Prahlad Jasti

English 103: Section HQ

Professor Michael Monescalchi

11 December 2019

Societal Establishment of Conformism Through Data Publication

Introduction

As more people rely on their devices and the Internet to carry out their daily routines, there exists an ever-growing need for their activity online to be protected from malicious attacks. These attacks range from individualized data breaches to power grid shutdowns, and their effects on the public's welfare are so detrimental that they warrant the protection of government agencies such as the National Security Agency (NSA). However, these agencies, along with technological giants such as Facebook, whose influence over the Internet is akin to these agencies, have employed tactics which have put the privacy of the public's data in jeopardy in order to achieve their goals. One justification for these tactics is that the publicity of our data promotes a sense of trust and security among Internet users. Although many advocates for communication privacy have spoken out against these actions, one of the reasons these agencies and companies persist is due to their subtle, but powerful advocacy of a notion of conformity to justify their actions. A potential necessity for this reinforcement of conformity can be explained by technological determinism, which explains how society's advancement of technology determines our cultural and social virtues. As the prevalence of technology in society has grown, social values, especially those of the U.S., have shifted to a conformist standpoint in order to accommodate the trust necessary for cybersecurity agencies to accomplish their goals.

The shift in the societal landscape of the U.S. is a case study that Bruce Bimber explores in his book *Karl Marx and the Three Faces of Technological Determinism.* This book explains the various perspectives in which technological determinism is construed, each of which can be used to explain the relationship between technological determinism and conformism. The values that constitute a conformist standpoint suggest that those willing to follow this standpoint must sacrifice certain ideals that promote individualism. Data privacy is one of the most notable of these ideals, as it gives an individual a sense of comfort in knowing that one may express one's true identity without fear of any unwanted publicity. Facebook, for example, is a company that demonstrates the belief of establishing conformity in order to promote security through many avenues in Franklin Foer's essay, "Mark Zuckerberg's War on Free Will". In this essay, Foer demonstrates the ramifications of conformism created by technological determinism through Zuckerberg's discussion of a technocracy potentially dictating societal values. Zuckerberg shows through his discussions how he can take advantage of a culture such as technocracy in order to promote conformism. The culture surrounding societal beliefs is able to spread ideals, such as those of technological determinism, very easily, mainly due to its prevalence across a country such as the United States, and possibly even the world. In fact, technocracy is a form of culture that has a potent prevalence because it governs the domain of technology in an age where it is quickly advancing, and it becomes necessary that cybersecurity efforts are strictly enforced in order for a technocracy to keep up with rapid progression. It is imperative that experts in the cybersecurity field consider the consequences of their decisions to publicize user data with respect to not only its economic or political effects, but also how the societal landscape is shifted. In this paper, I argue that cybersecurity efforts take advantage of the ideals of technological determinism to justify their agency over the privacy of user data. The gradual loss of agency and

individualism that the public used to have over their data suggests that technological determinism plays an integral role in the efforts of cybersecurity agencies. Additionally, the ideals of technological determinism that these agencies promote are prevalently spread across the world through online culture surrounding the technological world. By taking advantage of the vast expanse that online culture such as social media governs, these agencies are responsible for the shift in societal values away from individualism to conformism.

Technological Determinism

When analyzing the effects of publicizing data, it is integral to understand how technological determinism underscores a relationship between technological and societal advancement. Although various interpretations of this theory exist, Jürgen Habermas elucidates on one such interpretation in Bruce Bimber's book which analyzes the control of societal standards through technology, where he writes "...the issue underlying technological determinism is how societies can employ ethical conceptions to exert conscious, willful control over the norms of practice involved in technological progression" (336). By reading Habermas' understanding of "technological progression" in the context of data privacy, agencies in the field of cybersecurity form the basis of their tactics on safety in conformism as an "ethical conception" of society in order to advance their efforts in the progression of cybersecurity. In fact, conformism is a vehicle in which "the norms of practice" facilitate "technological progression", as conformism's establishment of safety through data publicity not only discourages Internet users to express their individuality in the safety of anonymity, but also prevents detrimental societal standards from forming judgements that would discourage technological growth. Although proponents of technological determinism find security in publicity, the ideals promoted by these invasive cybersecurity efforts may also hinder

technological growth. Habermas demonstrates the negative effects of an ideology that breaches privacy such as data publicity in Warner's text *Public and Private,* where Warner discusses the attributes of society that are public and private, along with the ramifications of the qualities of privacy and publicity. In this text, Warner writes, "[Habermas] wishes to show that bourgeois society has always been structured by a set of ideals that were … compromised by its own ideology … modern culture has compromised the ideals further" (46). In our contemporary society, where our use of the Internet and other technology is monitored, the ideals of "modern culture", such as conformism, are ironically incompatible with contemporary technological advancement, as these ideals discourage the development of new ideas through individualistic thinking, therefore "compromising" any further progress. Habermas shows in these two texts how data publicity is a double-edged sword in that it promotes trust but discourages technological advancement, even if cybersecurity agencies believe otherwise.

The misguided belief in technological advancement as a result of data publicity can be seen in Gabriel Dance's text "As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants". Dance shows Facebook's colossal influence and potential for technological advancement by saying "Facebook has never sold its user data, fearful of user backlash ... it did the next best thing: granting other companies access to parts of the social network in ways that advanced its own interests" (3). Facebook demonstrates the power of technological determinism here, as they created partnerships with other tech giants to "advance its [Facebook's] own interests", which include enforcing cybersecurity efforts among the Internet and growing the tech industry. Technological determinism is also at play when Facebook "advanc[es] its own interests" with respect to "user backlash", which indicates that an advancement of societal values is occurring by satisfying both their goals and the public's desires. Specifically, it suggests a shift

from individualism to conformism among Internet users in order to accommodate with the growing tech industry. Facebook's agency over data privacy is also shown when Dance compares the value of data today to "... the oil of the 21st century, a resource worth billions to those who can most effectively extract and refine it" (3). Because oil is both an important commodity and one of the major driving factors in the U.S. economy, it is able to sway the societal landscape of the U.S. In the same manner, data is one of the greatest proponents of technological determinism, as it shifts societal values, especially those within the U.S. Because of the data's value, anyone or any group with overwhelming control over it is able to control the societal landscape as well, as one can "extract and refine it" by analyzing it in depth in order to hold more control over what data is transmitted via the Internet. Technological determinism is shown by Dance's and Bimber's text to be an integral factor in allowing the NSA and Facebook to continue to function as a body capable of controlling societal values and instilling conformism in Internet users.

Culture

One common theme linking cybersecurity efforts and the privacy of the public's data is the culture promoted among the world of technology. A culture's effect on the risk of a privacy breach is demonstrated through the ramifications of the public's use of information and communication systems, as Chad Whelan writes in his book *Networks and National Security: Dynamics, Effectiveness, and Organisation*. In it, he attributes a culture's (especially the United States) tendency to connect with other cultures as responsible for cybersecurity's justification to publicize what would otherwise be private data. Specifically, he writes, "some of the ways in which technology is used today has really broken down a lot of the cultural barriers because [of] … creating interoperability between previously incompatible systems" (102). Whelan highlights

here that this “interoperability”, or the interconnectedness between various cultural infrastructures via informational and communication systems, has facilitated the efforts of governmental agencies such as the NSA in publicizing data. Online culture has brought upon this change because of the looming fear of privatized data potentially causing harm. However, this interconnectedness also creates problems for these agencies, as it also strengthens connections between various cybercrime networks, making it harder for government agencies to shut them down. Interoperability is shown to be an integral part of the culture surrounding the technological world. Because of its importance, it is one of the major aspects of culture that discourages the privatization of data. Along with governments, companies focused on technological revolution, such as Facebook, are responsible for “[breaking] down a lot of the cultural barriers” among the Internet and promoting interoperability as well. This demonstrates how they are also able to control what data are and aren’t public. Unlike governments, however, they do not have to suffer the burden of enforcing deterrence for cybercrime. Foer demonstrates the rationale of Facebook’s actions with data publicity in his essay, in which he describes the culture surrounding Facebook when he writes “Plenty of companies have similarly appropriated hacker culture--hackers are the un-disruptors but none have gone as far as Facebook … Zuckerberg began extolling the virtues of hacking [into] a philosophy that contains barely a hint of rebelliousness” (105). Hackers are usually portrayed as individuals who intentionally evade cybersecurity efforts merely to subvert the rules driving these efforts exist. However, Zuckerberg’s comprehension of the word “hacking” suggests that he wants Facebook to promote the growth of a culture in which hackers are conforming to the laws of the U.S. government. Because of this grasp of the term “hacker”, Facebook demonstrates that it is able to take advantage of the culture of the technological world in order to pursue similar actions in which it

enforces the goals of the government. As a result, both Facebook and the government have the power over the publicity of the public's data through cybersecurity efforts, even if Facebook does not necessarily bear the responsibility of fighting cybercrime across the country.

Because of the interconnectedness of the Internet facilitated by interoperability, culture is able to transmit potent ideas across the world. One of these ideas is cybercrime fear culture, which promotes a fear of cybercrime in order to abide by governmental standards. Through large-scale cyber attacks such as Wannacry in 2017, where the NSA encountered a ransomware attack, anyone in the U.S. who shares data on a daily basis is coerced into protecting one's privacy at all costs. Steven Brill demonstrates the prevalence of this fear in his article "15 Years After 9/11: Is America Any Safer?". Describing how our culture presents the threat of cyberterror, Brill writes, "...the two most-talked-about threats of the moment—lone wolves and cyberterrorism—so dominate headlines that they may have unduly diverted our focus from bigger dangers … Democracies tend to be reactive, not prescriptive" (45). One of the motivating factors, as shown by Brill, behind the aggressive push of cybersecurity efforts in publicizing data is that our culture promotes fear of cyberattacks, even if it "divert[s] our focus from bigger dangers". This spread of fear is occurring, because, in this "moment", the world is connected through technology more than ever, which also furthers the risk of cyberattacks. Brill is also suggesting that the U.S. government is attempting to be "reactive" by enacting its laws that would further publicize user data and attempt to prevent cybercrime in response to the current technological culture. The "reactive" behavior in which the U.S. is enacting its legislation is in opposition to a "prescriptive" government, which would adapt its laws to a situation such as a cybercrime epidemic. By suggesting this quality of the U.S. government, Brill is showing that fear culture is able to centralize a society's focus on a certain topic such as cybercrime, even if

other issues exist, due to cybercrime's contemporary nature. This societal focus of fear can also be seen by Facebook in Foer's text, when he wrote that "what [Facebook] really wants to advance is the transparency of individual … the sunshine of sharing our intimate details will disinfect the moral mess of our lives" (105). Foer's use of the word "sunshine" indicates that the belief that our data should be publicized is prevalent among the world. Additionally, Foer shows that its prevalent effect will "disinfect the moral mess of our lives", further demonstrating that companies like Facebook place an emphasis on the "moral mess" as an outlet for our fears regarding our data. Because of these fears, the "transparency" of our data will be an integral reason for the enforcement of many of Facebook's policies on data privacy, as it will establish trust among Internet users that no one is hiding malicious data. Cybersecurity efforts employ fear culture, as seen in Foer's text, so that Internet users will be more transparent and vulnerable for their data to be collected for these efforts.

Conclusion

Because of a culture's use of the interconnectedness of interoperability, it is able to spread ideals such as fear of cybercrime in order to coerce the public to put trust in cybersecurity efforts, further exhibiting the power that technological determinism has over a societal landscape such as the U.S. However, culture is also a major vehicle in conveying the ideals of an opposing societal construct to technological determinism known as technological constructivism, which explores how the individual has full control over technology and its advancement. Javier Lezaun explores technological constructivism in his book *Limiting the Social: Constructivism and Social Knowledge in International Relations,* where he discusses how viewing technological growth through the perspective of constructivist theory such as technological constructivism impacts how one views the impact of technology on international relations. In this book, he demonstrates

how technological constructivism promotes individualism when he cites a critic of this theory, Jennifer Sterling-Folker, who “characterizes constructivism as dealing exclusively with identities, norms, understandings, sentiments, and subjective beliefs, while the material, the "real-out-there," is understood as belonging to the domain of the biological” (231). Cybersecurity deters individualism when it publicizes user data by discouraging the expression of qualities such as “identities” and “subjective beliefs”, both of which are essential parts of individualism. Technological determinism shys away from these societal values in order to enforce cybersecurity efforts. However, Folker also claims that the reality of technological advancement, or “the material, the ‘real-out-there’”, strays away from these ideals of individualism. Although Sterling-Folker claims that conformism must occur in order to accommodate contemporary technology, technological constructivism allows for the ideals of individualism to hold while still keeping up with technological advancement. For example, cryptocurrency is a newer technology which allows for electronic ledgers to be privatized for use within select parties, out of sight from cybersecurity agencies. Nick Paumgarten explores the motivations for the creation of different forms of cryptocurrencies with respect to technological constructivism in his essay “The Prophets of Cryptocurrency Survey the Boom and Bust”. In this essay, the creator of a cryptocurrency called Ethereum, Vitalik Buterin, demonstrates the individualism acquired through cryptocurrency when he says “... what drew him in was the elegance of the system, invented, it seemed, by a rogue outsider out of thin air. It suited a world view, a dream of a fluid, borderless, decentralized financial system beyond the reach of governments and banks, inclined as they inevitably are toward corruption and self-dealing, or at least toward distortions of incentive” (Paumgarten 8). The “distortions of incentive” that Buterin hopes to avoid with the advent of cryptocurrency is what discourages the individual’s control over technology, as it

misconstrues the focus of technological development. On the other hand, a “borderless, decentralized financial system” indicates that the individual has no limitations on their control of technology enforced by an outside technocracy, such as the individual’s loss of privacy of his or her data due to cybersecurity efforts. Cryptocurrency is an example of contemporary technology that encourages individualism, as people can make private purchases with cryptocurrency and start businesses based around cryptocurrency. Although technological determinism promises security in conformism through publicity, systems that follow technological constructivism, such as cryptocurrency, can promote more user-friendly technology in order to keep data secure. In fact, Buterin’s vision of Ethereum as a “system, invented.... by a rogue outsider out of thin air” shows a “rogue outsider” can help keep user data private through technological advancement; Buterin’s vision of a “rogue” is in contrast to Zuckerberg’s vision of hackers in Foer’s essay, who are usually portrayed as “rogue outsider[s]”. Zuckerberg desires that hackers enforce invasive cybersecurity strictly instead of displaying a “rebellious” nature. Although an orthodox portrayal of hackers in a technologically deterministic lens and an individualistic portrayal in a technologically constructive lens appear contradictory to each other, they highlight the effects of cybersecurity efforts in their promotion of conformism. Even if Sterling-Folker claims that conformism is what constitutes reality, there exist forms of technology that may soon allow for individualism to be fully expressed, while still complying with contemporary technological advancement, which constitutes reality as well.

The United States is a major leader in sophisticated technology such as smartphones and interoperability through avenues such as social media. One of the major carriers of the United States’ technological advancement is data, the unique information about everyone and everything involved in such technology. Data is a major pathway in which any individual may express his or

her identity. However, this technological advancement, by contrast, also comes with the cost of our individuality, as according to the ideals of technological determinism, technological progression must deter individuality in order to expedite its growth. The data surveillance of the government and tech giants suggests that a societal shift from individualism to conformism is necessary in order to enforce cybersecurity efforts and assist the growth of technology and interoperability among the world. These government agencies and tech giants are spreading the beliefs of conformism through data publicity, ideals of technological determinism, using the interconnectedness of our current technology, such as the Internet. Additionally, cultures such as hacker culture can also solidify these orthodox ideals of technological determinism among the public. On the other hand, a culture can establish individuality in the face of technological advancement by demonstrating the benefits of expressing individuality through the Internet and other contemporary technology. Buterin's vision of cryptocurrency as a decentralized system, free from the limitations of publicity, can manifest into a societal value that encourages individualism. Individualistic technology such as cryptocurrency would make the conformistic nature of cybersecurity more noticeable to the public, as it would become clearer that the development of more individualized technology is hindered by cybersecurity. Although the publicity of data may ensure trust among the public, it is a drastic measure, and its effect may be achieved alongside technological development and individuality instead. Technological advancement has occurred since the dawn of humanity, and its efforts across the world will only grow, further expanding our abilities to connect to others and solve problems once thought unsolvable.

Works Cited

Bimber, Bruce. "Karl Marx and the Three Faces of Technological Determinism." *Social Studies*

of Science, vol. 20, no. 2, 1990, pp. 333–351. *JSTOR*, www.jstor.org/stable/285094.

Brill, Steven. "15 Years After 9/11, Is America Any Safer?" *The Atlantic*, Atlantic Media Company, 18 Jan. 2018, https://www.theatlantic.com/magazine/archive/2016/09/are-we-any-safer/492761/.

Dance, Gabriel J.X., et al. "As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants." *The New York Times*, The New York Times, 19 Dec. 2018, https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html?action=click&module=Top Stories&pgtype=Homepage.

Foer, Franklin. "Mark Zuckerberg's War on Free Will." *The New Humanities Reader*, edited by Richard Miller and Kurt Spellmeyer, Cengage Learning, 2019, pp.100 -116.

Lezaun, Javier. "Limiting the Social: Constructivism and Social Knowledge in International Relations." *International Studies Review*, vol. 4, no. 3, 2002, pp. 229–234. *JSTOR*, www.jstor.org/stable/3186483.

Paumgarten, Nick. "The Prophets of Cryptocurrency Survey the Boom and Bust." *The New Yorker*, The New Yorker, 9 July 2019, https://www.newyorker.com/magazine/2018/10/22/the-prophets-of-cryptocurrency-survey-the-boom-and-bust?reload=true.

Warner, Michael. "Public and Private." *Publics and Counterpublics*, Zone Books, 2005, pp. 21-63.

Whelan, Chad. *Networks and National Security : Dynamics, Effectiveness and Organisation*, Routledge, 2012. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/rutgers-ebooks/detail.action?docID=834072.