# TechPower to the People:
# State's Monopoly Over Security and Surveillance in Turmoil

By

Marko Bogunovic

A thesis submitted to the Faculty of Political Science in partial fulfilment of the requirements for the degree of

Master's

in

International Security Studies

Charles University
Prague, Czech Republic

**Abstract**

Emerging technological trends have opened the possibilities for information manipulation across multiple platforms resulting in a power shift from the state to its citizens. This study takes on three cases as exemplars which will demonstrate how technology fabricates power in liberal states, causing a power dynamics shift. Each of the case studies will illustrate how technological vigilantism in one form or another allows for the citizen emancipation. The erosion of the relationship between the perpetrator and victim will also be discussed as private and public tracking devices becomes widespread. The initial findings suggest that the introduction of private software tracking has amplified the rate at which the state's monopoly over security and surveillance is eroding. Representing three key sections of a society — public, private, and civil — the cases analyzed show that each section is moving towards micromanagement meaning that citizens are taking the law into their own hands, despite high police competency. Find My iPhone, Twitter, Snapchat, Facebook, as well as other social networks and tracking software help support the rise of technology vigilantes. The state's monopoly over security and surveillance is in turmoil. Thus, this multi-case study will take on a discussion between two potential outcomes—one stating that technological vigilantism reinforces the liberal state, and the other stating that it erodes it and causes an anti-systematic empowerment of the people. Through the analyzation of multiple cases including the case studies, this study does not believe that technological vigilantism reinforces the liberal state. Rather, through the proliferation of technology, emancipation of the people leads to the erosion of what is the current basis of a liberal state.

**Keywords:** technological vigilantism, anti-systematic, emancipation, monopoly

Extent of study: 17 068 words, 108 311 characters

**Declaration of Authorship**

1. The author, Marko Bogunovic, hereby declares that he compiled this thesis independently, using only the listed resources and literature.
2. The author, Marko Bogunovic, hereby declares that all the sources and literature used have been properly cited.
3. The Author, Marko Bogunovic, hereby declares that the thesis has not been used to obtain a different or similar degree.

This declaration is proof that I, Marko Bogunovic, have fulfilled and take responsibility for all requirements listed as of the 10th of May, 2018.

Signed,

Marko Bogunovic.

**Acknowledgements**

First and foremost, I would like to express my sincere respect and gratitude to my supervisor Mgr. et Mgr. Tomáš Bruner. His valuable support, guidance, and hard work has enabled me to express my own ideas and interests into my work. I would also like to thank all of the faculty members at Charles University, who through their hard work, ensured that students like myself had a pleasant experience. Furthermore, I would like to extend a special thank you to Angela Paric for her unfailing support and continuous encouragement. Finally, I am incredibly grateful to my family for their love and support, and all my friends for their encouragement. This venture would not have been possible without all of you. Thank you.

**Table of Contents**

# 1 Chapter: Introduction

A state's legitimacy can be derived from the social contracts proposed by John Locke, Thomas Hobbes, or Jean-Jacques Rousseau, who propose that a state's ability to govern citizens comes from individuals who surrender their rights to the sovereign. One important aspect of the social contract is the idea that citizens surrender their rights and freedoms to the state (e.g. monopoly over security), which helps form the social contract. Social contracts still prevail—for example, citizen 'A' gives up their personal rights over security and violence in order to live in a society, resulting in the state's ability to use legitimate force against citizen 'B', who also gave up their rights, if citizen B harmed citizen A. In this regard, the obligation that citizens have to the state is to abide by the laws even if a wrong was done to them. It is the job of the state to intervene as the legitimate party. Thus, the citizens can use violence or pursue their own security to a very limited extent in a liberal state to repeal their obligations to the government by voting, protesting, or any showcasing means of displeasure—be it legal or illegal.

Of the many rights that individuals have given up in a social contract, the right over the use of violence has become one of the most difficult to define—in particular, delineating the state's right to safeguarding security by means of legal and legitimate violence, which is derived from the right for security of its citizens. The proliferation of private security and surveillance systems have made security more complex than before. For example, in the majority of cases, a state possesses legislation to balance privacy sector laws with the ability of actors to use closed circuit televisions (CCTV). The cause of confusion regarding security arises from sophisticated technologies which have multiple roles in society. What is routinely discussed in literature is the state's ability to use technology like CCTV to infringe the rights of citizens. Britain is an example of a state that has taken surveillance to an extreme, resulting in the constant intrusion on the average citizen's life. The most spied country in the world, according to news outlet, has become Britain (Johnston). It has been reported that the Britain has 1 CCTV camera for every 11 people (Johnston). Britain has becoming well known for the expansion of surveillance. The state's image is tarnished by being labeled as the villain because it is exerting its power over citizen's private lives.[1] While the

[1] The 2010 G20 summit in Toronto, where the Public Works Protection Act was used to detain protestors, is an example where a state had its reputation tarnished to an extent. Regardless of the legitimacy or controversy that occurred, the state did exert its power

proliferation of surveillance monitoring, like in Britain, is a concerning issue to all individuals, some citizen reactions are taking place outside of Britain. Thus, what is not often discussed is the response from citizens to these advancements in technology, and how technology is being used by the citizens in contrast to the rule of law.[2]

Technology itself does not favor sides, rather it is the product of an individual's response to a perceived issue. For the purposes of the subsequent discussions, technology will adapt a broad term encompassing both software and hardware. Regardless of the origin of technology, it will eventually be released to the open market in liberal societies. Anti-CCTV glasses are a perfect example regarding the above discussion (White). The reflective glasses in question were developed by Scott Urban after his assessment of the proliferation of CCTV cameras in Chicago (White). This technology is an example of a private individual using technology against the State, while other technologies, like 'Find My iPhone', are products of a corporation to combat theft. The global Positioning System (GPS), originally developed by the military, allowed for the development of technology in the tracking industry. Find My iPhone, a software developed by Apple, is a key example of tracking software that allows an ordinary individual to conduct vigilantism, which is one of the basis of this research paper. Thus, the focal point of technological vigilantism is the ability of citizens through common technology to conduct their own investigations and produce results. Perhaps one of the most widespread advancements in electronics is the ability to track lost or stolen items and high-quality cameras. Both the camera and GPS capabilities of electronics is vital to the proceeding discussion.

The primary focal point of this study is on empirical data analysis. By introducing the literature review and theories as part of the introduction, this study can focus on presenting the data and analysis concisely. Thus, the subsequent literature review will cover the theories and frameworks used to discuss details in which technology has become a tool for vigilantism contrary to the rule of law. Drawing upon authors such as Pauline Hope Cheong, Daniel Trottier, Yosi Kristian, Nicola Schmidt, Bruce Potter, and Frances Shaw, current theories concerning vigilantes and technology will be considered. More emphasis will be placed on private technology and its

over citizens through legislature. Post G20 summit, the image of the state, in the eyes of the Canadian people, suffered. The citizens lost faith in the police and questions regarding the conduct of the government were brought up in discussion.

[2] The rule of law is the basis of a liberal state, stating that all members in society, including government, is subject to and accountable under the legal process. Enforced by a Constitution, the rule of law ensure a just society.

effect on the states' monopoly over security. The widespread use of private technology (i.e. cellphones) has the potential to affect the states monopoly over security and violence. As will be discussed in the proceeding sections, the dependency on technology is something that needs to be closely monitored in relation to the state. Cyberspace[3] is becoming an extension of reality, and has already become extremely hard for the state to monitor individual access to the internet. Furthermore, Critical Security Theory will be applied to technological vigilantism to better grasp the idea of emancipation through technology. It should be noted that this study is evidence-driven in order to enrich the theory chosen. The three theories of Critical Security Theory – the Welsh, Copenhagen, and Paris School – will be used as a framework for the theory of emancipation. Lastly, the proposed research will look at two potential outcomes of the effect of technological vigilantism with regards to the empowerment of citizens. Three cases taken from North America and Europe will be analyzed and discussed to illustrate how technology is leading to widespread vigilantism—in particular, how citizens are utilizing basic technology to conduct vigilantism. Camera and tracking technology has become common and a standard feature on most electronics, but the potential collateral damage of such technology warrants further investigated.

### 1.1 Literature Review

CISCO, an international technology conglomerate, stated through their Visual Networking Index that 429 million mobile devices and connections were added in 2016. It is expected that by 2021 there will be 1.5 million devices per capita in the world (CISCO). Additionally, according to the Pew Research Centre, 100% of individuals in the United States aged 18-29 own a cellular device (Pew Research Center). The numerical figures presented are examples of how technology is increasingly perceived as a human necessity. As such, the role of electronic devices in technological vigilantism and their effects on the state's monopoly over security merit further examination. A research study conducted by Daniel Trottier on Digital Vigilantism (DV) examined how ordinary citizens use cyberspace to conduct their own policing, resulting in their empowerment (Trottier 55). It was also found that scrutinizing personal information in cyberspace

[3] The definition of cyberspace will be used according to the Tallinn Manual, which states that, "The environment formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify, and exchange data using computer networks" (Schmitt 257).

is in the state's best interest (Trottier 63). Other authors, like Shona Leitch and Mathew Warren, explore the issue of whether social media platforms should be held accountable for the lack of oversight when it comes to using social media for unintended consequences like vigilantism (Warren 34). Leitch also mentions that many issues we face in the real world are reflected into cyberspace (Warren 36). What Leitch means is that issues like social issues are also carried on into cyberspace. Bullying for example has become a popular topic to discuss in relation to the use of the internet. What differs between the intern and real life is that on the internet people are able to hide themselves, to a certain extent. The anonymity of the internet has created a platform where social issues can actually be elevated, because the sense of interaction with another human is lost. The above phenomena can be seen in the second case study that this study will undertake, where Anthony van der Meer begins to feel remorse for the individual he was tracking in cyberspace. Lennon Y.C. Chang and colleagues further explored the consequences of cyberspace and state that citizens have become empowered through co-production of cyber security to help law enforcement (Gong 101).

The current thesis examines how the use of technology to conduct vigilantism affects the state's control over security and violence. Cyberspace and technology is increasingly discussed, by authors like McLuhan (2006), who argue that cyberspace draws the human into the technology (McLuhan 545). But, the potential to erode state control as a result of widespread technology has been neglected. When examining the literature, it seems to focus on one aspect of the digital world, which is the theft of information by private entities, without giving consideration to the use of technology a tool. Daniel Trottier (2017) suggested that, 'surveillance processes can be broken up into discrete steps: the collection of personal data, the interpretation of that data and social consequences stemming from the assessment' (Trottier 65). To fully comprehend the consequences of the collection of personal data, it should be examined, in detail, how users are able to collect data. Many liberal states have laws protecting personal data and the ability to reclaim devices based on the collection of data. Under EU regulation 2016/679 General data protection regulation, collection of sensitive data is legitimate as long as it is proportional to reclaiming the item (European Union). What the legislature means is that individuals should not collect more data than is needed in order to reclaim their property. As a result, since tracking devices connected to the internet are widespread, individuals might prefer to rely on themselves rather than the police to recover their property or ensure that justice is done. These actions may include violence and will be discussed in a case study in the subsequent chapter. For example, Sarah Maguire tracked down a thief and confronted them without the authorities by using Find My iPhone (Lovett). Sarah's case is not unusual or isolated, rather it has become common practice among individuals with Apple devices. Since the introduction of Find My iPhone, it has been reported that iPhone theft dropped by 50 percent in London (Lovejoy). People are using the provided software on their devices to prevent theft, meaning that since police cannot prevent theft individuals have to through technology. Since tracking software, like Find My iPhone, is extremely difficult to remove, the average thief can usually be tracked down once the device connects to the internet. Regardless if the device is rebooted, the device will always send a GPS signal to the software that can be accessed remotely. Thus, individuals like Sarah seem to believe that they have the right to conduct their own investigation and reposes their property. And, this is where technological vigilantism begins, with the people rather than the cyberspace.

Traditionally researchers are more focused on digital space and the theft of information rather than focusing on how individuals use technology in relation to cyberspace. Cyberspace is reliant on content and technological components that allow content to be uploaded onto the internet. This digital environment will become more intrusive and enable sousveillance (i.e. the act of counter-surveillance) (Dennis 354). As a result, the future will be transparent in the sense of privacy, security, and information on the internet (Dennis 355). Thus, the social pressures and other factors that (i.e. government, emancipation, effectiveness of law, etc.) lead individuals to conduct technological vigilantism will be considered. Since technological vigilantism relies on the individual, their motives for conducting vigilantism needs to be considered.

Focusing on one aspect of the relationship between technology, the state, and its actors does not fully answer the question regarding why individuals or groups are using technological vigilantism. As stated by Pauline Cheong and Jie Gong, 'cyber vigilantism is dependent on getting access to personal data through things like hacking' (Gong 471). Digital or cyber vigilantism's dependency on accessing personal data is too narrow in focus due to the potential use of technology. What is required is a broader term, such as technological vigilantism, to encompass scenarios that do not fall under cyber or digital vigilantism. Vigilantism pertaining to cyberspace is discussed through the recent works of Daniel Trottier, titled, 'Digital Vigilantism as Weaponisation of Visibility'. Additionally, 'Cyber vigilantism, transmedia collective intelligence, and civic participation' by Pauline Cheong and Jie Gong, and Jeff Kosseff's article titled, 'The

Hazard of cyber vigilantism', should be given more consideration since they discuss aspects of technological vigilantism like the relation between law enforcement[4] and vigilantism (Kosseff 642). The above authors are primarily focused on individual or group use of cyberspace in order to conduct what is called digital or cyber vigilantism.

While cyberspace is important and should be discussed, it is only one aspect of how technology contributes to vigilantism. Trottier does not discuss the consequences of digital vigilantism for the state. For example, *hacking* has become a catchy word that reflects vigilantism or empowerment of people, but as previously mentioned, it does not fully explain why people are choosing emancipation. What is often overlooked is the ability of citizens to upload their own content to cyberspace, and maintain access for the purpose of conducting vigilantism.

France Shaw stated that 'through the use of mobile media distribution platforms such as YouTube, UStream and other live stream services, protestors are able to form networks of mobilization and representation which he states is counter-surveillance (Shaw 3). Shaw focuses on how during the Occupy Movement, citizens filmed police brutality through the use of their own mobile devices and uploaded the content to the internet (Shaw 2). Lawfully receiving information from a public space is different than breaching someone's privacy and obtaining sensitive information. A limitation of Shaw's research is that there is a lack of constitution in what effects counter-surveillance have on the state in a democratic political order.

One of the most harmful and widespread technologies is GPS, due to the potential of offline and online tracking. GPS and other similar software have become embedded into tablets, computers, smartphones and other technologies. What makes these devices harmful is how much information is sent via signals to receivers between the actor and target. Bruce Potter's article titled, 'Wireless-based location tracking', provides good insight into the capabilities of tracking software and how easily it is implemented into a device. Potter focused primarily on the ability to track devices that have technologies like 802.11 and Bluetooth installed (Potter 4), but this is also a limitation of his research because it does not go beyond this particular software and hardware technology. Rather what should be taken from Potter is that advanced equipment for tracking is available to the public and more consideration should be taken in protecting digital privacy. The

[4] The term law enforcement and "the state" will be used interchangeably, due to the reason that law enforcement or police are agents of the state. Through policing, law enforcement reflects the values of the state onto civil society. Thus, law enforcement or police are interchangeable given the context of the discussions.

work by Yosi Kristian and colleagues (2012) looks at the different ways in how devices send signals regardless if they are connected to the internet (Yosi Kristiana 299). 'Utilizing GPS and SMS for Tracking and Security Lock Application on Android Based Phones', focuses primarily on the information that is stored on a phone (Yosi Kristiana 299). Technological devices store tremendous amounts of information, everything from tracking information to private files. The article suggests on a preventative measure installed on Android based phones that locks out foreign users by integrating the locking software with texting (Yosi Kristiana 305). The problem with android is that it is less secure than Apple (Norton). Another problem is that Android is open source, meaning that Android allows private developers to have the original coding of the operating system. Whereas Apple is restricted, which means that all developers have to ask Apple for permission to create applications for their operating system.

While the above studies provide valuable information and mention empowerment of people, authors like K.K.E Silva discuss' legal investigation. Silva brings forward the potential of vigilantism to disrupt evidence, stating that security vigilantes have become recurring and disruptive in fighting cybercrime (Silva 30). One should not assume that technology is inherently bad or good, rather it provides people with more autonomy. Instead, cyberspace is the domain where knowledge reigns supreme (Schmidt). The discussion on super-empowerment focuses on the individual and their knowledge, it does not take into consideration an individual's ability and willingness to form groups with similar minded individuals. The internet is full of communities of individuals who form their own groups based on similarities. The groups can include people who enjoy the same type of music or sports. Thus, the example of groups is a reflection on how cyberspace is an extension of the real world. Similar to the real world, individuals have been known to form their own groups and act as a team. Anonymous is a great example of this type of group. They have conducted cyber-attacks like Operation Stop Reclamation in 2015, which attacked Chinese cyberspace in relation to disputes in the South China Sea. Organizations like Anonymous exhibit how valuable information is and how people are willing to act as one for a common cause. Forming groups via the internet is also reflected in the real world. The Islamic State in Syria and other terrorist organization have used the internet to recruit people to their groups. Thus, an argument could be made that cyberspace is an extension of the physical world where individuals or groups can also make contributions and assume an identity.

Most research involving cyberspace and vigilantism looks into how information is gained from an individual's cyber bubble. In the cases provided, aside from the discussion on super-empowerment, vigilantism and cyberspace have become a niche to discuss cyber security. Accordingly, cyber vigilantism is something that occurs in cyberspace where people gain personal information from another actor. Personal information is then used against the target in order for someone to exert their own sense of justice. For example , the killer of Cecil the lion had his reputation destroyed through the internet (Rogers). While the above is one aspect of how cyberspace (i.e. internet) is used for vigilantism, information regarding how technology as a whole is allowing for vigilantism remains to be reported. Technological vigilantism will be further discussed in relation to Critical Security Theory and emancipation of individuals.

**1.2 Theoretical Framework**

The dynamics surrounding security studies have changed since the post-Cold War period, shifting from measuring security in terms of the interaction between states and between actors. Within security studies, the Aberystwyth (Critical Security Studies), Copenhagen, Welsh, and Paris Schools, have attempted to explain security and its relation to various actors. As security reaches further into the lives of citizens, the various schools compete for relevance. The interaction of citizens with the cyber world, and other upcoming fields, is an example of where security studies will have to be applied. To better conceptualize the idea of emancipation through technological vigilantism, the theory of Critical Security Studies will be used. Under the umbrella label Critical Security Theory, this study hopes to group the various approaches together. Compatibility between all forms for critical security studies will be dependent on emancipation. While emancipation is a broad term, it has the ability to shift focus from the state to individuals or groups who interact in society. As will be discussed in the proceeding sections, only under emancipation can current and upcoming subjects like cyberspace be explained. Thus, since cyberspace is within the reach of security studies and is dependent on technology, a novel framework for technological vigilantism needs to be created.

Critical security theory was chosen as the most appropriate theory to understand technological vigilantism given its focus on emancipation. Developed by Ken Booth and Richard Wyn Jones, Critical Security theory aims to define human relations within the concept of emancipation (Wæver 13). The problem with viewing security in terms of the state is that the state is the solution as much as the problem (Wæver 13). Since individuals want to be free, and the state wants to be secure, a conflict occurs when striking a balance between freedom and security. Thus, emancipation of people should be given priority in the debate between power and order (Booth 319). Liberal states are based upon the notion of freedom, where citizens have the right to fundamental freedoms such as expression, belief, religion, media, peaceful assembly, and association. Citizens have a vested interested in being free from constraint. Thus, as state by Ken Booth (1991), 'Emancipation is the freeing of people (as individuals and groups) from those physical and human constraints which stop them carry out what they would freely choose to do'. (Booth 319). In contrast to the state, the emancipation of people would mean that the state would be forced to leverage their monopoly over security to the people. For Booth and Jones, the question of begged whether it is the states or the people's security which comes first? (Booth 319).

Rita Floyd, in the article titled, "Towards a consequentialist evaluation of security: bringing together the Copenhagen and Welsh Schools of security studies", draws a criticism about Critical Security Studies that needs to be addressed. Floyd looks at the timeline of security and begs the question where does security stop? (Floyd 333). The answer to the question presented could be found in Booth's article titled, "Security and Emancipation", where he stated that, 'Integral to emancipation is the idea of the reciprocity of rights" (Booth 322). The reciprocity of rights means that the rights of one person cannot interfere with the rights of another. Thus, person "A"s freedom to kill is taken away because it would interfere with person "B"s right to live. Simply, if all individuals are free to do as they please and not interfere with other's rights, then security would have a beginning and end. Security would answer to the people since it is the people who chose what should be secured. Therefore, the use of cyberspace brings about a new challenge in the sense of whether it can work within the confines of security studies.

Cyberspace is seen as an alternate area to reality where individuals are able to not only hide their identity, but take on new personas. Whether security studies can be applied to cyberspace is difficult to conceptualize. Lene Hansen and Helen Nissenbaum take on the question of whether security studies can be applied to cyberspace and state that cyberspace is not exempt from security studies (Nissenbaum 1157). The main goal of Hansen and Nissenbaum's article is to confine cybersecurity within a broader terms of Security Studies (Nissenbaum 1157). For Hansen and Nissenbaum the sector of cyber security is linked to the individual and the network, making it also part of state security (Nissenbaum 1171). While taking on the same view as Hansen and Nissenbaum, the framework of Critical Security Theory rather than the Copenhagen School will be used. The Copenhagen School, unlike Critical Security Theory, focused on a ridged framework. According to Barry Buzan, Ole Waever, and Jaap de Wilde (1998), the Copenhagen School of Security Studies is defined as a speech act composed of, one, the identification of the threat, two, an emergency action, and three, the acceptance of the action that breaks the status quo (Barry Buzan 6). On the other hand, to solve the problems of the Copenhagen School, the Paris School of Security Studies attempted to create their own framework in the field of Security Studies by the works of Didier Bigo. Paris School states that security is the act of practices at the micro level by various agents within the security field (Booth 322). Thus, unlike the rigidity of the Copenhagen School, the Paris School introduces flexibility in how security works. To best describe the Paris School, think of going to the airport where during the post 9/11 times individuals were greeted with extraordinary measures at security check-in's that became common practice and eventually accepted. While both schools of thought present convincing arguments, they seem to suggest that the spectrum of the state's security is more important than the people's.

Unlike the other theories of Security Studies, Critical Security Theory is the only one that fully grasps technological vigilantism. As stated by David Mutimer and colleagues (2013), the opposition of policy is what it means to be 'critical' (David Mutimer 3). Additionally, Booth and Jones indicate that critical scholars have been leaders in the role of arguing for the reduction of security in citizen's lives (Booth 320). The balance of power between the state and its citizens is volatile. The use of technology brings forward the challenge of the state's attempt to maintain its monopoly over security versus citizen's freedoms. Monitoring the internet and the use of personal devices is extremely difficult, as was seen in China, where the government has attempted to block parts of the internet they considered threatening to social and political stability (Nissenbaum 1157). Clearly China is not a liberal state, yet they have extreme troubles blocking vigilantism as discussed by Pauline Cheong and Jie Gong in the previous chapter. Therefore, the framework within Critical Security Studies is able to explain why citizens, even in places like China, go beyond state legislature. Emancipation of people is at the core of Critical Security Studies and a vital aspect of living in a liberal state. The state exists for the people, and not the people for the state.

On the other hand, it is also worth mentioning why realism, liberalism, constructivism, and other are not adequate in explaining the erosion of the liberal state monopoly over security and surveillance. It should also be noted that the theories listed will only be briefly mentioned due to time and space constraint. Realism and neorealism primary focus in politics is the relationship between the states, giving emphasis to the state. Emphasizing the state and not the actors is an important draw back that should be considered. Liberal states are not one entity that harmoniously works together, rather they are a collection of institutes and individuals that cooperate together to form the state. For example, the judiciary is an extremely important institute of a liberal state, yet it is autonomous and can even work against the state's wishes. Rather, the judiciary and the state work for the sake of the people. Constructivism, on the other hand, states that society is made up of pieces or actors that influence each other. The fault with constructivism is that within this theory the actors and the structure are not equal. Emancipation indicates the freeing of the people, and therefore if the people can be freed then the structure and the actor cannot be equal. And finally, liberalism and neoliberalism make a much more intriguing argument. Liberalism stated that the basic actors in the political system are social groups and the actors. But, liberalism fails to account for emancipation due to the power struggle between the state and citizens.

When considering a society, there are power struggles occurring between state legislature and that citizens will. Furthermore, neoliberalism favors more political system in terms of deregulation and the decreasing state interreference. Similarly, neoliberalism runs into trouble when dealing with emancipation. Emancipation, in the real world, is constantly observed where agents attempt to gain power. As stated by Gérard Duménil and Dominque Lévy in, 'The Handbook of Neoliberalism', by Simon Springer and colleagues (2016), that neoliberalism's main goal was to increase the power and wealth of the upper classes (Simon Springer 551). The question of whether the words free-market can actually mean free, if restrictions have already been made by the most powerful, should be addressed. The case study in the proceeding sections will further discuss what a free-market means in a society that has about 1% control over the modes of production. Thus, the theories above fail to explain how citizens are willing to erode the state's monopoly over security and violence. Critical theory is needed in order to explain situations where realism, neoliberalism, and other theories fail to understand the importance of emancipation.

### 1.3 The proposed research

The aim of this study is to research the impacts of technological vigilantism on the state's monopoly over violence and security. Since the advancements of technology, cyberspace usage has become widespread. Through technology and in contrast cyberspace, individuals have been able to use the internet for everything ranging from spying on other people to educational purposes. Clearly, technology has had allowed people to use the internet as they see fit. The internet has become an area where individuals are able to express themselves freely. Additionally, since cyberspace censorship is the lowest among liberal countries (Sanja Kelly), citizens are able to fully utilize social media any tools that are available to them like Find My iPhone. With the introduction of Find My iPhone, Facebook, Twitter, and other platforms, individuals have been able to go beyond the constraints of the state and exert their own social justice. The ability to distribute personal information, track people, and gain personal information via technological devices with internet showcase the potential of a connected society. A connected society is not necessarily an advantage for the state, due to the state's inability to maintain control over technology advancement.

When considering individual use of technology and the state's inability to maintain control, there seems to be a paucity of research. The empowerment of individuals through technology has lead citizens to conduct their own investigations without help from the state. Thus, this study will address two hypotheses.[5] First, one that states that technological vigilantism reinforces the liberal state, causing an emancipatory empowerment of people that benefits the state, and second, that technological vigilantism erodes the liberal state, causing anti-systematic empowerment of people. Both hypotheses will be analyzed with respect to the recent trends that are occurring in society. It should be noted that there is potential for both hypothesis to be true. Technological vigilantism has the potential to reinforce the liberal state depending on the circumstances. The balance between eroding and reinforcing the liberal state will be something that will be addressed in the proceeding sections.

In addition to evaluating the effects of technological vigilantism, the potential for technology to blur the lines between who is the victim or perpetrator will be discussed. Since technology does not differ between users, meaning that anyone can access its potential, the

[5] Something that needs to be clarified is the word 'hypothesis', which is being used as a synonym for possibility rather than a problem that needs to be solved.

potential for victim can switch. For example, a thief can easily become the victim if personal data was released by the vigilante that goes beyond the means of the vigilante reclaiming his property. Technology holds unlimited potential and is something that has unintended consequences that can be positive or negative. At the core of the argument presented above is human emancipation. Thus, it would be expected that a state allows some degree of freedom from constraint, but the full extent of technological vigilantism to erode the rule of law has yet to be fully distinguished within a working framework.

# 2 Chapter: Methodology

A multiple case study will be analyzed based on the factual circumstances taken from North America, Europe, and Australia. In terms of human freedom, North America, Europe, and Australia in 2017 represent the most liberal states in terms of personal, civil, and economic freedom (Porčnik). For the purpose of this study, liberal nations are vital to analyze to determine whether people, if given freedom, will pursue emancipation through technology. Citizens free of coercion by the state or other actors have the potential to pursue their own form of justice. Thus, the first case involving Jeremy Cook was assessed because the individual in question used tracking technology that is already available on all iPhones or other devices to locate his device (Butler). Apple introduced Find My iPhone, a tool that lets individuals track their phones, and later in their operation software iOS 7 in 2013 an activation lock making the phone unusable without the correct credentials once reported lost or stolen with Find My iPhone. Find My iPhone allows individuals to access their phone data remotely even if the phone is completely erased. The above is accomplished because iPhone's require an internet connection to Apple's server in order to be activated. For example, if a thief wants to use the iPhone, he must establish an internet connection through Wi-Fi prompting the entry of iCloud credentials, which would result in the phone sending a GPS signal to the remote website where it can be accurately tracked. Similar to the first, the second case uses private software tracking that allows full, remote access of the device, including the camera. A Dutch citizen, Anthony Van Der Meer decided to make a short film in which his device was stolen after he installed tracking software (Meer). Probably a thief's worst nightmare, Anthony was able to have a very personal look into the thief's life and document his activity.

While the above cases are reliant on technology to track an individual, the last case study will focus on user generated content. Thus, the last case study is more abstract in the sense that it revolves around the use of technology to create content and distribute it though social media, making cyberspace a medium for vigilantes. More specifically, the Occupy Movement in Australia will be used as an example for this case study. Lately, during protests, citizens have been able to generate content and upload it to social media in order to show injustices. The internet has become a powerful tool, not only for liberal nations, but individuals or groups throughout the world. Even in countries like Egypt, during the Arab Spring, internet content uploaded showing social injustices. The reason the term social injustice is used is because there is discrepancy between what the state believes is an injustice and what society believes. Take the examples of police use of arbitrary power during protests like the Occupy Movement or G20 Summit in Toronto. Citizens may believe that their actions are just, while the state is attempting to uphold the law. Just because a law is legal, it does not mean it is just or in accordance to social values. Thus, each of the cases studied represent a different ways of how technological vigilantism can occur. While in each case cyberspace is important and technology is connected to the internet, it only plays a mediating role between two or more actors involved.

## 2.1 Method and Reasons

In terms of trends in society, a multiple case study is useful in gaining insight into a phenomenon, especially one that is not isolated. The multiple case study was based upon the work by Robert E. Stake (Stake) and Stephen Van Evera (Evera). In terms of trends in society, a multiple case study is useful in gaining insight into a phenomenon, especially one that is not isolated. Instrumental case studies, as dictated by Stake to be cases that are examined primarily for insight into particular issues (Stake), are drawn upon. Thus, recent trends in the proliferation of technology seem to indicate that dependency on technology is increasing and that the ability to connect to technology is becoming more sophisticated. Since cases involving the use of technological vigilantism are qualitative in nature, an analysis that takes into consideration some aspects of society, such as norms, trends, and environmental conditions, needs to be conducted. Since Evera's interpretation of conducting case studies includes the possibility of drawing upon characteristics of cases in advance (Stake). Technological vigilantism is reliant on the continued advancement in technology that will allow individuals to potentially emancipate themselves. Thus, the method used aims to include future trends.

The method in which cases were analyzed are discussed in a 4 point system, which were used to validate the hypotheses. Since technological vigilantism revolves around actors engaging with each other the case study determined the common factors that lead an actor to conduct technological vigilantism. Thus, in relation to technological vigilantism, the case studies first analyzed the most important facts. Factual information is undisputed evidence that will be used and built upon in the case studies. The first step is essential in proving validity for the remaining steps in the analyses. Second, key issues were drawn upon from the cases and then presented and discussed. The second step is reliant on how technology plays a role in vigilantism. While the second step might leave room for controversy, it was the goal of the case studies to rely on factual information from the first step to justify the key issues. Third, the course of action taken by the actors in each case was evaluated and discussed regarding why the case is branded as technological vigilantism. And finally, based on the facts and actions by the actors, final remarks will be made with respect to how an actor should have engage given the circumstances of the case.

The cases that were studied were compared because the factors contributing to emancipation. As stated by Stake, multiple case studies are conducted when there is more interested to investigate a phenomenon (Stake). In each of the case studies, the actors involved conducted actions that were contrary to the liberal state, resulting in emancipation. A liberal state allows a certain degree of emancipation to citizens, when it comes to reclaiming their property or in terms of self-defense. The studies further showed how the line is crossed between acceptable form of freedom and emancipation from the state's constraints. The state's threshold between freedom and emancipation can be crossed either by failing to act or by conducting measures contrary to the state. By utilizing technology to gain power, citizens conduct technological vigilantism to free themselves from the constraints of the state. Therefore, each case is related in the sense that the various scenarios represent how citizens emancipate themselves.

# 3 Chapter: Results

## 3.1 Case Study 1: Tracking lost or stolen property

As already discussed in the study, the release of tracking capabilities by companies like Apple has empowered individuals to not only monitor devices through GPS, but also to gain access to their device through a medium like the internet. GPS capabilities have become integrated into devices like cellphones and are used on a daily basis. Jeremy Cook was an individual who took advantage of iPhone's capability, through iCloud, which allows individuals to track their devices. Living in the small town of London, Canada, Mr. Cook lost his cellphone and used the standard tracking software provided by the manufacturer to reclaim his property. As Mr. Cook confronted the thief, the interaction escaladed to where Mr. Cook was left dead (Butler). The case of Jeremy Cook represents one possibility when individuals attempt to confront an accused. While the results of Mr. Cook attempts to confront the accused are devastating, the case is an excellent example of how emancipation occurs on a regular basis. When users use technology to track down a device, and confront another person, they become vigilantes. Therefore, the case regarding Mr. Cook represents one of many real world examples where individuals use technology to confront another individual or group. The case is also significant, because it drew attention from the media and made headlines across the state.

*Facts*

While on his way to the bar, Mr. Cook lost his iPhone in the back of a taxi (Butler). Following Mr. Cook's return home, he presumably used Find My iPhone to track down his phone (Butler). Upon accessing iCloud, the phone was tracked to a parking lot near Mr. Cook's flat where he and his sister went to confront the two men accused who were sitting in a car (Butler). The accused wanted proof that the phone was Mr. Cook's, in which he complied by first calling his own cellphone and second by entering his passcode (Butler). Even with proof, the accused did not relinquish the phone, which resulted in an altercation where Mr. Cook was dragged behind a car (Butler). Soon after gunshots were heard and Mr. Cook was found dead (Butler). While the story does end with Mr. Cooks death, it should also be noted that even after the accused fled the scene, the phone inside the car was still sending its location. Thus, Mr. Cook's sister dialed law enforcement, leading them to the crashed vehicle of the accused (Butler).

*Key issue(s)*

The case of Mr. Cook is quite simple and only has one key issue that needs to be addressed in relation to this case study. Mr. Cook and his sister did not involve law enforcement in their attempts to reclaim the property. Circumventing the law is a major issue that needs to be focused on when discussing individual use of technology in private investigations. In this case, the police were only involved after Mr. Cook was shot. The police are an agent of the state that hold a monopoly over security and violence, but the case presented is contrary to law enforcement. Mr. Cook decided to not only conduct his own investigation through the tracking of his device, but also attempted to reclaim the property himself. Having the potential to involve law enforcement reflects back onto why this particular case was chosen, aside from making it onto the national news. The actions of the parties involved in any confrontation is an insight into the values that are projected in society. While it is unclear whether Mr. Cook would have resorted to violence, he still conducted technological vigilantism.

*Course of action*

The agent, Mr. Cook, decided to log onto the internet and use Find My iPhone in order to track his device. While it has already been discussed that this course of action is vigilantism that circumvents the law, what needs to be discussed is why it is technological vigilantism. Mr. Cook's iPhone had the capabilities to be tracked installed, but he could only access the information through the use of technology and a medium. The internet played as a medium which allowed technologies to interact based on Mr. Cook's request. The phone was stolen or lost and acted as a tracking beacon, which allowed Mr. Cook to conduct his own investigation. Thus, it is the technology that enables the individual to locate the device, making the situation technological vigilantism. Whereas, cyber vigilantism involves the use of personal information through hacking, for example, to exert one's own form of justice.

*Suggestion and discussion*

The case study presented serves to not only show that technology itself emancipates citizens to the extent that they conduct technological vigilantism, but that they chose to do it despite having the opportunity to involve law enforcement. Take for example Mr. Cook, he could have conducted his own investigation *and* involved the police. Having the ability to track a lost or stolen device is relatively new. Since locating a stolen device with only the help of the police is difficult, unless it turns up at a pawnshop, the information provided by Mr. Cook could have been used more productively. Mr. Cook could have contacted the police, who would have helped him confront the thieves as stated by Canadian police in another news article covering Jeremy Cook's case (Bogart). Thus, in a liberal state, individuals would have a choice to use technology like Find My iPhone, and access their data remotely. But, the problem arises when individuals decide to take it upon themselves and reach too far into the state's realm of violence and security. Since a liberal state allows individuals to reclaim their property reasonably, sometimes violence occurs. The case of Jeremy Cook is such an example where he attempted to holster himself to the vehicle, so the accused would not be able to escape (Butler). Thus, reclaiming property, such as with Mr. Cook, could work in cooperation with law enforcement, but the problem is people choose to rely on themselves. Individuals are choosing to circumvent the law despite having opportunities to share data with law enforcement. In extreme cases, like in the case of Jeremy, then individuals seem to rely on the state to protect them and administer justice.

### 3.2 Case Study 2: Unintended consequences of technology

Anthony van der Meer, who was frustrated by his iPhone being stolen and large amounts of thefts of phones in the Netherlands, decided to conduct his own investigation regarding phone thefts. Knowing that tracking software on the market only provides a limited amount of access and potential, he decided to contact the creator of Cerberus. Cerberus is unlike Find My iPhone in the sense that it is a third-party application that is capable of being installed onto the system of the phone, rather than the 'user' memory (Meer). Electronic device's memory is portioned into two part, first the part where the operating system is stored, and the second part where the administrator data is stored. Thus, when a phone is restarted or erased, only the data from the administrator is rebooted. Through Cerberus, Anthony gained the ability to remotely interact with his phone from another device via the internet. Since Cerberus is almost impossible to delete, it meant that the phone would be accessible to Anthony even with a reset of the entire phone's memory. Furthermore, since applications like Cerberus have become widespread (e.g. Mobistealth, mSpy, FlexiSPY, Spyera) the case of Anthony was chosen, due to the creation of his film. The short film created by Anthony has already reached 6.9 million views as of the May, 2018. Since having the potential to reach large amounts people, it is reasonable to assume that others will mimic the film.

Therefore, the second case study further justifies why emancipation of the people is occurring through technology.

*Facts*

With the use of private, third-party software tracking, Anthony set out to make a short film about the theft of his phone and the events that occurred afterwards (Meer). After successfully getting his phone stolen in Amsterdam, Anthony immediately started recording audio, taking pictures, and tracking his device remotely with the help of his computer. Additionally, in order to show how problematic cellphone theft is in the Netherlands, Anthony reported the theft to the police without telling them he has the potential to track the device (Meer). The police proceeded to let Anthony know that his phone will most likely be sold for parts in an Eastern European country (Meer). After a few days lapsed, the thief began to use the stolen device, which can fully be accessed by Anthony without the thief's knowledge (Meer). It also should be noted that the thief's identity was protected throughout the film.[6]

*Key issue(s)*

Anthony went beyond the scope of the law in what is acceptable in reclaiming his private property. But, his choice to retain more data than is required to reclaim his property is not something that will be discussed with this particular case. Rather, the first issue that should be discussed is Anthony's potential to gain access to the private life of the thief. For example, in one scene, Anthony backs up the device's information onto his computer. Clearly this is a larger issue than it seems because the new user of his device could have stored sensitive information on the phone. Having the ability to remotely access a device and not only make back-ups of all the data stored, but take photographs, videos, and audios whenever connected to Wi-Fi is something that is concerning. While the phone is Anthony's, his ability to remotely access his phone while someone else if using the phone is beyond the scope of proportionality. It would be proportional for Jeremy to only be capable of accessing GPS data, but Cerberus has allowed him to go beyond the capabilities of just GPS. The potential for more individuals to fall victim to Cerberus is

[6] Throughout the entire film, Anthony never reveals the identity of the thief nor does he seek any ill intent, as was observed. The above is an important in order to further justify using the Anthony case. Rather than showing the consequences of utilizing technology, Anthony showed the potential harmful effects that can be later discussed.

possible, consider that Sales at Redeem, in the United Kingdom, reported that the after-market for cellphones grew to 95 million (Titcomb). On the other hand, cellphones sold privately are almost impossible to track. Thus, Anthony's movie is a proof of concept of where individuals have the potential to install menacing applications on their software that can target specific individuals.

The second issue of technological vigilantism is the identifying the true victims and the culprits. In the case of Anthony, he did choose to get his phone stolen, but others may install the same software installed for protection. The argument presented is not in the defense of thieves or culprits, rather that data protection laws should work both ways. Just because the phone, for example, is in the possession of one person does not mean that it was stolen. Take for example in the Anthony case, he presumed that his phone was sold and continued to gather data on the individual until he could identify him (Meer). Similarly, when Apple released iCloud lock for their devices, an system that is a phone kill switch, many individuals found themselves buying stolen devices. As stated above after-market cellphone sales have increased, and it does not even take into consideration sites like eBay and Amazon. A simple search for iCloud locked devices will show thousands of search results. If the iCloud locked devices on eBay, for example, are lost or stolen remains to be questioned, but speculations can be made that the person selling the phone is not the original owner. Thus, the line between who is the victim and who is the thief is blurred. Even Anthony, once he got to know his victim, began to feel guilty and even sympathized with the individual (Meer).

*Course of action*

The intention of the short film was to create a documentary tracking the whereabouts of a stolen phone. Here, Anthony's activities are evaluated. In the movie, he stated that cellphone theft was a huge problem in the Netherlands (Meer). Filming and documenting an individual's private life through a cellphone is technological vigilantism. Anthony's actions clearly targeted thieves. Thus, having the ability to remotely access a device and using the ability is violation of the principle of proportionality. Anthony's actions go beyond the threshold of what is reasonable in a liberal society to reclaim property. Thus, technological vigilantism was committed. He could have had numerous ill intents, but the only thing Anthony did was send money to the victim's cellphone to keep his service going (Meer). Additionally, he did confront the thief to get to know him better (Meer). Having accessed the accused's financial information and tracked the thief to only face him, without the thief knowing, was not ill intended. Rather, the actions of Anthony could have resulted in a serious breach of privacy laws had the full extent of the tracking software been utilized. Cerberus has the potential to not only harass the victim by having the phone function without the user, but the data stored could have been released. For example, the thief in the Anthony case was caught on video by Anthony in a very private and intimate situation that could have been released over YouTube, which would result in destroying the reputation of the individual. Technology such as Cerberus is meant to reclaim lost property and not exert vengeance.

*Suggestion and discussion*

The case of Anthony van der Meer is difficult to discuss since his intentions from the beginning were to get his electronic device stolen. Intentions are one of the factors that should be considered in relation to technological vigilantism. If Cerberus was installed for the purpose of reclaiming the stolen device, then Anthony's actions were justified. On the other hand, since Cerberus was installed for the malicious reason of exploiting the thief, then the case becomes more difficult to examine. Rather, the proof of concept and the relation to the law should be examined. As stated previously, according to European legislature it is appropriate to track one's own property within appropriate measures. Thus, an individual would be able to install private software as long as they used it within the confines of the law. Anthony, on the other hand, collected personal and private information with the intention of creating a film and not reclaiming his device. Instead, Anthony could have reported the theft to the police and indicated that he is able to track the thief. However, simply tracking the thief would not have made an amusing and profitable film. Anthony's intention was to utilize technological vigilantism for the amusement of social media platforms like YouTube. In conclusion, the film shows a proof of concept where an individual is able to install private software onto a device and delivering it to a target either by allowing it to be stolen or selling it on the open market.

### 3.3 Case Study 3: Technology as a 'good' and 'evil'

The final case study is more complex than previous cases in the sense that it is in relation to the Occupy Movement and takes place across multiple continents. More specifically the Occupy Movement was increasingly concentrated across the most liberal states; North America, Europe, and Australia/Oceania, coincidently similar to the liberal states that this study analyzes. The Occupy Movement was a series of movements that erupted in 2011 to protest the inequalities between the proletariat and bourgeoisie classes.[7] Across major cities like New York, Toronto, Paris, Rome, and Sydney, thousands of individuals took it upon themselves to occupy public spaces in protests. What ensued was widespread police brutality against protestors that was captured on social media and distributed through multiple platforms. For the purpose of this case study, Occupy Sydney will be used as the primary example that will draw upon news stories and social media outlets to demonstrate how technological vigilantism was utilized. Occupy Sydney is significant in the sense that it demonstrates that within a liberal state, individuals are showcasing their emancipation. Protests and movements represent situations where individual or group actions can be analyzed with relation to the use of technological vigilantism. Furthermore, the Occupy Movement as a whole showboated how surveillance, one of the most utilized forms of pacification by the state, can be counter utilized.

*Facts*

Following "Occupy Wall Street", individuals around the world created their own form of the movement such as "Occupy Sydney", for example. Outside the central Reserve Bank of Australia and at Martin Place in the central business district in Sydney, about two thousand citizens took up peaceful protest (Strauss). What made these movements special is that protestors did not have any demands, rather it was a protest against greed within the liberal system. A few days into Occupy Sydney and police conducted unprovoked violence, as documented by a YouTube blogger under the name "Occupy Sydney Media".[8] In a particular video under the title "From the 99%: Unprovoked Police Violence", there is clear evidence of police brutality where the individual who attempted to speak was put into a choke hold and visibly in pain (occupysydneymedia). In another video protestors indicated how the police seized private property without any notice during a video

---

[7] Making news across the globe, the Occupy Movement began with Occupy Wall Street and soon spread to other major cities. The main goal of the protest was a battle between the 99% being the proletariat, and the 1% being the bourgeoisie class who control the method of production-production of what??. While it is not fully clear on the origin of the protest, the slogan "We are the 99%" originated on Tumblr, but that is speculation.

[8] To analyze all of the videos by the YouTube channel Occupy Sydney Media is beyond the scope of this study, but it is encouraged to visit the site and view some of the videos. The site is as followed: https://www.youtube.com/user/occupysydneymedia/videos.

posted on the 15th of October, 2011 (occupysydneymedia). There are hundreds of private videos showcasing controversial police activity that were taken by individuals with their devices and uploaded to YouTube.

*Key Issue(s)*

The main issues with respect to the Occupy Sydney movement will be discussed from the perspective of the protestors. While police brutality and use of violence is controversial, the real issue that this study takes on is the use of surveillance to counter the state's actions. As previously discussed, there are many hours of footage from citizens who filmed police activity. Filming is a form of surveillance. In addition to the state conducting surveillance against the protestors, the protestors conducted counter-surveillance, or as Kingsley Dennis stated, *sousveillance* (Dennis 354). In the process of sousveillance, the citizens such as in Occupy Sydney use technological devices to film and post police conduct online. In order for sousveillance to be effective during protests, there must be platforms and an audience that will acknowledge the footage. Furthermore, the process of sousveillance, in the Occupy Movement, was conducted to gain evidence of police brutality, making it technological vigilantism. The second issue is that conducting sousveillance against the state (i.e. law enforcement) results in disparity between the state and the citizens. Since both the state and the citizens can conduct surveillance, then the issues of who is just is brought into question. Corresponding to Critical Security Theory and Ken Booth, the security of the citizen's would come first. Sousveillance then is one of the factors that contributes to emancipation through technological vigilantism. Instead of citizens going through the proper channels, they choose to utilize technology to emancipate themselves from the constraints of a liberal state that acts unjust.

*Course of action*

Peaceful protests are one of the key rights that are granted to citizens in a liberal state. However, states are known to engage in controversial actions such as those that occurred during protests like Occupy Movement and G20 Summit in Toronto. Similar to the Occupy Movement, the G20 Summit in Toronto was an example of the police use of arbitrary power in order to detained innocent citizens. The summit in Toronto made headline news across Canada due to the wide variety of videos that surfaced on YouTube showcasing police brutality. In response to police brutality, citizens have decided to take it upon themselves and document injustices. By capturing photographs, video surveillance, and even audio of law enforcement, then citizens are in the action of emancipating themselves through technological vigilantism. As discussed, cellphones have become widespread in the sense that everyone is equipped to conduct sousveillance. As technology becomes more advanced, sousveillance will become much easier and cellphones will get smaller and have capabilities to capture data in various situations. Additionally, the data can be stored and saved even if the phone is destroyed with the aid of cloud storage.[9] After data is stored, it becomes a tool for the user to distribute according to their intentions. Even if video footage of police brutality it taken, it does not mean that it would be released right away. As seen during the Arab Spring[10], video, photo, and audio data is extremely difficult to stop and can be easily distributed to the world via Facebook or YouTube. Social media outlets have become widely used and play an important role in the everyday life of individuals and how they interact with cyberspace. Since sousveillance is extremely dependent on users gathering information with technological devices, it should be branded as technological vigilantism. The goal of sousveillance is to document injustices and distribute the evidence among social media in order to bring the culprits to justice.

*Suggestions and discussion*

Sousveillance is a justifiable course of action within a liberal state. In fact, having the ability to film police conduct increases the transparency between the interaction of the state and the public. Discussions have been increasing across many states regarding whether police should be wearing cameras for the public and their own protection (Wiley). With recent trends in the United States, like the #blacklivesmatter movement, there is additionally pressure for state accountability. Unfortunately, body worn cameras are one sided. Since cameras are limited in their range of view and inability to capture the user, there is potential for partiality towards the individual who is conducting the surveillance. For example, a police officer could easily twist his body to only capture one angle of the confrontation with a citizens. This discussion is not

[9] Cloud storage refers to the ability of electronic devices like cellphones to store data into cyberspace. Cyberspace storage is special because access can be granted across multiple platforms, as utilized by companies like Apple and Android.

[10] The Arab Spring, specifically in Egypt, deserves special mentioning with respect to the social media distribution of data. Middle East countries, like Egypt, are well known to conduct censorship of data and websites. Yet, even in the Middle East, states are not able to control the private release of protest footage through social media platforms.

advocating that there needs to be fully surveillance, rather that both the public and the state are able to conduct surveillance when it comes to a confrontation. Thus, partiality can be remedied by private individuals taking film whenever they deem it necessary in public settings. A public space is meant for the public to interact where a reason reasonable level of freedom is expected. The word reasonable is used because even within emancipation citizens are free to the extent that they do not hinder the freedom of other citizens. For example, an individual walking through a busy area cannot expect to have full privacy rights where tourists are taking thousands of pictures and videos. Similarly, in a liberal state citizens should have the freedom to take photographs, video, and audio of agents of the state in public areas without fear of prosecution. In the above case of Occupy Sydney, the state in question should answer to the people, rather than the people answer to the state. The reporting of police misconduct is difficult, since the onus to prove harm is on the victim rather than the accused. Therefore, sousveillance is a tool that can be used as evidence to ensure justice. sousveillance cannot be justified as being evil or good. Rather, counter-surveillance is part of emancipation from the constraints of a partial liberal system.

# 4 Chapter: Discussion – open state monopoly over security

The three case studies presented in this study showcase various aspects in which the state's monopoly over security and violence is perceived to have begun to erode. For the purpose of the discussion, both the erosion and enforcement of the state's monopoly over violence will be mentioned. Thus, the first case study represents a situation in which an individual had the opportunity to involve law enforcement, but used the tools available to conduct his own investigation regarding a potential crime committed against him. Mr. Cook chose to go beyond what is deemed to be appropriate in a liberal state, and conducted his own form of technological vigilantism. While the first case study had a devastating ending with the vigilante's death, the risk was foreseeable. Whenever there is a confrontation between two or more individuals, there is potential for violence depending on the situation. The failure of the state's involvement in a crime reflects upon the actors involved. Since a liberal state's purpose is to control violence, cases like Mr. Cook give indications that the state's monopoly over violence and security is eroding. A liberal society is made up of different individuals with different values, which is supposed to be mediated by the state having control over conflicts. The second case study, represents a situation where a citizen, tired of the inability of law enforcement to act, decided to taken it upon himself to showcase the potential of technological vigilantism. Anthony van der Meer was able to demonstrate the abilities of private software tracking and how it can be used in relation to technological vigilantism. Finally, the case of the Occupy Movement demonstrates how technology is utilized via social media as a defensive and offensive mechanism against arbitrary state power. In terms of technological vigilantism being a defensive mechanism, individuals would be able to defend themselves against arbitrary powers if they have the potential to guard themselves. As an offensive mechanism, technology helps ensure that agents of the state are more careful with how they conduct their investigations.

Furthermore, the second case study and third case study further showcase the erosion of the state's monopoly over security and violence in the utilizing of surveillance. Surveillance, due to technological evolution, has given everyone the potential to conduct sousveillance. Almost every cellphones, even archaic ones, have cameras installed. As long as a person is in possession of an electronic device with a camera, they can conduct counter-surveillance. Thus, through sousveillance the transparency of law enforcement has increased, due to the potential of police misconduct being documented and distributed online. As stated by Kingsley Dennis, surveillance have been internalized in society (Dennis 348). What Dennis means by internalization is the notion that an action like the news is being generated by the public. More often than not, videos that were taken by the public make it onto the news. Platforms like YouTube and Twitter have dramatically increased the rate at which information is distributed.

Additionally, the widespread distribution of technology has resulted in the unlimited potential in harnessing data for the purposing of altering the status quo. For example, cloud storage technology has made data extremely difficult to erase from a person's possession. Thus, even if a device is arbitrarily taken and destroyed, the data that is stored survives. What the above means is that even if law enforcement destroyed electronic devices during protests, they cannot stop the status quo from changing. If the state is able to control the flow of information, then they are able to change and alter facts. On the other hand, if citizens control data and the flow of information then they are able to change the status quo depending on their norms. Emancipation, therefore, does not only play a key role in dictating norms, but it also corresponds to the evolution of the state. The erosion of the state's monopoly over security and violence is a consequence of the emancipation of the people.

### 4.1 Common factors in case study

There might be some confusion between what might be considered cyber vigilantism and what is technological vigilantism. In fact, the third case study presented was chosen because it had potential for controversy with respect to how sousveillance is considered. Sousveillance is dependent on cyberspace and also on the technology to gather data. Since data is distributed via cyberspace and the victims face scrutiny by being exposed online, cyber vigilantism could be considered to have taken place. But, this case study takes on the view similar to authors like Cheong and Gong that cyber vigilantism is the theft of private data for use against the target. Cyber vigilantism does not account for the use of technology to generate data and distribute it online. Therefore, this study does not advocate for the elimination of cyber vigilantism, rather it hopes to diminish it to cases where the targets own data is used against them to administer justice. To better illustrate cyber vigilantism, consider the case of a hacker obtaining personal information against a target and posting it on the internet. The entire case presented would take place on the internet, rather than in a real life interactions. On the other hand, technological vigilantism is a much broader concept in that it includes various cases that use technological devices to conduct vigilantism and use the internet as a medium. For example, if an individual tracks his own lost or stolen device and confronts the thief, then that is technological vigilantism. Technological vigilantism is based upon the notion that cyberspace only plays a supporting role in the particular case. The case of Sean Power, who recovered his computer, is a real-world illustration of the use of technological vigilantism. Mr. Power utilized an application called Prey to recover his computer and also documented the ordeal on Twitter (Bell). The above case also demonstrated a reoccurring situation that was previously mentioned. Individuals seem to share their ordeals online, which further contributes to emancipation. A proof of concept idea like tracking a stolen device, if successful, is utilized by other citizen's, because it demonstrates results. The faith in law enforcement can be further questioned if more cases like Mr. Power's come to fruition. Since electronic devices have almost become an extension of a person's life, when presented with an immediate remedy to their stolen device, they will most likely take matters into their own hands. Therefore, by the distribution of cases online where individuals recovered their stolen device, through technological vigilantism, people have become emancipated to circumvent the state.

To reiterate, the main difference between technological and cyber vigilantism is that in technological vigilantism cyberspace plays a supporting role rather than a key role. As demonstrated, if all the actions by the vigilante take place on the internet, then the action can be called cyber vigilantism. On the other hand, if technology is the main component of the vigilante, then technological vigilantism would be a more adequate term. To address a potential counter argument that everything is cyber vigilantism, then cyber vigilantism would need a proof of concept to apply to all cases. For example, if an individual takes videos of police brutality and distributes the data through a USB stick, then cyber vigilantism would not be sufficient. When exceptional cases surface that involve the distribution of data through means other than the internet, then cyber vigilantism need to explain the phenomenon. In the case presented the individual would have used technology to conduct technological vigilantism, since his actions were dependent on technology and distributed via a USB stick. The distribution of data through a USB stick is a supporting action that enhanced the use of technology. Similarly, cyberspace is a supporting action for technological vigilantism. Since the entire basis of technology is reliant on an internet connection, technological vigilantism does not narrow itself in simplicity. What is meant by the previous remark is that technological vigilantism needs to have commonality in order for a pattern and proof of concept to exist. As Frances Shaw stated, that mobile media distributions platforms are able to form networks of mobilization (Shaw 3). What is meant by Shaw is that through the internet, everyone is able to interact. Similarly, the common factors between cases of technological vigilantism is that cyberspace is a medium that helps the various agents in various situations interact. While technological vigilantism is not dependent on cyberspace it does utilize it for tracking or the distribution of data that is captured by an individual. But, if data is stolen from another user and distributed, then it can be considered cyber vigilantism. In conclusion, technological vigilantism might share some resemblance to cyber vigilantism, but it encompasses a different factual background. With the proliferation of technology, the ability for society to connect and distribute information is becoming easier. As more and more data is generated, the state's tolerance to emancipation will increase. If the state widens its threshold over what it considers a reasonable freedom and emancipation, then the state would be conceding its monopoly over security and violence.

### 4.2 Will of the people

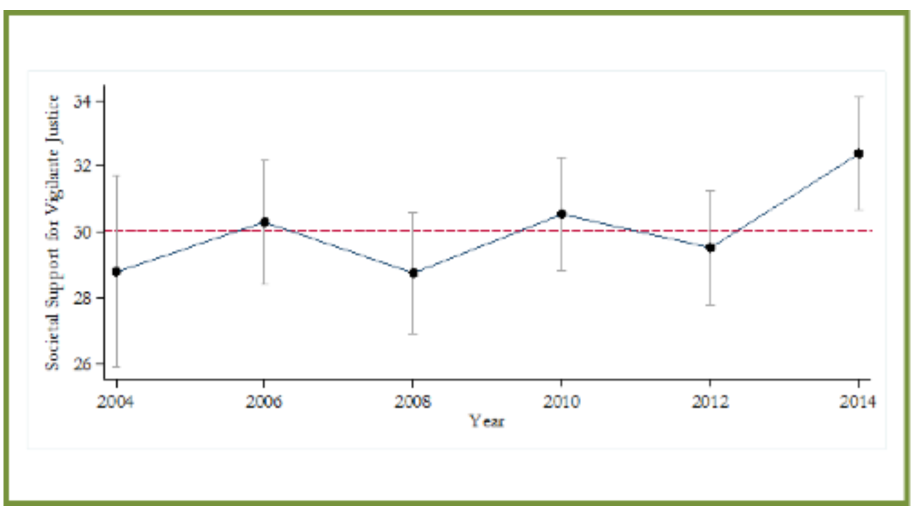
Technological vigilantism, similarly to normal vigilantism, is illegal and in all aspects contrary to the rule of law. When a vigilante conducts technological vigilantism, he circumvents law enforcement in administering policing measures to individuals who broke the law. But, there is a certain threshold of vigilantism that the state would allow. To illustrate the above point adequately, imagine that in the first case study that Mr. Cook tracked down the accused and then proceeded to contact law enforcement. While Mr. Cook would have conducted technological vigilantism, it would be within reasonable limits that a state would allow. But, people are choosing to conduct their own investigations and circumvent the state by administering their own justice. In all cases provided, the actors decided to take it upon themselves to administer their own form of justice rather than go through the legal process. Cases from individuals tracking their own electronic devices and confronting the thief, to taping and releasing footage of police misconduct, are examples of technological vigilantism. The question that is begged is, why do people choose their own form of justice versus what the state provides?

The work conducted by Lena Y. Zhong and colleagues, state that vigilantism is a result of the people's perception that the government is not able to deal with the issues (Lennon Y.C. Chang 108). What Zhong and colleagues mean is that as society grows and populations increase, there will be more theft, and law enforcement is not able to handle all situations with their full attention. Furthermore, stating that when the state fails to take actions against illegal behavior, then the public loses confidence in the state (Lennon Y.C. Chang 108). Keeping with the theme of confidence with the police, Nicole E. Haas (2013) also stated that the support for vigilantism varied depending on police response (Nicole E. Haas 235). Thus, it could be reasonably seen that actors decide to conduct technological vigilantism when there is belief that the state is not able to take action. Looking back at the case studies, more specifically the third case study, it could be reasonably concluded that bringing law enforcement to justice is difficult. To be more concise, take the example of Toronto Police Superintendent Mark Fenton who was scheduled to be charged in connection with misconduct with issuing arrests of innocent bystanders (The Canadian Press). The problem with Supt. Fenton is that, similar to his colleague Inspector Gary Meissner, he can avoid the penalty of dismissal if he retired early (The Canadian Press). Accountability when it comes to law enforcement and agents of the state seems to be an issue that individuals are becoming more aware of. Furthermore, in 2009 the chief constable of Surrey, England acknowledged that police were removing their ID numbers during protests. Even if police would be brought to justice, the penalties are a mere slap on the wrist, as seen in the case of Supr. Fenton who would potentially only face dismissal (The Canadian Press). Abuses of power need to be handled with better care, rather than finding a scapegoat as what Supr. Fenton might become. Rather than punishing an individual, there should have been an investigation launched against the way in which the system operates. In conclusion, after reading the various ways in which police have found ways to use arbitrary power, citizen's perception of law enforcement would dramatically suffer. Citizen's ability to conduct sousveillance is therefore a valuable tool, due to its ability to hold police officers socially and even legally accountable. If trust is lost between the public and the police, then the entire rule of law is in jeopardy.

While the third case study was straight forward as to why technological vigilantism would be a reasonable course of action, the first and second case study are more complex. The complexity of the cases stems from the ability of individuals to have the potential to cooperate with the state, and therefore stay within the limits of vigilantism that is allowed by a liberal state. Discussing the first case study, Mr. Cook could have asked for assistance from law enforcement prior to his engaged. Therefore, technological vigilantism would work together with the state rather than against it, yet the outcome is different. This study does not deny that there are cases were individuals have involved the police in their private investigations, but it looks at the overall effect of the phenomena of technological vigilantism. As was shown throughout various examples, individuals or groups seems to favor not involving the state. In the second case study, Anthony actually went to the police station to report his stolen device and received an answer that his phone would most likely end up in an Eastern European country (Meer). Thus, theft of electronic devices has been common and one of the reasons that electronic companies like Apple have decided to intervene and offer tracking and locking software that is integrated into the device. The studies conducted by Nicole Haas and Lena Zhong corresponds with the notion that when it comes to so-called smaller crimes, such as the theft of electronic devices, that police is less likely to be able to offer full assistance. Rather, the state's ability to respond to theft needs to be addressed. Resources are finite; therefore law enforcement cannot respond to every call. In response to police inability to offer full assistance, people may choose to conduct technological vigilantism and solve their own problem. Referring back to the notion of emancipation and what is reasonability allowed by the state, individuals are choosing to go beyond what the state has allowed. The point being is that there could be multiple, even hundreds, of reason why someone would conduct technological vigilantism that goes beyond the state's threshold. What is important to discuss is that there are more and more cases of technological vigilantism that negatively affects the state's monopoly over security and violence.

**4.3 The Liberal State and consequences**

A liberal state accepts a certain degree of technological vigilantism, as already discussed. But, emancipation of individuals through the use of technological vigilantism has the potential to either reinforce the liberal state causing empowerment of the people or it can erode the liberal state causing anti-systematic empowerment of the people. In order to better grasp the potential presented, vigilantism support with the example of the Americas will be utilized. Daniel Zizumbo-Colunga, with the cooperation of Vanderbilt University, and Center for Economic Research and Teaching, conducted a 10 year study that looked at the support for vigilantism in the Americas (Daniel Zizumbo-Colunga). While the above study does encompass all forms of vigilantism, regardless it is worthy to note to showcase the public support for vigilantism. Figure 1, shows Social Support for Vigilante Justice in the Americas across time (0-100 scale) (Daniel Zizumbo-Colunga).



While it seems that support for vigilantism has fluctuated from 2004 to 2012, 2014 indicates a large increase in public support (Daniel Zizumbo-Colunga). The data presented might be limited in the sense of corresponding to the Americas, but it is in line with the work done by Nicole Haas. Since data regarding vigilantism is scarce, Haas deals with the issue by exploring social justice research that looks at individuals' responses and judgment about the crime committed (J. W. Nicole E. Haas 5). Thus, this research is meant to illustrate two things; first, that vigilantism as a whole is a common trend, and second, to question whether individuals are aware that they are conducting technological vigilantism.

When discussing vigilantism becoming a common trend, one of the best examples to use was cyber vigilantism. More specifically, hacking or similar actions of maintaining the status quo by scrutinizing the target online. For example, many individuals have faced social backlash for pictures or comments they have posted on the internet. Walter Palmer knows well how cyber vigilantism was conduct when he killed Cecil the lion and posted a trophy picture (Rogers). Palmer became an international target of scrutiny, resulting in him taking a leave of absence from society (Rogers). Individuals took to the internet and conducted their own cyber vigilantism, since Palm's actions were in accordance to hunting laws in Africa. While cyber vigilantism has become a trend and is well known, technological vigilantism is not something that has had a similar impact, regardless if it is already occurring. Yet, technological vigilantism as a concept has been observed to be occurring more frequently. As discussed in the previous sections, authorities are not able to respond to every situation and even if they could the law might not match with the social status quo. What is meant by the above is that, taking the case of Palmer for example, states might allow for trophy hunting, but it does not mean that society will have the same view. Discrepancy is known to exist between the law and society. Social values are not always reflected in legislature. In fact, there are many social norms that are not illegal but are frowned upon in society. A more relatable example, than Cecil, would be an individual not giving their seat to the elderly on the bus. If someone refuses to abide by social norms, then they could be put on social platforms like YouTube and face public prosecution. Additionally, some low level crimes like parking in a handicap space may carry a larger social burden than the ticket issued by law enforcement. What should be noted is that the law responds to social norms, and it might lag behind. With technology becoming widespread, legislature will have a difficult time responding in a timely manner to changing norms.

Technology has entered all aspects of society. As Kingsley Dennis correctly stated that, "Citizen journalism is now a more exposed part of mainstream news coverage, and marks a growing convergence between the professional and amateur realms of reportage…" (Dennis 349). Whenever an individual watches the news or other media, it is extremely difficult not to be exposed to some form of amateur generated content. Thus, in corresponding to Dennis' insight, technological vigilantism has already made the news, and footage has been used in news reporting's across liberal states. Similar to the third case study, news outlets have used amateur footage that has been submitted on the internet, usually taken from YouTube or other social media outlets. For example, during the G20 Summit in Toronto and Occupy Movement, police brutality caught on amateur video seemed to always make the news. Individuals who conduct sousveillance, and in contrast technological vigilantism, might be oblivious to what they are doing. Rather when a group during protests films injustice and posts it online, they may believe they are abiding within reasonable limits to protect the people. But, to better understand the above claim, an individual's intention will be analyzed. Technological vigilantism is brought about through a perceived injustice, similar to normal vigilantism. The injustice does not necessarily have to affect the individual, but needs to be recognized. Drawing from the example of the Occupy Movement and G20 summit, police misconduct was a vital concern of citizens who engaged in the protests. Thus, in order to protect themselves they engaged in group sousveillance and used their mobile devices to conduct technological vigilantism. Vigilantes in question have a goal of maintaining the social status quo and bringing forward injustices via cyberspace. Through cyberspace, data can be transmitted to various outlets including the media. In addition to the internet, the media maintains a crucial role in distributing information to the general public. But, since the internet is rich in information, to stay up to date, media has drawn more data from amateur footage, especially when it contains controversial information. While citizens might not know they are conducting technological vigilantism when they conduct sousveillance, it is something that is occurring nonetheless.

### 4.4 Future Research

Already existing data on technological vigilantism is limited, due to the qualitative nature of cases. Furthermore, gathering more data and cases on technological vigilantism is challenging. Consider the cases presented on technological vigilantism, they only made the news because they are extreme cases or the vigilante documented the case online. If the interaction between the accused thief and the owner of a device is pleasant, then there would be no news. Rather, what makes the news is cases when a situation escalades beyond the control of the vigilante. Thus, in order to collect data with similar circumstances, authors have to rely on social experiments and quantitative research that measures people's opinion on vigilantism. Additionally, the distinction between the various forms of vigilantism would need to be indicated into the study, so that information is gathered. For example, polls could be conducted in discussing whether individuals in a society have ever used Find My iPhone or other applications to track down their lost or stolen device?

Thus, the purpose of this final section is to reflect upon the future research that can be taken in order to better understand technological vigilantism, and its relation to the state's monopoly over security and violence. One aspect that can be better researched is the overall consequence of the emancipation of the people. To what extent do individuals want the state to interfere in their matters is something that changes throughout time. As norms in society change, so do people's perception of how the state should act. Thus, what is meant by the above claim is that this study has conducted a discussion and generated a new term for the use of technological vigilantism. Therefore, to further the research, a study can be taken on to discuss if liberal states are evolving in the sense of generating emancipation where security of citizens comes above the state's security. Reiterating Ken Booth (1991), 'Emancipation is the freeing of people (as individuals and groups) from those physical and human constraints which stop them carry out what they would freely choose to do' (Booth 319). Emancipation is not to be confused with anarchy. Through emancipation individuals and groups choose to live in a society free from violence and in fact as pointed out by Booth, it is the only way one person can enjoy their freedom. In anarchy, people are not free, rather they are constrained by the free will of others. For example, in anarchy individuals would be free to conduct violence, but freedom to conduct violence on another person limits the other persons freedom to be free from violence. To circumvent issues of which right takes priority, positive and negative rights should be attributed to the debate. Theoretically, a negative right is an individual's right not to be subject to another person's will. Violence is an example of a negative right that individuals should be free from. In contrast, a positive right is something that is provided or guaranteed by an agent like the state to provide. An example of a positive right would be the right to a trial. Thus, emancipation through technological vigilantism occurs when a pre-established norm like that citizens should not conduct vigilantism occurs. Without having to expedite a great deal of time, it should be noted that technological vigilantism is a reflection of a society. Therefore, it could be further studied if a countries crime rate, more specifically petty theft like electronic theft, affects technological vigilantism. Furthermore, social opinions can be measured with respect to the use of technological vigilantism for theft.

Technology vigilantism has also had another consequence which was briefly mentioned throughout the study—sousveillance—which has the potential to bring additional transparency to the interactions between the state and citizens. By showing law enforcement that they are under surveillance, there is potential to alleviate many issues that have plagued states like America. Recently, American law enforcement has been under tremendous scrutiny for their controversial actions. In response, as discussed, American law enforcement are making more of a commitment to body worn cameras. Therefore, a second study could be conducted on sousveillance and other forms of technological vigilantism to explore why some use of technology enables systematic emancipation and others anti-systematic. This study acknowledges that not all cases are as simple as what was presented, but due to space future endeavors would have to address the above issue. Furthermore, the study could take a comparison between historical cases and present cases, and compare them based on social ques.

# 5 Chapter: Conclusion

With the advancement of technology, people have become more dependent on accessing data through their electronics. Technology has affected all aspects of society, from the state to private interaction. An individual presence online has manifested to the extent that even dating has becoming an online activity. Therefore, not only do individual rights erode, but the state's monopoly over security and violence begins to deteriorate. The proliferation of technology has brought with it various tools that can be utilized to fulfil a person's will and protect themselves. Therefore, the factors in emancipation with respect to the state's monopoly over violence needs to be closely monitored. There are multiple ways to utilize technology, and technological vigilantism was brought forward in this study and discussed. Similar to vigilantism, technological vigilantism is the process in which citizens use technology for purposes of fulfilling their needs for security. For example, the emergence of sousveillance can be argued to be as a result of the state's involvement in the (in)security of its citizens. Since technological vigilantism is something that has been coined in this study, and due to the complexity of recovering information, there is a lack of data corresponding to the phenomenon. Nonetheless, having been motivated by cases of citizen's utilizing technology as a tool for vigilantism, this study took it upon itself to further explore the issue. In order to fully grasp why technological vigilantism has begun to surface pre-existing notions of cyber security, vigilantism, surveillance, and data protection laws have been considered.

The traditional research on digital space and how cyber vigilantism works had to be considered. Authors like Kingsley Dennis and Daniel Trottier explored issues of surveillance and how can be utilize by the state and by the people (Trottier) (Dennis). The use of surveillance has become one of the staple indicators of a security state, such as Britain. Thus, in order to counter surveillance, various authors discussed the notion of sousveillance. Sousveillance is one of the most important tools that citizens are able to utilize, which is a process in which technology is used to film injustices and publicize the data. By making data public and spreading it through social media, social pressure is able to counter the state's use of arbitrary power. Additionally, victims of police violence circumvent the rule of law by publicizing the data, resulting in the government being scrutinized. If public opinion drops regarding police, then governments face further erosion of their monopoly over violence. Thus, the line between who is viewing and who is being viewed becomes harder to distinguish. Furthermore, when it comes to the distribution of data, authors like Shona Leitch and Matthew Warren explore the issues of social media distributing data regardless of content (Warren 34).The above authors dig deeper into cyberspace and seem to make the claim that, since social media interacts with people, there should be more oversight by them (Warren 34). The interaction between technology and cyber vigilantism, in cyberspace, is one of the most difficult obstacles that this case study needed to overcome. Cyber vigilantism has been gaining ground on the intellectual front, and it is being considered more in society. To reiterate, Pauline Cheong and Jie Gong stated that, 'cyber vigilantism is dependent on getting access to personal data through things like hacking' (Gong 1). Thus, cyber vigilantism is different from technological vigilantism in the sense that there is some overlap, but technological vigilantism is more inclusive.

Technological vigilantism was created to be more inclusive, as a notion to demonstrate a particular trend in society. Unlike technological vigilantism, one of the weakness of cyber vigilantism is the dependency on recovering personal data. The gathering, uploading, and distributing of data needs special consideration when it comes to society interacting with cyberspace. Technologies interaction with cyberspace should be able to be a stand-alone notion without reference to cyber vigilantism. As stated, people's obsession with staying connected via the internet warrant the attention through the term technological vigilantism. Cyber vigilantism and cyberspace is routinely discussed, but what is neglected is the potential for vigilantism through cyberspace to erode the states monopoly over violence and security.

There are a multitude of theories that attempt to explain and comprehend the state and its interaction with citizens. To better explain why citizens would conduct technological vigilantism contrary to the liberal state is through the use of Critical Security Theory. The reason that Critical Theory was chosen was because the work of Ken Booth and Richard Wyn Jones who focus on emancipation. Other theories were not chosen, because critical theory already acknowledges that the state is a solution and a problem (Wæver 13). Liberalism and realism are too focused on the state, rather than the citizens. In connection with citizens choosing to conduct technological vigilantism, only Critical Security Theory can full grasp the issue. The state is for the citizens, rather than the citizens for the state, meaning that the questions posed in Critical Theory whether the state or the citizens comes first is answered by emancipation itself. Therefore, this study brought forward the question of what is the impact of technological vigilantism on the state's monopoly on violence? To answer the above research question, two or more possibilities were considered. Possibility A was that technological vigilantism reinforces the liberal state causing an emancipatory empowerment of the people. Possibility B was that technological vigilantism erodes the liberal state, causing anti-systematic empower of the people. Furthermore, there could be a possibility of both A and B. To better clarify, three case studies were examined.

The study chose 3 cases, among 3 different continents, that are considered the most liberal. Given the circumstances surrounding vigilantism and technological vigilantism, a multiple case study was the only way in which to explain technological vigilantism. The first case of Jeremy Cook, in London, Canada, represented the simplest form of technological vigilantism. Mr. Cook tracked his stolen cellular device without the aid of law enforcement. In the first case, there was potential for Mr. Cook to involve the police, but chose to confront the suspected thief by himself.

The second case was similar to the first, but the victim Anthony van der Meer, in the Netherlands, intentionally got his device stolen. Unlike Mr. Cook, Anthony did contact the police, but did not disclose the fact that he had installed private software tracking. In both cases, the two victims used technology to conduct technological vigilantism. Finally, the last case dealt with the Occupy Movement in Sydney, Australia, where citizens utilized technology to film law enforcement injustice and distribute it via cyberspace.

The question that is begged is whether technological vigilantism erodes or reinforces the liberal state through emancipation of the citizens? For the sake of discussion and to prevent more confusion, technological vigilantism can contribute to possibility A and B. But, the study will take on the notion that technological vigilantism erodes the liberal state causing anti-systematic empowerment of the people. While it might be controversial, taking into consideration Critical Security Theory and the cases provided, the liberal state is eroded by emancipation through technological vigilantism. The process of emancipation is being set free from constraints. Therefore, citizens are breaking the constraints created by a social contract to generate their own security.

In each of the case studies presented, the liberal state is a constraining agents. While the first case is simple and is more or less regarded as an individual attempting to regain his private property, it can be easily analyzed. Thus, an individual should not fear other actors, but rather should be free to regain his property without fears of violence. The results of the case were devastating, but criminality is an issue that the state needs to address. Therefore, Mr. Cook was dependent on the state administering its legislation with regards to gun control, which it failed. The second case is more complex in the sense that Anthony did actually contact the police, but as discussed, the answer he received was not adequate. Anthony, as a result, administered his own form of justice and proved that the someone can be brought to justice without the aid of the state. The information Anthony could have used would have resulted in tremendous social pressure for the target. And finally, the last case is the most complex because it involves the use of surveillance against the state. Law enforcement across the most liberal states studied, in this study, have conducted controversial behavior against its citizens. Thousands of hours of footage from G20 summits and protests exist, where the state is conducting arbitrary arrests and brutality. If not for technology and the use of social media then injustices by the state would be difficult to prove. As a result, sousveillance emerged as a form of technological vigilantism that relies on users to generate data and spread it via cyberspace. In conducting sousveillance citizens are able to hold the state accountable and draw social pressure. Thus, for the reasons listed above and the various cases studied, technological vigilantism exists not only for the purpose of guarding against the state, but also to withdrawing a small portion of the social contract back. Technology has allowed citizens to become emancipated where they could have more say in terms of how security interacts in society.

Whether the analysis above stands the test of times remains to be seen. As society becomes more dependent on an internet connection, individuals will have a larger footprint in cyberspace. Rather than being a mystical world, cyberspace is an extension of the human world, where people project themselves onto as discussed by Marshall McLuhan (McLuhan). Thus, as an individual becomes more intertwined with cyberspace, there will be more potential to control their own security. What is meant by the above comment is that the transparency between people and their security with relation to one another will be more fragile. Transparency increases the ability for personal information distribution. If interaction in cyberspace becomes the new status quo, then the ability for the liberal state to govern such interactions would be extremely limited. Cyber vigilantism has already proven that monitoring individuals in cyberspace is extremely difficult and costly. Technological vigilantism, on the other hand, brings about new issues and challenges that the state will have to address. This case study raises awareness regarding how technological vigilantism affects the liberal state.

## References


Barry Buzan, Ole Waever, and Jaap de Wilde. *Security: A New Framework for Analysis*. London: Boulder , 1998.

Bell, Melissa. "Sean Power and the case of the missing laptop." The Washington Post, 13 May 2011. News Release.

Bogart, Nicole. "Police warn against tracking stolen smartphones, here's what you should do instead." Global News, 17 June 2015. Press Release.

Booth, Ken. "Security and emancipation ." *Review of International Studies* (1991): 313-326.

Butler, Colin. "Teen seeking lost cell phone bled to death in parking lot, murder trial hears." CBC News , 06 September 2017. Press Release .

CISCO. *cisco.com*. 07 February 2017. 01 May 2018.

Daniel Zizumbo-Colunga, Vanderbilt University, and Center for Economic Research and Teaching. "AmericasBarometer Insights: 2015." 2015.

David Mutimer, Kyle Grayson and J. Marshall Beier. "Critical Studies on Security: an introduction." *Critical Studies on Security* (2013).

Dennis, Kingsley. "Keeping a close watch – the rise of self-surveillance and the threat of digital exposure ." *The Sociological Review* (2008): 347-357.

European Union. "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016." *Official Journal of the European Union* (2016).

Evera, Stephen Van. *Guide to Methods for Students of Political Science*. Ithaca: Cornell University Press, 1997.

Floyd, Rita. "Towards a consequentialist evaluation of security: bringing together the Copenhagen and the Welsh Schools of security studies." *Review of International Studies* (2007): 327-350.

Gong, Pauline Hope Cheong and Jie. "Cyber vigilantism, transmedia collective intelligence, and civic participation." *Chinese Journal of Communication* (2010 ): 471-487.

Johnston, Philip. "The Telegraph." *Britain: the most spied on nation in the world*. The Telegraph, 02 November 2006. Press Release. 01 May 2018.

Kosseff, Jeff. " The hazards of cyber-vigilantism." *computer law & security review* (2017): 642-649.

Lennon Y.C. Chang, Lena Y. Zhong, and Peter N. Grabosky. "Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime." *Regullattiion&Goovveernrnaanncece(* (2018): 101-114.

Lovejoy, Ben. *9TO5Mac.com*. 11 February 2015. 01 May 2018.

Lovett, Ian. "When Hitting 'Find My iPhone' Takes You to a Thief's Doorstep." the New York Times, 03 May 2014. News Release .

McLuhan, Marhsall. *Media and Cultural Studies* . Blackwell Publishing Ltd. , 2006.

Nicole E. Haas, Jan W. de Gerben J. N. Bruinsma. "Public support for vigilantism: an experimental study." *Journal of Experimental Criminology* (2012).

Nicole E. Haas, Jan W. de Keijser & Gerben J.N. Bruinsma. "Public support for vigilantism, confidence in police and police responsiveness." *Policing and Society* (2014): 224-241.

Nissenbaum, Lene Hansen and Helen. "Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarte* (2009): 1155-1175.

Norton. "www.us.norton.com." *Android vs iOS: Which is more secure?* Norton by Symantec, n.d. News .

occupysydneymedia. "From the 99%: Unprovoked Police Violence." YouTube, 22 October 2011. Video.

—. "Occupy Sydney Day 01: Police Seize Property." YouTube, 15 October 2011. Video.

Pew Research Center. *Mobile Fact Sheet*. 05 February 2018. 01 May 2018.

Porčnik, Ian Vásquez and Tanja. "The Human Freedom Index - 2017." 2017.

Potter, Bruce. "Wireless Security." *Wireless-based location tracking*. n.d. Article.

Rogers, Katie. "American Hunter Killed Cecil, Beloved Lion Who Was Lured Out of His Sanctuary ." New York Times, 28 July 2015. News Release .

Sanja Kelly, Mai Truong, Adrian Shahbaz, Madeline Earp, and Jessica White. "Freedom on the Net 2017." 2017.

Schmidt, Nikola. "Super-empowering of Non-State Actors in Cyberspace." n.d.

Schmitt, Michael N. (editor). *Tallinn Manual on the International Law applicarable to Cyber Warfare*. New York : Cambridge University Press , 2013.

Shaw, Frances. "“Walls of Seeing”: Protest Surveillance, Embodied Boundaries, and Counter-Surveillance at Occupy Sydney." *Transformations Journal of Media & Culture* (2013): 1-9.

*Short Film: Find my Phone* . Dir. Anthony van der Meer. Perf. Anthony van der Meer. 2016. YouTube.

Silva, K. K. E. "Vigilantism and cooperative criminal justice: is there a place for cybersecurity vigilantes in cybercrime fighting?" *International Review of Law, Computers & Technology* (2018): 21-36.

Simon Springer, Kean Birch, and Julie MacLeavy. *The Handbook of Neoliberalism*. Abingdon : Routledge, 2016.

Stake, Robert E. *The Art of Case Study Research*. Sage Publications, 1995.

Strauss, Jesse. "'Occupy the Hood': Including all of the 99%." AlJazeera, 10 October 2011. Press Release.

The Canadian Press. "Police Supt. Mark Fenton, guilty of G20 misconduct, won't be fired or demoted." CBC News, 15 June 2016. Press Release.

Titcomb, James. "Rising phone prices leads to boom in second-hand mobile market." The Telegraph, 08 October 2017. Press Release.

Trottier, Daniel. "Digital Vigilantism as Weaponisation of Visibility." *Philosophy Technology* (2017): 55-72.

Warren, Shona Leitch and Matthew. "Cyber-bulling and vigilantism: Should social media services be held to account?" *Sixth AUSTRALIAN INSTITUTE OF COMPUTER ETHICS CONFERENCE*. Burwood: School of Information Systems, Deakin University, 2012. 32-37.

Wæver, Ole. "Aberystwyth, Paris, Copenhagen New ’Schools’ in Security Theory and their Origins between Core and Periphery." 17 March 2004. Article.

White, Charles. "The Sun." *Anti-CCTV ‘Reflectacle’ glasses will let criminals evade the law and activists dodge ‘the surveillance state’*. The Sun, 29 December 2016. Press Release.

Wiley, Maya. "Body Cameras Help Everyone — Including the Police." Time, 09 May 2017. News Release.

Yosi Kristiana, Hendrawan Armantob, and Michael Frans. " Utilizing GPS and SMS for Tracking and Security Lock Application on Android Based Phone." *Social and Behavioral Sciences* (2012): 299-305.