University, 2015 ("Re-Engineering the Mutual Legal Assistance Treaty Process," Draft of a Paper that will be published in the *NYU Annual Survey of American Law*, Available Online at http://www.heinz.cmu.edu/~acquisti/SHB2015/Swire.docx, Accessed 11-02-2015)

A. Factual Changes Leading to the Increased Importance of MLATs

We emphasize **two factual changes** that **are leading to the increased importance of MLATs:** (1) **the trans-border nature of many cyber-crime and cyber-security investigations; and** (2) **the reasons why increased use of encryption shifts law enforcement from real-time wiretaps to access to stored records in the cloud, often stored in other countries**.

1. The trans-border nature of cyber-crime and cyber-security investigations. **Even before** the **Snowden** revelations began in 2013, **MLATs were becoming more important due to the trans-border nature of many cyber-crime and cyber-security investigations**. In the physical world, the thief and the victim are typically in the same country, so there is rarely any need to seek records abroad. **On the Internet,** by contrast, **data breaches and other cyber-crime often involve a foreign perpetrator and a domestic victim. Law enforcement thus far more often has reason to seek records abroad while tracking down criminals**. Indeed, the experience of one of the authors (Swire) is that major spam operations that target U.S. individuals have shifted over time from domestic to foreign; the ability to track down perpetrators is high enough within the U.S. that it is only lucrative for spam rings to operate from overseas.

A similar pattern exists for cyber-security. After commercial use of the Internet began in the 1990's, U.S. law enforcement succeeded in getting legal changes, such as nationwide service of process for federal investigations, that enable relatively effective investigations into the source of attacks from within the country. The focus of effort thus has shifted over time to methods for detecting and countering cyber-attacks that originate from, or are routed through, other countries. MLATs are one tool for gaining evidence about such attacks.

2. Why encryption drives law enforcement to seek records in the cloud, by use of MLATs. **The increasing use of encryption** for on-line communications **is a strong accelerator of this trend toward law enforcement seeking evidence from abroad**. The reasons are set forth in a 2012 article by Swire called "From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud." The central point is that **encryption makes traditional wiretaps far less likely to be effective; in the absence of wiretaps, law enforcement is driven to the place in the system where data is unencrypted. For e-mails and many other forms of electronic evidence, that place turns out to be the cloud. For many non-U.S. law enforcement investigations, the cloud turns out to be a server in the U**nited **S**tates. **The way to gain access to that server is through an MLAT**.

They Say: "CP Doesn't Solve Cybersecurity"

MLAT reform turns encryption — the counterplan prevents law enforcement from "going dark" by ensuring access to cloud data. This reduces pressure for backdoors.

Swire and Hemmings 15 — Peter Swire, Nancy J. and Lawrence P. Huang Professor of Law and Ethics at the Georgia Institute of Technology, Senior Counsel with Alston & Bird LLP—an international law firm, Senior Fellow with the Future of Privacy Forum, Policy Fellow with the Center for Democracy and Technology, served on President Obama's Review Group on Intelligence and Communications Technology, served as President Obama's Special Assistant to the President for Economic Policy, served as Chief Counselor for Privacy in the U.S. Office of Management and Budget during the Clinton Administration, recipient of the Privacy Leadership Award from the International Association of Privacy Professionals, holds a J.D. from Yale Law School, and Justin D. Hemmings, Research associate at the Georgia Institute of Technology, Policy Analyst at Alston & Bird LLP—an international law firm, holds a J.D. from the Washington College of Law at American University, 2015 ("Re-Engineering the Mutual Legal Assistance Treaty Process," Draft of a Paper that will be published in the *NYU Annual Survey of American Law*, Available Online at http://www.heinz.cmu.edu/~acquisti/SHB2015/Swire.docx, Accessed 11-02-2015)

3. More efficient MLATs can counter the perceived risks of strong encryption. An additional reason, which deserves more extensive deliberation, is that **an effective MLAT process can reduce concerns by law enforcement officials that they are "going dark" due to more pervasive use of encryption technology; efficiently-filled MLAT requests that can access emails and other records in plaintext at the server are an attractive alternative to approaches supported by** FBI Director **Comey and** UK Prime Minister **Cameron for weakening encryption technologies**.

For the same reason that law enforcement has begun seeking access to the cloud, making that access easier for other justified law enforcement requests would give officials concerned about strong device encryption an alternative means of accessing important data. No matter how well encrypted an individual devices are, **true end-to-end encrypted transfers of data are rare. Law enforcement can therefore often access the data in unencrypted format on whatever server or servers the target's device uses, addressing the need to break the device encryption entirely**. Swire has written previously about the risks of weakening encryption and to providing government backdoors, such as concerns about the backdoors being abused or discovered by malicious parties. . Indeed, **the foundation of Internet commerce relies on strong and trusted encryption, and weakening those standards could pose greater risks to a key commercial infrastructure. If a better, more efficient MLAT process can assuage the concerns of those seeking to weaken encryption standards, then it seems a safer and easier fix than key escrow to address the issues raised by** Director **Comey**, Prime Minister Cameron, and those that share their specific concern.

They Say: "CP Links To Terrorism DA"

No it doesn't — it preserves NSA's critical intelligence authorities and strengthens global law enforcement cooperation. The counterplan *alone* decreases the risk of terrorism; the plan and permutation increase the risk.

MLAT reform solves terrorism — the counterplan fosters global law enforcement cooperation. This is vital to effective counter-terrorism — that's Cunningham.

They Say: "CP Links To Presidential War Powers DA"

No it doesn't — it preserves the President's intelligence gathering authority. The counterplan only constrains law enforcement, not the intelligence community. The President needs flexible power to gather intelligence to wage the war on terrorism — only the counterplan preserves it.

They Say: "CP Links To EU Tech Sector DA"

Correct — that's not our net-benefit.

They Say: "Data Localization DA"

( ) Turn — LEADS prevents data localization.

NAM 15 — National Association of Manufacturers, 2015 ("Questions & Answers: Law Enforcement Access to Data Stored Abroad Act," January 1st, Available Online at http://www.nam.org/Issues/Technology/LEADS-Act/LEADS-Act-Q-A.pdf, Accessed 11-03-2015, p. 2-3)

Would the **LEADS** Act lead to data localization efforts by other countries?

A: No, this bill **will not increase localization efforts. Section 5** of the Act **specifically provides that data localization requirements are incompatible with the borderless nature of the Internet, an impediment to online innovation, unnecessary in order to meet the needs of law enforcement, and that the U**nited **S**tates **should pursue open data flow policies with foreign nations**.

The bill distinguishes primarily between content held on behalf of U.S. persons and content held on behalf of non-U.S. persons. The key issue is therefore **the nationality of the customer—not the nation in which the stored data is located**. Under the Act, when a provider receives a valid warrant for content belonging to a U.S. person, it must disclose that content—regardless of where the data is stored. That requirement is the same for all providers, and it does not depend on how or where a provider stores that person's data. The only exception is when the provider challenges the disclosure because it would violate foreign law. **We think this approach will focus attention on the nationality of a provider's account holders, rather than on the locations in which a provider stores data, thereby reducing any localization concerns. The LEADS Act will remove an argument that other countries can currently use to create data localization laws and mandate use of domestic companies**.

This framework will help resolve the problem that providers regularly confront of conflicting legal obligations from different jurisdictions. The conflicting laws and obligations on providers results [end page 2] **in de facto localization of data today; the LEADS Act takes an important step toward reversing that trend, by establishing a clear framework for accessing data stored across borders, with a process that protects providers from violating the laws of another jurisdiction**.

They Say: "Data Localization DA"

( ) Turn — MLAT reform prevents data localization.

Swire and Hemmings 15 — Peter Swire, Nancy J. and Lawrence P. Huang Professor of Law and Ethics at the Georgia Institute of Technology, Senior Counsel with Alston & Bird LLP—an international law firm, Senior Fellow with the Future of Privacy Forum, Policy Fellow with the Center for Democracy and Technology, served on President Obama's Review Group on Intelligence and Communications Technology, served as President Obama's Special Assistant to the President for Economic Policy, served as Chief Counselor for Privacy in the U.S. Office of Management and Budget during the Clinton Administration, recipient of the Privacy Leadership Award from the International Association of Privacy Professionals, holds a J.D. from Yale Law School, and Justin D. Hemmings, Research associate at the Georgia Institute of Technology, Policy Analyst at Alston & Bird LLP—an international law firm, holds a J.D. from the Washington College of Law at American University, 2015 ("Re-Engineering the Mutual Legal Assistance Treaty Process," Draft of a Paper that will be published in the *NYU Annual Survey of American Law*, Available Online at http://www.heinz.cmu.edu/~acquisti/SHB2015/Swire.docx, Accessed 11-02-2015)

D. Conclusion: MLATs as Synecdoche

As mentioned above, one U.S. official with a literary sensibility has suggested that **MLATs are becoming a synecdoche for international Internet cooperation in the wake of Snowden**. As just discussed, **MLATs and localization proposals are enmeshed in broad issues such as anger at U.S. surveillance practices, protectionist economic impulses, and efforts to bargain with the U.S. to change surveillance practices going forward. Even more broadly, the localization impulse is closely correlated with the U**nited **N**ations/International Telecommunications Union **approach to Internet governance, where each nation plays a more central role in defining how communications and data are handled within that nation. Frustration with the MLAT process feeds into this nation-focused approach to the Internet, counter to the open, interoperable, and international model of communications that the U**nited **S**tates **has fostered and should favor**. Put differently, **we should fix the MLAT process to take away a major excuse for a localized and worse Internet**.

( ) No Localization — countries aren't following through on their threats.

Davies 14 — Simon Davies, Visiting Senior Fellow at the London School of Economics, Director of Privacy International, Advisory Board Member at the Future of Privacy Forum, the Electronic Privacy Information Center, and the Foundation for Information Policy Research, 2014 ("A Crisis of Accountability: A global analysis of the impact of the Snowden revelations," *The Privacy Surgeon*, June, Available Online at http://www.privacysurgeon.org/blog/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf, Accessed 11-03-2015, p. 5)

The Snowden disclosures have triggered a noticeable shift in thinking across the world toward increased awareness of the importance of accountability, transparency and the rule of law with regard to both the activities of **security agencies and** the value of **privacy**. This shift - in many parts of the world - has empowered civil society, created a resurgence of interest in legal protections and sensitised media to key issues that have hitherto escaped public scrutiny at any substantial level.

This shift notwithstanding, the overwhelming majority of countries assessed in this report **have not responded in any tangible, measurable way to the Snowden disclosures** that began in June 2013. **While there has been a notable volume of "activity" in the form of diplomatic representations, parliamentary inquiries, media coverage, campaign strategies, draft legislation and industry initiatives, there has – at the global level – been an insignificant number of tangible reforms adopted to address the concerns raised by the Snowden disclosures. Two thirds of legal professionals and technology experts from 29 countries surveyed for this study reported that they could recall no tangible measure taken by government**.

They Say: "Data Localization DA"

( ) Internet Freedom Low — countries are cracking down on online expression.

VOA 15 — Voice of America News, 2015 ("Global Internet Freedoms Decline Fifth Year in a Row," Byline Doug Bernard, October 28th, Available Online at http://www.voanews.com/content/global-internet-freedoms-decline-fifth-year-in-a-row/3025985.html, Accessed 11-03-2015)

When it comes to protecting freedom of expression online, the news is not good.

For the fifth straight year in a row, the World Wide Web became less free for millions of people, as governments around the world continued restricting online expression, censoring websites and cracking down on a variety of tools designed to protect user privacy.

That's the conclusion of a new report, "Freedom on the Net 2015," **released** Wednesday **by Freedom House, a nonprofit promoting democracy and free expression globally. It's the sixth annual survey of 65 governments and their policies regarding censoring online content, electronic surveillance, and how they may punish citizens whose online activities they disapprove of**.

"**Internet freedom on a global scale is continuing to decline**," **said** Laura **Reed, a research analyst for the Freedom on the Net project**. "**This is a decline we've seen over the past five years, but now we're seeing a lot more of these declines coming from new laws being passed**."

Among the greatest threats to online freedom, Reed told VOA, **are an escalation in Internet user intimidation and arrest, the growing number of nations conducting surveillance** – whether publicly acknowledged or not – **and new efforts to remove, rather than merely block, offensive content**.

"**The most surprising shift was from blocking to the removal of content**," Reed said. "**Now that we're seeing governments target content at the source, it's really concerning; both in the sense that that content is removed forever, and also the pressure they bring with that – on social media companies, on individuals**."

They Say: "Data Localization DA"

( ) No Human Rights Impact — internet freedom doesn't prevent authoritarianism.

Morozov 10 — Evgeny Morozov, Yahoo! Fellow at the Institute for the Study of Diplomacy at Georgetown University, former Fellow at the Open Society Foundation, 2010 ("The Digital Dictatorship," *Wall Street Journal*, February 20th, Available Online at http://www.wsj.com/articles/SB10001424052748703983004575073911147404540, Accessed 11-03-2015)

It's easy to see why a world in which young Iranians embrace the latest technology funded by venture capitalists from Silicon Valley, while American diplomats sit back, sip tea and shovel the winter snow on a break from work, sounds so appealing. But is such a world achievable? Will Twitter and Facebook come to the rescue and fill in the void left by more conventional tools of diplomacy? **Will the oppressed masses in authoritarian states join the barricades once they get unfettered access to Wikipedia and Twitter?**

This seems quite unlikely. In fact, **our debate about the Internet's role in democratization—increasingly dominated by techno-utopianism—is in dire need of moderation, for there are** at least as **many reasons to be skeptical**. Ironically, the role that the Internet played in the recent events in Iran shows us why: **Revolutionary change that can topple strong authoritarian regimes requires a high degree of centralization among their opponents. The Internet does not always help here. One can have "organizing without organizations"**—the phrase is in the subtitle of "Here Comes Everybody," Clay Shirky's best-selling 2008 book about the power of social media—**but one can't have revolutions without revolutionaries**.

Contrary to the utopian rhetoric of social media enthusiasts, the Internet often makes the jump from deliberation to participation even more difficult, thwarting collective action under the heavy pressure of never-ending internal debate. This is what may explain the impotence of recent protests in Iran: Thanks to the sociability and high degree of decentralization afforded by the Internet, Iran's Green Movement has been split into so many competing debate chambers—some of them composed primarily of net-savvy Iranians in the diaspora—that it couldn't collect itself on the eve of the 31st anniversary of the Islamic revolution. The Green Movement may have simply drowned in its own tweets.

The government did its share to obstruct its opponents, too. Not only did it thwart Internet communications, the government (or its plentiful loyalists) also flooded Iranian Web sites with videos of dubious authenticity—one showing a group of protesters burning the portrait of Ali Khamenei—that aimed to provoke and splinter the opposition. In an environment like this—where it's impossible to distinguish whether your online interlocutors are your next-door neighbors, some hyperactive Iranians in the diaspora, or a government agent masquerading as a member of the Green Movement—who could blame ordinary Iranians for not taking the risks of flooding the streets only to find themselves arrested?

Our earlier, unfounded expectations that the Internet would make it easy for the average citizens to see who else is opposing the regime and then act collectively based on that shared knowledge may have been inaccurate. In the age of the Spinternet, when cheap online propaganda can easily be bought with the help of pro-government bloggers, elucidating what fellow citizens think about the regime may be harder than we thought. Add to that the growing surveillance capacity of modern authoritarian states—also greatly boosted by information collected through social media and analyzed with new and advanced forms of data-mining—**and you may begin to understand why the Green Movement faltered**.

They Say: "Conditionality Bad"

Conditionality is good —

( ) Most Logical — the judge should never be forced to choose between a bad plan and a bad counterplan when the status quo is a logical third option. Logic is an objective and fair standard that teaches valuable decision-making skills.

( ) Argument Innovation — because debaters are risk-averse, they won't introduce new positions unless they retain a reliable fallback option. Innovation keeps the topic interesting and encourages research and preparation.

( ) Gear-Switching — being able to change gears and defend different positions over the course of a debate teaches valuable negotiation skills and improves critical thinking. Deciding what to go for is a useful skill.

( ) No Infinite Regression — each additional position has diminishing marginal utility. We've only read one counterplan. This is reciprocal: they get the plan and permutation and we get the counterplan and status quo.

( ) Strongly Err Neg — the judge should be a referee, not a norm-setter. Unless we made the debate totally unproductive, don't vote on conditionality — doing so gives too much incentive for the aff to abandon substantive issues in pursuit of an easy theory ballot.

2AC — LEADS Act CP

( ) Permute: Do Both — enact the plan *and* LEADS. They aren't mutually exclusive. This solves their MLAT reform net-benefit.

( ) No Solvency — LEADS alone doesn't solve. Curtailing NSA surveillance is vital.

Fein 15 — Bruce Fein, Constitutional Lawyer, former Visiting Fellow for Constitutional Studies at the Heritage Foundation, former General Counsel to the Federal Communications Commission, served as Assistant Director for the Office of Policy and Planning, Special Assistant to the Assistant Attorney General for Antitrust, and Associate Deputy Attorney General under President Ronald Reagan, served as Special Assistant to the Assistant Attorney General for the Office of Legal Counsel in the U.S. Department of Justice during the Nixon impeachment investigation, holds a J.D. from Harvard Law School and a B.A. in Political Science from the University of California-Berkeley, 2015 ("Protecting Privacy in a Politically Balkanized World: Sailing Between Scylla and Charybdis," *The Huffington Post*, October 21st, Available Online at http://www.huffingtonpost.com/bruce-fein/protecting-privacy-in-a-p_b_8349716.html, Accessed 10-27-2015)

Microsoft's president argues in favor of an international legal regime in which privacy rights in the form of personal data or otherwise **move across borders. As applied to the U**nited **S**tates **and** the **EU, this would mean that the U.S. government would demand information stored only in the U**nited **S**tates; **and, in making such demands, the U**nited **S**tates **would honor the privacy rules of the EU if the target of the demand was an EU national. This approach bears similarities to** the pending Law Enforcement Access to Data Stored Abroad Act (**LEADS**).

United States judges, however, are amateurs of EU privacy rules--including the recently minted right to be forgotten. More important, the **NSA, acting under Executive Order 12333**, **and** the **F**oreign **I**ntelligence **S**urveillance **A**ct of 1978, as amended, **probably intercepts in real time virtually every email or phone call in the world**. (Pervasive secrecy and the NSA's penchant for dissembling make an authoritative conclusion problematic). **Privacy is massively breached by the U**nited **S**tates **government before storage of personal data, not afterwards**. And as with nuclear weapons, predator drones, or otherwise, it is only a matter of time before the EU, China, Russia, Japan, Israel etc. acquire NSA-like capabilities to intercept unfathomable volumes of personal information during transmission before storage.

In sum, **a priority in privacy protection** today **should focus government Panopticon-like seizures of electronic communications. The companion approaches suggested by** Microsoft and **LEADS are constructive, but will be eclipsed if Big Brother government is not prevented**.

( ) Links To Terrorism DA — LEADS makes it harder for law enforcement to access electronic communications by requiring a warrant to access cloud data. If the plan links, so does the counterplan.

( ) Links To Presidential War Powers DA — LEADS restricts the executive branch's surveillance power by requiring a warrant to access cloud data. If the plan links, so does the counterplan.

2AC — LEADS Act CP

( ) Data Localization DA:

A. LEADS causes data localization.

MacCarthy 15 — Mark MacCarthy, Senior Vice President of Public Policy at the Software and Information Industry Association—the principal trade association for the software and digital content industry, Adjunct Faculty Member with the Communication, Culture, and Technology Program at Georgetown University, holds a Ph.D in Philosophy from Indiana University and an M.A. in Economics from the University of Notre Dame, 2015 ("A Better Way to Think About the Microsoft-Ireland Case," *SIAA Blog*—the Software & Information Industry Association's blog, September 8th, Available Online at http://blog.siia.net/index.php/2015/09/a-better-way-to-think-about-the-microsoft-ireland-case/, Accessed 10-27-2015)

This is a no-win situation. No matter what the outcome of the court case, the result is miserable for U.S. business, U.S. citizens and indeed for all who rely on a free and open global Internet. So it is important to re-think the issue. The good news is that Congress is considering legislation. Senators Hatch and Coons have introduced **the LEADS Act** which **is flawed, but a good first step** toward setting up a workable jurisdictional framework.

The bill says that U.S. law enforcement can access information about a U.S. citizen through a warrant served on a U.S. company, regardless of where the data is stored.

However, when information about a foreign national is stored overseas, the warrant to the U.S. company would not be valid.

The bill rightly disregards location when dealing with U.S. citizens, but oddly makes it determinative when dealing with foreign nationals. As a result, if a U.S. company stored information about a foreign national in the United States, it would be subject to U.S warrants, even though the person involved lived abroad and was subject to foreign jurisdiction. To protect their citizens, then, other countries would require that information about their citizens not be stored in the United States.

So, the LEADS Act as drafted will foster mandated data localization rules. It creates incentives for other countries to require data to be hosted outside the U.S., so as to avoid U.S. jurisdiction.

Basing the validity of warrants on the location of data is inconsistent with cloud computing norms, one of the leading forms of computing for the Internet. Cloud computing often relies upon storing data in multiple locations for redundancy, security, and latency. The LEADS Act legislates against this 21st century business model attuned to the needs of a global economy.

2AC — LEADS Act CP

B. Data localization crushes global internet freedom.

Hill 14 — Jonah Force Hill, Technology Policy Consultant at Monitor 360—a consulting firm, Fellow of the Global Governance Futures 2025 Program at the Brookings Institution, Adjunct Fellow with the Strategic Technologies Program at the Center for Strategic and International Studies, former International and Global Affairs Fellow at the Kennedy School of Government at Harvard University, served in the Office of the Cybersecurity Coordinator at the White House, holds an M.P.P. from the Kennedy School of Government at Harvard University, 2014 ("The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," Lawfare Research Paper Series, Volume 2, Number 3, July 21st, Available Online at https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf, Accessed 11-03-2015, p. 33-34)

C. Free Expression & Internet Freedoms Are Not Well-Served

Most troubling of all the potential harms of data localization is its effect on free expression and Internet freedom. This is ironic, in that to many of its advocates, data localization is a remedy to the threat posed by the NSA to free expression and Internet freedom. I suggest that the opposite is actually true, that the "remedy" only serves to make the danger greater.

The Internet and other online media have become indispensable tools for individuals to communicate globally, and have furthered individual participation in the political process, increased transparency of governmental activities, and promoted fundamental rights. Data localization, by centralizing control over digital infrastructure, can diminish this capacity in a number of ways. As was discussed above, **data localization** as a local server or local data storage requirement **can limit freedom by permitting countries more easily to collect information on their citizens** (through domestic surveillance). **It allows a government more quickly and effectively to shut down Internet services** (usually via legal threats to local Internet service providers) **that the government believes is abetting unwanted political opposition**.121

Data localization mandates also can obstruct Internet freedom in other, indirect ways. Restricted routing, in particular, **is problematic**, **because it is not technically possible as the existing Internet is designed or organized**. Unlike the telephone network, **the Internet operates under a model known as "best effort delivery," where data is delivered to its destination in the most efficient manner possible, without predetermined routes**. For instance, data sent from the United States to Botswana will attempt to travel along the shortest and most direct route possible. However, if there is a bottleneck along the shortest route, a packet may find a longer but more expeditious route. **This is a core feature of the Internet that makes network congestion easy to navigate around. In order to restrict data routing to specific geographies as governments are advocating, all Internet routers that are currently programmed to follow this "best effort" routing model would have to be reconfigured to prohibit data from one country from moving through the territory of "prohibited" countries**. Moreover, **since Internet addresses are not always assigned according to a specific geography, the Internet's addressing system currently would have to be dramatically altered as well**. Thus, the Border Gateway Protocol (one of the core Internet networking protocols), the Internet's routing tables (the address books by which routers send data), and the process by which IP addresses are allocated, would all have to be modified. **Such an undertaking would require a fundamental overhaul not only of the Internet's operating structures, but also of** [end page 33] **the governance structures by which those structures are implemented and standardized**.

These are not just arcane concerns of those involved in Internet governance, although they surely are matters that greatly trouble those who favor an efficient and interoperable Internet. **These alterations in the way the Internet works will**, I believe, **materially restrict the power of the Internet to support free expression. These modifications to these core characteristic of the current Internet**—modifications **that localization would require**—**may result in intelligence agencies acquiring a previously unavailable capacity to assess where data had originated and where it was heading, because the origin and destination information would be included in the data packet**.122 **A centralized governance process**, further, which would be required to change the routing protocols and IP allocation system, **would give authoritarian countries significantly more influence over how information on the Internet is regulated**. In fact, **this is one of the main reasons why China, Russia, many Arab states (among others) have pushed for tracked routing protocols in the past**,123 just as they have lobbied for a handover of the global Internet governance system to the U.N.'s International Telecommunications Union.124

[Evidence Continues — No Text Removed]

2AC — LEADS Act CP

[Continued from Previous Page]

In short, **localization would require dramatic changes to the current structure of the Internet**, changes **that would have adverse consequences for those who see it as** a principal—if not **the principal**—**means of global democratization**. For some, those adverse consequences would be unintended; more chillingly, there are those who intend precisely those consequences. **This would be an enormous price to pay**, particularly **since the other objectives** that are **promoted as justifications for localization**—namely, security for communications and economic development—**are illusory**.

2AC — LEADS Act CP

C. Internet freedom is the lynchpin of global human rights.

Coons 12 — Chris Coons, Member of the United States Senate (D-DE), holds a J.D. from Yale Law School, 2012 ("Internet Freedom Is a Human Right," *The Huffington Post*, July 10th, Available Online at http://www.huffingtonpost.com/chris-coons/internet-freedom-is-a-hum_b_1506042.html, Accessed 11-03-2015)

Sometimes it's called "information security." Other times, it's called "Internet management," or a "hate-free Internet." Whatever the code-name for it, **too many foreign governments**, including Syria, Iran and China, **restrict Internet freedom as a tool for suppressing free speech, free assembly and a free press**.

Though the United States has invested tens of millions of dollars in defending Internet freedom around the world in recent years -- including by equipping censored populations with technologies to evade digital repression -- **we can and must do more to ensure Internet freedom remains a fundamental tenet of U.S. foreign policy**.

With nearly one-third of mankind -- some **two billion people** -- **now online, the Internet has clearly become the public square of the 21st century**. It is where ideas are exchanged, viewpoints are debated, and commerce takes place, and in this modern, networked world, we must ensure the right to free expression is as protected online as they are offline.

There is deep bipartisan support in Congress for robust U.S. engagement to secure digital freedom around the world. In fact, the Senate Global Internet Freedom Caucus, led by Senators Mark Kirk (R-Ill.), Bob Casey (D-Pa.) and myself, and the House Global Internet Freedom Caucus, led by Representative Chris Smith (R-N.J.) are teaming up today with the Center for a New American Security for a discussion of U.S. policy to promote Internet freedom globally.

The Internet can be used as a tool of liberation, as we saw in revolutions that swept the Arab world last spring, **or of repression, as we continue to witness in places such as Iran and China. Popular movements and entrenched governments both clearly see how the unique power of the Internet can spread democratic ideas and demands for human rights and basic freedoms**.

These fundamental values, which should be granted to citizens around the world as enshrined in the Universal Declaration of Human Rights, are central to who we are as Americans.

We must continue to pursue an American foreign policy that protects the "right to connect" as a U.S. foreign policy priority. The Senate Global Internet Freedom Caucus advocates for the promotion of policies that promotes rights of all people to use the Internet and other forms of technology to exercise basic freedoms globally. In order to achieve this goal, **we must** engage with governments, individuals, and the private sector to **preserve the Internet as an open platform for commerce and communication**.

Led by Secretary of State Hillary Clinton, this administration has recognized the "right to connect" as a fundamental human right, and the American people have already made a significant investment of more than $70 million since 2008 in protecting and promoting Internet freedom globally. This funding has supported a number of projects, including the development of censorship-circumvention technology, cyber self-defense training, and equipping people to evade repression.

Despite remarkable innovations in technology, there is more work to be done, as restrictions to Internet access and online censorship, manipulation, and monitoring continue to rise around the world. **U.S. global leadership is critical if we are to make progress** in this area, and we cannot be hampered by the false perception that global Internet freedom is at odds with domestic cyber security measures and the protection of intellectual property. In fact, these policies can and should complement each other. We can implement vigorous standards to protect intellectual property and network security while still wholeheartedly supporting Internet freedom globally.

Internet freedom – the freedom to exchange thought, opinion, expression, and association to meet political, social, education, or religious objectives – should not be restricted for law-abiding citizens in the United States or **anywhere in the world. Advancing this right in repressive regimes across the globe must be a fundamental tenet of our foreign policy in the 21st century. As with all great moral challenges we face as an international community, continued American leadership and engagement is essential if we are to succeed**.

2AC — LEADS Act CP

D. Survival is at risk — human rights prevent mass violence.

Annas et al. 2 — George J. Annas, Edward R. Utley Professor and Chair of the Health Law Department at the Boston University School of Public Health, Professor of SocioMedical Sciences and Community Medicine at Boston University School of Medicine, Professor of Law at Boston University School of Law, holds a J.D. from Harvard Law School and an M.P.H. from Harvard School of Public Health, et al., with Lori B. Andrews, Distinguished Professor of Law at the Chicago-Kent College of Law, Director of the Institute for Science, Law, and Technology at the Illinois Institute of Technology, holds a J.D. from Yale Law School, and Rosario M. Isasi, Health Law and Bioethics Fellow in the Health Law Department at the Boston University School of Public Health, holds a J.D. from Pontificia Universidad Catolica del Peru and an M.P.H. from the Boston University School of Public Health, 2002 ("Protecting the Endangered Human: Toward an International Treaty Prohibiting Cloning and Inheritable Alterations," *American Journal of Law & Medicine* (28 Am. J. L. and Med. 151), Available Online to Subscribing Institutions via Lexis-Nexis)

II. Human Rights and the Human Species

The development of the atomic bomb not only presented to the world for the first time the prospect of total annihilation, but also, paradoxically, led to a renewed emphasis on the "nuclear family," complete with its personal bomb shelter. The conclusion of World War II (with the dropping of the only two atomic bombs ever used in war) led to the recognition that world wars were now suicidal to the entire species and to the formation of the United Nations with the primary goal of preventing such wars. n2 Prevention, of course, must be based on the recognition that all humans are fundamentally the same, rather than on an emphasis on our differences. In the aftermath of the Cuban missile crisis, the closest the world has ever come to nuclear war, President John F. **Kennedy**, in an address to the former Soviet Union, **underscored the necessity for recognizing similarities for our survival:**

> **Let us not be blind to our differences, but let us also direct attention to our common interests and the means by which those differences can be resolved** . . . . For, **in the final analysis, our most basic common link is that we all inhabit this small planet**. We all breathe the same air. We all cherish our children's future. And we are all mortal. n3

That we are all fundamentally the same, all human, all with the same dignity and rights, is at the core of the most important document to come out of World War II, the **Universal Declaration of Human Rights**, and the two treaties that followed it (together known as the "International Bill of Rights"). n4 **The recognition of universal human rights, based on human dignity and equality as well as the principle of nondiscrimination, is fundamental to the development of a species consciousness**. As Daniel Lev of Human Rights Watch/Asia said in 1993, shortly before the Vienna Human Rights Conference:

> **Whatever else may separate them, human beings belong to a single biological species, the simplest and most fundamental commonality before which the significance of human differences quickly fades**. . . . **We are all capable, in exactly the same ways, of feeling pain, hunger,** [*153] **and a hundred kinds of deprivation. Consequently, people nowhere routinely concede that those with enough power to do so ought to be able to kill, torture, imprison, and generally abuse others**. . . . **The idea of universal human rights shares the recognition of one common humanity, and provides a minimum solution to deal with its miseries**. n5

Membership in the human species is central to the meaning and enforcement of human rights, and respect for basic human rights is essential for the survival of the human species. The development of the concept of "crimes against humanity" was a milestone for universalizing human rights in that it recognized that there were certain actions, such as slavery and genocide, that implicated the welfare of the entire species and therefore merited universal condemnation. n6 Nuclear weapons were immediately seen as a technology that required international control, as extreme genetic manipulations like cloning and inheritable genetic alterations have come to be seen today. In fact, cloning and inheritable genetic alterations can be seen as crimes against humanity of a unique sort: they are techniques that can alter the essence of humanity itself (and thus threaten to change the foundation of human rights) by taking human evolution into our own hands and directing it toward the development of a new species, sometimes termed the "posthuman." n7 It may be that species-altering techniques, like cloning and inheritable genetic modifications, could provide benefits to the human species in extraordinary circumstances. For example, asexual genetic replication could potentially save humans from extinction if all humans were rendered sterile by some catastrophic event. But no such necessity currently exists or is on the horizon.

2AC — LEADS Act CP

( ) Conditionality is a Voting Issue — the neg should get the status quo *or* an unconditional counterplan, not both. Conditionality creates an unproductive argument culture because it values coverage more than engagement. This discourages in-depth clash and argument resolution (because less time is spent on each position) and lowers the barrier of entry for low-quality arguments (because the neg has a fallback option and is trying to distract the 2AC). Different advocacies should be debated in different debates, not crammed into this one. The judge is a norm-setter: vote for the theoretical position that best encourages high-quality debates.

2AC — Solvency Deficits (SSRA/Upstream)

( ) Doesn't Solve Constitutional Privacy — NSA will still use its X-Keyscore dragnet to sweep up millions of communications without a warrant. This crushes privacy and the Fourth Amendment — that's Lee. Even if the counterplan resolves one privacy harm, every violation of Constitutional privacy should be rejected — that's Solove. This outweighs the net-benefits because the Constitution can never be balanced away — that's Cole.

( ) Doesn't Solve Tech Competitiveness — foreign customers won't trust U.S. companies when they know NSA is engaging in dragnet surveillance. NSA reform is key — that's Donohue. This outweighs the net-benefits: competitiveness is vital to sustain U.S. leadership and prevent global conflict escalation — that's Goure and Lieber.

( ) Doesn't Solve Investigative Journalism — NSA's surveillance of journalists deters whistleblowers and undermines global press freedom. They fear intelligence agencies, not law enforcement — that's Froomkin and Marthoz. This outweighs the net-benefits: robust investigative journalism is vital to effective whistleblowing and social change that breaks down systems of oppression — that's Schenwar. The impact is suffering, death, and tyranny — that's Appelbaum.

2AC — Solvency Deficits (SDA/Encryption)

( ) Doesn't Solve Constitutional Privacy — NSA encryption backdoors violate privacy and the Fourth Amendment because they enable dragnet searches and seizures without a warrant. Only the plan solves — that's Mukunth. Even if the counterplan resolves one privacy harm, every violation of Constitutional privacy should be rejected — that's Solove. This outweighs the net-benefits because the Constitution can never be balanced away — that's Cole.

( ) Doesn't Solve Tech Competitiveness — foreign customers won't trust U.S. companies when they know NSA is engaging in dragnet surveillance. NSA reform is key — that's Donohue. This outweighs the net-benefits: competitiveness is vital to sustain U.S. leadership and prevent global conflict escalation — that's Goure and Lieber.

( ) Doesn't Solve Cybersecurity — NSA encryption backdoors devastate cybersecurity by introducing vulnerabilities into critical systems that adversaries can exploit — that's Open Letter and Crypto Experts. Strong encryption is the lynchpin of cybersecurity — that's Kehl. This outweighs the net-benefits because cyber attacks threaten grid collapse and nuclear war — that's Tilford. This is the most probable impact: even less extreme attacks have devastating consequences — that's Nolan.

Extend: "CP Doesn't Solve NSA"

The counterplan doesn't do anything about NSA surveillance.

Rosenzweig 15 — Paul Rosenzweig, Visiting Fellow in the Douglas and Sarah Allison Center for Foreign and National Security Policy of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy at The Heritage Foundation, Distinguished Visiting Fellow at the Homeland Security Studies and Analysis Institute, Professorial Lecturer in Law at George Washington University, Adjunct Professor at the Near East South Asia Center for Strategic Studies at the National Defense University, served as Deputy Assistant Secretary for Policy in the Department of Homeland Security, holds a J.D. from the University of Chicago Law School, 2015 ("E-mail Digital Privacy," *Saving Internet Freedom*—a Heritage Foundation Special Report, June 3rd, Available Online at http://www.heritage.org/research/reports/2015/06/saving-internet-freedom#_7emailprivacy, Accessed 11-03-2015)

ECPA reform must not be allowed to affect intelligence investigations and counterterrorism programs. The **F**oreign **I**ntelligence **S**urveillance **A**ct **has its own set of rules for government access to e-mail and documents stored in the "cloud." ECPA reform legislation will not affect those rules in any way**.

Extend: "Data Localization DA" — Link

LEADS causes data localization because it bases protections on geography — this crushes privacy.

Hill 15 — The Hill, 2015 ("Web giants warn email privacy bill would undermine protections," Byline Julian Hattem, February 12th, Available Online at http://thehill.com/policy/technology/232649-web-giants-warn-email-privacy-bill-would-undermine-protections, Accessed 10-27-2015)

New legislation designed to protect people's emails might have the unintended consequence of actually weakening their privacy on the Internet, major companies warned on Thursday.

The head of the Internet Association, which represents Silicon Valley giants including Google, Facebook, AOL and Yahoo, issued a statement on Thursday **criticizing** Sen. Orrin Hatch's (R-Utah) Law Enforcement Access to Data Stored Abroad (**LEADS**) Act.

"**Government surveillance laws that extend beyond U.S. borders are a significant problem for Internet companies and their global community of users, but** the **LEADS** Act, as currently written, **could incentivize data localization and therefore weaken user privacy**," trade group president Michael Beckerman said in a statement.

The bill from Hatch and Sens. Chris Coons (D-Del.) and Dean Heller (R-Nev.) seeks to update the 1986 Electronic Communications Privacy Act (ECPA), which allows law enforcement agencies to obtain emails and other digital information stored in the "cloud" without a warrant as long as they are more than 180 days old.

It also addresses an ongoing standoff between Microsoft and the Justice Department over evidence stored on a foreign server. The LEADS Act would prevent the government from nabbing data stored abroad if it is not associated with an American or would violate that host country's laws.

Tech companies have long urged for an update to the 1986 law, which they say is woefully out of date and puts users' privacy at risk. Lawmakers supporting the new legislation said that without it, foreign tech companies could gain a competitive advantage by telling people that American firms don't protect their data from the U.S. government.

BSA | The Software Alliance, another industry trade group, on Thursday said that the bill "affirms electronic privacy rights and helps rebuild consumer trust" without sacrificing law enforcement's powers.

But the Web trade group **took issue with its focus on where data is stored, which it warned might inspire host governments to clamp down on their operations and undermine online privacy**.

Extend: "Data Localization DA" — Link

The statement in the bill that opposes localization is irrelevant because it isn't binding.

Nojeim 14 — Greg Nojeim, Senior Counsel and Director of the Freedom, Security, and Technology Project at the Center for Democracy & Technology—a non-profit public policy organization, Member of the Data Privacy and Integrity Advisory Committee which advises the Department of Homeland Security on privacy matters, Co-Chair of the Coordinating Committee on National Security and Civil Liberties of the American Bar Association's Section on Individual Rights and Responsibilities, former Associate Director and Chief Legislative Counsel of the ACLU's Washington Legislative Office, holds a J.D. from the University of Virginia, 2014 ("LEADS Act Extends Important Privacy Protections, Raises Concerns," Center for Democracy and Technology, September 18th, Available Online at https://cdt.org/blog/leads-act-extends-important-privacy-protections-raises-concerns/, Accessed 10-27-2015)

Also, **we have to consider how foreign governments will react**. Some adverse consequences would be mitigated because the LEADS Act would make it clear that data stored in the U.S. could be disclosed only with a warrant. **Even if foreign governments copied the LEADS Act's extraterritorial assertion of authority over data regarding their own citizens, those governments could not unilaterally force U.S. companies to disclose data stored in the U.S. ECPA already protects that data and requires compliance with the MLAT process, and the LEADS Act enhances that protection. However, all stakeholders need to think carefully about how the LEADS Act would affect the global balance of privacy versus government power with respect to data U.S. providers store outside the U.S. for account holders who are not Americans**.

There is also **a risk that the LEADS Act will increase the pressure for data localization mandates. The bill includes language that puts the Senate on record as opposing data localization, but it may not be enough**.

Prefer our evidence — leading Internet companies agree that LEADS creates incentives to increase geographic tracking.

Godwin 15 — Mike Godwin, Director of Innovation Policy and General Counsel for R Street Institute—a non-profit and non-partisan public policy research organization, former General Counsel for the Wikimedia Foundation, former Staff Counsel for the Electronic Frontier Foundation, holds a J.D. from the University of Texas-Austin, 2015 ("Our Inboxes, Ourselves," *Future Tense*—a joint publication of *Slate*, the New America Foundation, and Arizona State University, September 14th, Available Online at http://www.slate.com/articles/technology/future_tense/2015/09/ecpa_reform_the_1986_email_privacy_law_might_finally_get_updated.single.html, Accessed 10-27-2015)

The fact is, **real public dialogue about the degree to which our communications deserve protection from government snooping hasn't yet happened. The best ECPA reform proposal** currently before Congress—S. 356, **the Lee-Leahy ECPA Amendments Act—would require warrants for content disclosure and would rationalize and simplify the ECPA's various provisions for how this is done. But despite its virtues, the bill is not aimed at metadata at all**.

Another ECPA reform bill—Sen. Orrin Hatch's Law Enforcement Access to Data Stored Abroad Act, or **LEADS** Act—**is more problematic than the Lee-Leahy bill**.* **The LEADS Act sets conditions under which companies have to disclose user information, including content, but those conditions raise difficult questions. Notably, the act bases its compliance obligations on whether the user is a U.S. citizen and whether, by producing information that resides on a foreign server, a company might be violating a foreign country's privacy laws**.

The author and sponsors of the LEADS Act mean well—the law would address a particular legal problem with which Microsoft has been wrangling—**but Internet companies like Google, Yahoo, and Facebook argue that the LEADS Act creates incentives both to track users' citizenship and to track the geographic location of user information at all times**.

Extend: "Data Localization DA" — Impact

Data localization crushes human rights.

Plaum 14 — Alexander Plaum, Writer at Access—an international human rights organization, 2014 ("The impact of forced data localisation on fundamental rights," *Access*, June 4th, Available Online at https://www.accessnow.org/blog/2014/06/04/the-impact-of-forced-data-localisation-on-fundamental-rights, Accessed 11-02-2015)

Neither ensuring security nor privacy, the adoption of forced data localisation measures could have a corrosive effect on human rights and the open, global nature of the internet. While many states have a knee-jerk desire to bring their citizens' data within their borders, a better way to protect users is this: Adopt high standards for privacy and data protection, speak out against surveillance operations that undermine the integrity of fibre optic cable systems, and advocate for rights-respecting surveillance policies and practices in line with the International Principles on the Application of Human Rights to Communications Surveillance.

Data localization undermines global privacy.

Plaum 14 — Alexander Plaum, Writer at Access—an international human rights organization, 2014 ("The impact of forced data localisation on fundamental rights," *Access*, June 4th, Available Online at https://www.accessnow.org/blog/2014/06/04/the-impact-of-forced-data-localisation-on-fundamental-rights, Accessed 11-02-2015)

A tool to target dissidents

Through the adoption of forced **data localisation** laws, **a government can increase control over its residents' online activities, raising the possibility of abuse and putting at risk citizens' right to privacy and freedom of expression**. Russia, for example, which already has one of the most pervasive surveillance programs in the world (the System for Operative Investigative Activities aka SORM), has recently approved a draft law on forced data localisation. If the Russian government is actually able to force service providers such as social media companies to store data locally, civil rights organizations, opposition members, investigative journalists, LGBT rights activists, and other groups at risk, will face an even more severe crackdown as sensitive, personally identifying information about them is exposed to the Russian government.

Some countries have already succeeded in adopting forced data localisation laws. This is the case in Vietnam, for example, where a combined censorship/forced data localisation law was introduced in September 2013. This law has made it mandatory for every online service provider to keep a copy of virtually all Vietnamese data on a local server, so national authorities can access it if needed. A few months later, in January 2014, the Indonesian government proposed a draft regulation going one step further; if adopted, this new law would mandate all data carriers including foreign banks operating in Indonesia to establish local data centres. The adoption of such laws in these two particular countries is especially worrisome given the high number of human rights violations already happening there.

Forced jurisdiction

Forced data localisation also means forced jurisdiction. If providers need to locate servers in a country, they also need to give up the legal protections they and their users have under other jurisdictions. The right to privacy, freedom of expression, and many more rights are at risk here. For instance, a European citizen's fundamental right to data protection might not be ensured if some of his or her data is stored locally under a jurisdiction outside of the EU.

Extend: "Data Localization DA" — Plan Solves

Internet freedom is an add-on advantage to the plan — NSA reform is key.

Kehl et al. 14 — Danielle Kehl, Senior Policy Analyst at the Open Technology Institute at the New America Foundation, holds a B.A. in History from Yale University, with Kevin Bankston, Policy Director at the Open Technology Institute at the New America Foundation, former Senior Counsel and Director of the Free Expression Project at the Center for Democracy & Technology, former Senior Staff Attorney at the Electronic Frontier Foundation, former Justice William Brennan First Amendment Fellow at the American Civil Liberties Union, holds a J.D. from the University of Southern California Law School, Robyn Greene, Policy Counsel specializing in surveillance and cybersecurity at the Open Technology Institute at the New America Foundation, holds a J.D. from Hofstra University School of Law, and Robert Morgus, Program Associate with the Cybersecurity Initiative and International Security Program at the New America Foundation, 2014 ("Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity," Report by the Open Technology Institute of the New America Foundation, July, Available Online at https://www.newamerica.org/downloads/Surveilance_Costs_Final.pdf, Accessed 11-03-2015, p. 20)

Mandatory data localization proposals are just one of a number of ways that foreign governments have reacted to NSA surveillance in a manner that threatens U.S. foreign policy interests, particularly with regard to Internet Freedom. There has been a quiet tension between how the U.S. approaches freedom of expression online in its foreign policy and its domestic laws ever since Secretary of State Hillary Clinton effectively launched the Internet Freedom agenda in January 2010.170 But the NSA disclosures shined a bright spotlight on the contradiction: **the U.S. government promotes free expression abroad and aims to prevent repressive governments from monitoring and censoring their citizens while simultaneously supporting domestic laws that authorize surveillance and bulk data collection**. As cybersecurity expert and Internet governance scholar Ron Deibert wrote a few days after the first revelations: "There are unintended consequences of **the NSA scandal** that **will undermine** U.S. foreign policy interests – in particular, **the 'Internet Freedom' agenda** espoused by the U.S. State Department and its allies."171 Deibert accurately predicted that the news would trigger reactions from both policymakers and ordinary citizens abroad, who would begin to question their dependence on American technologies and the hidden motivations behind the United States' promotion of Internet Freedom. **In some countries, the scandal would be used as an excuse to revive dormant debates about dropping American companies from official contracts, score political points at the expense of the U**nited **S**tates, **and even justify local monitoring and surveillance**. Deibert's speculation has so far proven quite prescient. As we will describe in this section, **the ongoing revelations have done significant damage to the credibility of the U.S. Internet Freedom agenda and further jeopardized the U**nited **S**tates' **position in the global Internet governance debates**.