# 1NC

### We Negate the resolution, Resolved: On balance, the benefits of the Internet of Things outweigh the harms of decreased personal privacy.

### Definitions:

### Merriam Webster defines Internet of Things or IOT as: a proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data

### Framework

Burden: The affirmation must be able to weigh all of their benefits against decreased personal privacy

Now onto our two Contentions.

## Contention 1: Security

### Subpoint A: Back Doors

Claim: Attempts to collect personal information through indirect means is considered unfair and immoral.

Singer 15

Should consumers be able to control how companies collect and use their personal data? At a dinner honoring privacy advocates this week in Washington, Timothy D. Cook, the chief executive of Apple, gave a speech in which he endorsed this simple idea. Yet his argument leveled a direct challenge to the premise behind much of the Internet industry — the proposition that people blithely cede their digital bread crumbs to companies in exchange for free or reduced-priced services subsidized by advertising. “You might like these so-called free services,” Mr. Cook said during the event held by EPIC, a nonprofit research center. “But we don’t think they’re worth having your email or your search history or now even your family photos data-mined and sold off for God knows what advertising purpose.” Now a study from the Annenberg School for Communication at the University of Pennsylvania has come to a similar conclusion: Many Americans do not think the trade-off of their data for personalized services, giveaways or discounts is a fair deal either. The findings are likely to fuel the debate among tech executives and federal regulators over whether companies should give consumers more control over the information collected about them. In the survey, which is scheduled to be made public on Friday, 55 percent of respondents disagreed or strongly disagreed that “it’s O.K. if a store where I shop uses information it has about me to create a picture of me that improves the services they provide for me.” About seven in 10 people also disagreed that it was fair for a store to monitor their online activities in exchange for free Wi-Fi while at the store. And 91 percent of respondents disagreed that it was fair for companies to collect information about them without their knowledge in exchange for a discount. “Companies are saying that people give up their data because they understand they are getting something for those data,” said Joseph Turow, a professor at Penn’s Annenberg School for Communication and the lead author of the study. “But what is really going on is a sense of resignation. Americans feel that they have no control over what companies do with their information or how they collect it. ”The report on consumers’ attitudes to commercial surveillance comes at a pivotal moment for online marketers and advertisers. Companies are scrambling to develop new techniques to influence people who increasingly use mobile devices to shop, bank and socialize. Yet, even as millions of people embrace these data-driven services, many are mistrustful of the kinds of inferences that companies might make based on information gathered about them. Some marketing companies, for instance, segment individuals into clusters like “low-income elders” or “small town, shallow pockets” or categorize them by waistband size. The potential risk of inferior treatment is one reason that an increasing number of Internet users are downloading Ghostery, a free plug-in that allows consumers to see and control online tracking by data brokers, advertising networks and other third parties.

Internet of things as defined above allows common household items to send and receive data. Companies will use this connection, in this case unsecure wifi, to collect uneccessary data on you and anyother unlucky customer that falls into their trap. The internet of things will boost this back door idea for companies can collect information from anyones household item because they are all connected through the internet which each company provides. This would lead to companies gathering unwanted informations quote on quote legally from consumers. This is detrimental toward people’s personal privacy because it is unfairly taken away.

This would essentially lead to a decrease in national privacy as well because most companies do not have their headquarters established in the USA, therefore companies can share the information they gathered to their respective countries posing a real threat to national security and safety in the long run.

### Subpoint B: Targeting the Low Income population

Claim: hadasd

FTC 15

FTC Staff Report [Federal Trade Commission] "Internet of Things: Privacy and Security in a Connected World" Federal Trade Commission, 2015.

securing connected IoT devices may be more challenging than securing a home computer, for two main reasons. First, as some panelists noted, companies entering the IoT market may not have experience in dealing with security issues. Second, although some IoT devices are highly sophisticated, many others may be inexpensive and essentially disposable. In those cases, if a vulnerability were discovered after manufacture, it[s] may be difficult or impossible to update the software or apply a patch. And if an update is available, many consumers may never hear about it. Relatedly, many companies – particularly those developing low-end devices – may lack economic incentives to provide ongoing support or software security updates at all, leaving consumers with unsupported or vulnerable devices shortly after purchase.

Hi

Subpoint C: Identity Theft

#### IOT increases the chance of Identity Theft

Wei (Weslay) Xu [Research Associate, Pacific Northwest Library], "Security and the Internet of Things (IoT)," March 20, 2015. Paper for the Tuck School of Business at Dartmouth.

According to Weslay Xu

Privacy concerns: A large number of IoT devices collect some form of sensitive personal information such as name, address, credit card numbers, etc. In addition, these concerns are multiplied as many of these devices are connected via cloud services and mobile apps. These sensitive information can be transmitted on your home network unencrypted and subsequently attacked by hackers via the Internet, leading to serious privacy concerns Considering many of the devices offer access via the cloud, these issues are of more significant concerns. 5. Insecure software and firmware: Over 60% of the IoT devices HP examined had issues including no encryption when downloading software and firmware updates. Therefore malicious software and firmware could be installed into the original system via system updates.

The internet of things are giving hackers an easier job to secure users identities. 60% of IOT devices are vulnerable to hacking. In fact Identity theft will skyrocket due to the fact that passwords and personal information are not encrypted in an IOT world. This will lead to an Identity theft epidemic. Identity

theft is a very hard case to solve.

http://www.cbsnews.com/news/id-thieves-are-hard-to-catch/

In fact according to an article written by Rome Neal from CBS News: The Los Angeles County Task Force is trying to crack down on ID theft. They closed two cases. But, they know the work is far from over. Only 11 investigators are able to investigate 4,900 cases still open.

Identity theft is already a hard case to solve, the IOT is increasing the rate of identity theft and therefore should not be supported.

## Contention 2: Safety

Subpoint A: Automobile Vulnerabilities

#### The Internet of Things does not take hacking into account when defending against all of its threats.

Zetter 1

According to Kim Zetter reporter for WIRED,

Security researchers Charlie Miller and Chris Valasek forever altered the automobile industry’s notion of “vehicle safety” in July when they demonstrated for WIRED that they could remotely hack a 2014 Jeep Cherokee disable its transmission and brakes. Their work led Fiat Chrysler to issue an unprecedented recall for 1.4 million vehicles, mailing out USB drives with a patch for the vulnerable infotainment systems and blocking the attack on the Sprint network that connected its cars and trucks. That Jeep attack turned out to be only the first in a series of car hacks that rattled the auto industry through the summer. At the DefCon hacker conference in August, Marc Rogers, principal security researcher for CloudFlare, and Kevin Mahaffey, co-founder and CTO of mobile security firm Lookout, revealed a suite of vulnerabilities they found in the Tesla Model S that would have allowed someone to connect their laptop to the car’s network cable behind the driver’s-side dashboard, start the $100,000 vehicle with a software command, and drive off with it—or they could plant a remote-access Trojan on the car’s internal network to later remotely cut the engine while someone was driving.Other vulnerabilities they found could theoretically have been exploited remotely without needing physical access to the car first, though they didn’t test these.

This threat is dangerous for the privacy and safety of many individuals. An example would be of a business man travelling to an important meeting with a briefcase. If the businessman is part of a car crash without his wrongdoing, the government or anyone else may have access to classified documents in the businessmans briefcase. This reduction of privacy is unjust to that business man, that business, and any other person in the same situation. Therefore the internet of things should not be supported and this is another reason to vote neg.

## Contention 3: