# 1NC

[**https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf**](https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf)

**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.

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

## Contention 1: Security

Subpoint A: Back Doors

Claim: Governements attempts to gather citizen’s personal information is super charged due to IOT creating the threat of creating ‘back doors’ .

Subpoint B: Targeting the Low Income population

#### IOT targets low income population and rises the chance of a hack

FTC 15

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

These potential risks are exacerbated by the fact that  According to the Federal Trade Commision: 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.

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: