Affirmative Case: Information Security

Smart phones are a wonderful technology. You can carry your phone in your pocket, use it to snap a photo, upload it to Facebook…and within seconds it’s visible all over the world. Technology like that was unimaginable even ten years ago. It has made our lives richer and more connected, but it has also created a world of hidden dangers and risks.

Most people don’t care enough about putting the information from their phones onto the Internet, or what the consequences will be if the wrong person gets ahold of it. That is why I am *Resolved: When in conflict, the right to individual privacy is more important than national security.*

# Definitions

Let’s begin by addressing the definitions of today’s terms:

1. Privacy: “the state of being free from unwanted or undue intrusion or disturbance in one's private life or affairs.”
2. National Security: “a collective term for the defense and foreign relations of a country.”
3. Conflict: “incompatibility or interference, as of one idea, desire, event, or activity with another.”[[1]](#footnote-2)

I will now prove my case with a value and contention. Each will have a few sub-points. I will then conclude with an application.

# Value: Information Security

Information Security is operationally defined as “the protection of sensitive knowledge and data from unauthorized use.” Information Security serves as the perfect value for the round for two reasons:

## Value Link 1: Purpose of Privacy

The only way to know whether or not an individual’s privacy is being undervalued is to know its correct value. Information Security is the answer. As long as privacy is preserving Information Security, it is appropriate.

## Value Link 2: Core Moral Concept

Information Security is not a new idea. It is a basic notion that lies at the heart of morality. It is inseparable from the concept of human dignity: the idea that humans should be treated with a high degree of respect because they have souls.

If Information Security is being protected, the resolution is false. If Information Security is not being protected, privacy is being undervalued and the resolution is true.

I will now offer one structured contention proving that in conflict situations, individual privacy should be valued above national security. You’re going to be subtly surprised when I share with you the application.

# Contention: Today’s Threat Is With Information Security, not National Security

In the information age more than any other, Information Security is both maliciously and voluntarily violated to uphold lesser values. Their major perpetrators can be identified in the following sub-point.

*A) Developers & Hackers.* Those who create information-related products often cut corners when it comes to privacy. Others deliberately intrude. The popular Windows operating system is usually released with hundreds or even thousands of security flaws, prompting updates as they are discovered the hard way.

In 2008, Symantec reported that the number of computer viruses in circulation had passed a million.[[2]](#footnote-3) Even one of these viruses can be devastating. The 2004 MyDoom virus caused over $38 billion in damage.[[3]](#footnote-4) The failures of software developers to release safer products and the success of hackers are proof that privacy is undervalued.

Accept for one. The application I provide to you today is from the CEO of Apple himself…

Application: The iPhone

Nothing represents the information age like the iPhone. This handheld, easy-to-use device makes information more available than ever before. For years the iPhone, as well as many of the smart phone companies on the market, took privacy lightly, especially when gathering intelligence for counter-terrorism investigations. That has turned a significant turn as the CEO of Apple, Tim Cook, has backed up privacy over national security.

Apple has been criticized by national security advocates and even entire countries to grant access to its iPhone devices, especially after terror attacks in Europe and America. As reported in Silicon Valley’s *Business Journal* in December:

“If there’s a way to get in, then somebody will find the way in,” Cook told journalist Charlie Rose. “There have been people that suggest that we should have a backdoor. But the reality is if you put a backdoor in, that backdoor’s for everybody, for good guys and bad guys.”

Cook went onto explain, essentially affirming this resolution wholeheartedly:

“I don’t believe that the trade-off here is privacy versus national security,” Cook said. “I think that’s an overly simplistic view. We’re America. We should have both.”[[4]](#footnote-5)

This application of the iPhone should sway you to the affirmative side of the resolution. There are plenty of personal information on the phone, and this information culminates to an individual’s Information Security. Apple has made it foundational in the development of their iPhones that that information belongs solely to the individual. Even Apple itself doesn’t have access to the information you put on your phone. It’s all encrypted.

The negative will likely claim that this is a national security breach, that even if Apple isn’t able to read individual information that at least the government should. However, any backdoor can be unhinged by hackers, as mentioned in my contention. This conflict situation—ensuring national security by opening the backdoor to hackers—must not be an excuse used to uphold national security. There are other ways the negative and affirmative can ensure national security, but as Tim Cook said, let’s have both privacy and national security. When in conflict, side with the affirmative, Tim Cook, iPhone encryption, and individual security.

1. All definitions taken from Dictionary.com: <http://dictionary.reference.com> [↑](#footnote-ref-2)
2. "Number of Viruses." *Computer Knowledge*. 28 February 2013. <http://www.cknow.com/cms/vtutor/number-of-viruses.html>. [↑](#footnote-ref-3)
3. “8 Computer Viruses That Brought the Internet to Its Knees.” Who Is Hosting This? June 16, 2015. <http://www.whoishostingthis.com/blog/2015/06/01/8-worst-viruses/>. [↑](#footnote-ref-4)
4. Gina Hall. “Apple CEO Tim Cook talked encryption, taxes and overseas labor on '60 Minutes'.” Dec 21, 2015. <http://www.bizjournals.com/sanjose/news/2015/12/21/apple-ceo-tim-cook-talked-encryption-taxes-and.html>. [↑](#footnote-ref-5)