Thomas Bedford

21009807

Technical Media Report Analysis

**Tech giants warn cybersecurity bill could undermine user’s privacy**

Table of Contents

1. **Introduction2**

1.1 What is CISA?2

1.2 History of CISA2

**2. Discussion3**

2.1 Social and Ethical Impacts of CISA.3

2.2 Legal Impacts of CISA.3

**3**. **Conclusion** **4**

**4. References5**

# Technical Media Report Analysis

## Tech giants warn cybersecurity bill could undermine user’s privacy

Abstract - This report documents the analysis of a recent media article ‘Tech giants warn cybersecurity bill could undermine user’s privacy’ regarding the proposal of the CISA bill and the response of tech giant companies such as Facebook, Google and Yahoo. The analysis focuses on the social, legal and ethical impacts of the media article. It also incorporates the source of the articles credibility and reliability.

## Introduction

The article in question ‘Tech Giants warn cybersecurity bill could undermine user’s privacy’ [1] was published online on the 15th October 2015 by the Guardian. This report details the analysis of the social, legal and ethical implications of the articles context. It also reviews the articles source credibility and related media from alternative sources.

#### What is the CISA bill?

The CISA bill (Cybersecurity information sharing act) is a proposed legislation that claims it will be able to improve the enforcement of cyber security within the United States. The proposed legislation would allow technical and manufacturing companies to share client data with the government to help combat cyber threats and attacks. It would also provide immunity from privacy and antitrust laws to companies that do share this data with the government.

#### CISA history

During the 113th congress held in July 2014 the CISA (Cybersecurity Information Sharing Act) bill was inaugurated by the U.S Senate [2]. The bill was passed by the Senate Intelligence Committee but did not obtain a full senate vote. In March 2014 at the 114th Congress the CISA bill was re-proposed and again passed by the Senate Intelligence agency. The bill was then attached as an amendment to the ‘National Defence Authorization Act’ which did not make sufficient enough votes to be accepted. The CISA bill was a development from an earlier proposed legislation of the 112th congress held in 2011 named CISPA (Cybersecurity Information Sharing Protection Act) [3]. CISPA, introduced by Michael Rogers, was passed by the ‘House of Representatives’ in April 2012 but later rejected by President Barrack Obama due to concerns over unprotected civil liberties and confidentiality. The CISPRA bill was an amendment to the ‘National Security Act’ of 1947 which originally did not incorporate cybersecurity. There has been much scrutiny from the tech industry of the ethical, legal and social aspects of the bill since it was first presented.

## Discussion

Extracted from the article in question and surrounding research there is one thing clear here. There are some serious concerns in the proposal of the CISPRA/CISA bill. Large proportions of the public, tech companies and manufacturers have started online partitions [4] against the proposed legislation and reached out to a range of media outlets to voice their distress. Some of the collective reasons for opposing the bill is the ambiguity in which the bill is presented, the centralization of data under a government roof (NSA) and the disregard or overruling of existing privacy laws that would exploit safeguard systems established before and throughout the digital age.

The NSA play a big role in the concerns of the CISA bill and the degradation of public trust. After shaking the public’s trust with the agencies supposed illegal and unethical movements just over the past five years it is no wonder that there are alarm bells ringing with the thought of providing easier access to personal information.

On the 5th of June 2013 an American NSA Security analyst named Edward Snowden leaked his first NSA document that claimed the NSA had been seizing metadata from Verizon customer’s phone calls regardless of suspected criminal activity [5]. The next day, the 4th June 2013, the public woke to read the disconcerting news revealing the NSA PRISM project [6] that potentially infringes upon data privacy and security laws by spying on the public.

Snowden, like some government officials who opposed the bill believe that the main motivations for the CISA bill is surveillance and not data sharing protection. By granting the government exclusive access to sensitive customer data surely the CISA act looks to weaken security rather than reinforce it.

With the ongoing battle of net neutrality [7], intellectual property rights being challenged by the TPP (Trans Pacific Partnership) [8], discrepancies in governing the internet and ever growing cyber threats, the tech industry does not look to lower their guard or trust easy.

#### Social and ethical impacts of the bill?

Just the proposal off the CISA bill has resulted in a serious social response. Tech giants and representing organisations such as the CCIA (Computer and Communications Industry Association) reach out to the public to reveal the scepticism and concerns over the legal and ethical aspects of the bill. Newspaper articles and online media outline the legislations, civil liberties and privacy that would be jeopardised if such an act was legalised in its current form.

Individuals, businesses and organisations are less likely to use an electronic service knowing that there personal data is not safe and could be seized by the government at will. Business relations would wither with the lack of trust and security that can be guaranteed to one another. The mass majority of tech companies pride themselves on customer confidentiality and security and is some cases deliver data security solutions as their main business application. The bill would threaten the very qualities and service that these companies deliver to their clients.

#### Legal impacts of the bill

The CISA bill aims to provide legal support to companies that wish to report cybercrime or threats to the government by granting them immunity to data protection. The motivations are that companies concerned with the legal repercussions of sharing data would be more likely to report such threats aiding the war on cybercrime.

The currently proposed CISA bill will undermine and disregard existing data protection laws. Reporting cybercrime to government agencies is not the issue here, it is the manner in which it is done and the amount of immunity that is granted. The proposal looks to flex and violate the foundation laws of data sharing and needs clear revision before becoming an acceptable law.

Other related media articles have been analysed and discussed here to authenticate the article in question biasness and credibility. Another article found in the ‘Daily Mail’ [9] published on the 27th Oct reporting on the CISA bill progress seems to be a little less opinionated than the Guardian. However it still shows clear concern over the bill and details similar reasons.

## Conclusion

*There is no exception to the rule that every rule has an exception. [James Thurber] [10]*

Is the CISA bill really in the best interest of public security and fighting cybercrime? Can government agencies being trusted not to abuse the law? Is the CISA bill a government ploy to empower themselves?

There is no doubt that the tech industry need to collaborate more on cyber security as a global nation and support the government where possible but the laws upon which this information can be provided must not endanger data security. We do need to establish better channels for combating cybersecurity but not by decreasing data security. It would seem that it is not the thought of providing immunity to companies for sharing data is the problem but the level of immunity in which is granted may encourage or even lure tech companies into breaching privacy laws. There are fears that the bill could encourage and justify mass surveillance [11].

If government agencies such as the NSA where to abuse this law and monitor the public, that’s not to say that they aren’t already, private sensitive data would essentially be centralized under one government roof. This would decrease security on a strategic level. Some members of the senate comity who originally opposed the bill were also worried with the centralization of data.

As we know, tech companies track and analyse our online data through third party businesses compiling digital profiles of its users. This would suggest that tech companies most probably have a better idea of our digital presence than the government.

To be perfectly honest, after the recent events of the FTT, the movements of the NSA, whistle blower Edward Snowden’s moral stand against the U.S and a history of government secrecy and bent laws who in their right mind is going to back the government on this one.

## References

[1] The Guardian. (15/10/2015) Article of analysis. Available: <http://www.theguardian.com/technology/2015/oct/15/cybersecurity-bill-cisa-facebook-google-yahoo-privacy>

[2] Wikipedia. (Last modified 29/10/2015) Cybersecurity Information Sharing Act. Available: <https://en.wikipedia.org/wiki/Cybersecurity_Information_Sharing_Act>

[3] Wikipedia. (Last modified 29/10/2015) Cyber Intelligence Sharing and Protection Act. Available: <https://en.wikipedia.org/wiki/Cyber_Intelligence_Sharing_and_Protection_Act>

[4] Change.org. (18/10/2015) Protect Internet Privacy: Stop CISA. Available: <https://www.change.org/p/protect-internet-privacy-stop-cisa>

[5] The Guardian. (06/06/2013) NSA collecting phone records. Available: <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>

[6] The Guardian. (07/06/2013) NSA PRISM programme. Available: <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

[7] Wikipedia. (Last modified 29/10/2015) Net Neutrality. Available: <https://en.wikipedia.org/wiki/Net_neutrality>

[8] The Guardian. (10/10/2015) Berlin anti-TTIP trade deal protests. Available: <http://www.theguardian.com/world/2015/oct/10/berlin-anti-ttip-trade-deal-rally-hundreds-thousands-protesters>

[9] Daily Mail Online. (27/10/2015) U.S Senate approves major cybersecurity bill. Available: <http://www.dailymail.co.uk/wires/reuters/article-3292538/U-S-Senate-approves-major-cybersecurity-bill.html>

[10] Brainy Quote. (Last modified 28/10/2015) *There is no exception to the rule that every rule has an exception.* Available: <http://www.brainyquote.com/quotes/quotes/j/jamesthurb383659.html>

[11] Free Speech Radio News. (08/01/2015) Available: <https://fsrn.org/2015/10/u-s-senate-passes-cisa-a-cybersecurity-bill-critics-say-will-expand-mass-surveillance/>

Sputnik News (27/10/2015) Edward Snowden Cybersecurity. Available: <http://sputniknews.com/us/20151027/1029200214/edward-snowden-cisa-cybersecurity.html>

House of Representatives. Available: <http://www.house.gov/representatives/>

The Guardian. (21/10/2015) apple google and twitter oppose CISA bill. Available: <http://www.theguardian.com/technology/2015/oct/21/apple-google-and-twitter-among-22-tech-companies-opposing-cisa-bill>

Office of the History. 1947 national security act. Available: <https://history.state.gov/milestones/1945-1952/national-security-act>

Congress. Senate-bill. Available: <https://www.congress.gov/bill/114th-congress/senate-bill/754>

Toms Guide. (22/10/2015) All you need to know. The CISA bill Available: <http://www.tomsguide.com/us/cisa-bill-faq,news-21752.html>