Jake Dineen & Nishita Sheth
IST 618
5/27/2018
Privacy Debate

Our team will be arguing *against* the motion.

The motion for debate is:

Libraries should be required to maintain limited historical patron records to assist law enforcement and intelligence agencies to identify US persons who are likely to become radicalized by a terrorist organization.

Opening Statement:

Arguing against the motion that government organizations should have unlimited access to public information, particularly in reference to Libraries, we posit that unlawful search and seizure is a direct contradiction of the 4th Amendment and a gross violation of public trust [1]. The motion presented is representative of the old analogy, “finding a needle in the haystack”, where the haystack is the general American population, and the needle(s) are the few individuals who *potentially* pose physical or existential threats to them. Does the presence and awareness of such individuals warrant the impositions of the government at a level that toes the line between ensuring safety and excessive violations of personal privacy? At what point does the deontologist perspective, arguing for the needs of the many, violate the very principles of American culture? In our argument, we counter the notion that safety and privacy are bounded in a paradoxical paradigm, where the very essence of one marginalizes the promises of the other. Also, we vehemently express the dangers of warrantless suppression of intellectual curiosity and the ‘freedom to read’ brought about at the behest of US President Dwight D. Eisenhower in conjunction with the ALA [2]. At the end of the day, we are looking at a case of willful ignorance of transparency, and we must ask ourselves, to what ends. At what point does do the most common of provocations lead to misclassification and a tipping point is reached?

Jake Dineen & Nishita Sheth
IST 618
5/27/2018
Privacy Debate

Main points w/ factual representative evidence:

Author: Jacob D.

Before the rise of the digital age, libraries were known as the 'original search engines', and as such drew the curiosity of intelligence agencies [8]. Our first argument against the motion that libraries should be required to retain historical patron data for the purposes of conducting counter surveillance against the general American public is that it is a violation of the foundation upon which this country was built, specifically in reference to the 4th Amendment. Uniquities of the motion point to no restriction to the powers and reach of the US government. The 4th Amendment prohibits unreasonable search and seizure without the issuance of a warrant under the notion of probable cause. This is where the argument lies - The government extended their power to require libraries to store probable cause, unbeknownst to us, before determining that there was probable cause. As mentioned in our opening statements, there is nothing wrong with reporting idiosyncratic behavior, with merit, that may be suggestive of impending harm on US citizens. In reference to a particular case, a librarian in Florida recognized three names of from the list of hijackers responsible for 9/11. They phoned the FBI and their computer records were obtained and analyzed. This is a case where there was no advertent skirting of the law, and although the actions occurred after the fact, it was useful to understand potential drivers and habits of extremist activity [7]. The issue lies in the mass collection of behavioral data and tendencies of each and every library patron in hopes of finding the bad egg. It is also important to understand that libraries were protected from such activity before the tragedies of 9/11 and the implementation of the Patriot Act. With the search for information and knowledge shifting mediums in the past 20 years or so, the issue has spread from the libraries onto the internet, and our phone lines, without transparency.

Another important argument against the motion is the arbitrary assignment of what constitutes behavior, or content, that is a predictor of terroristic ideology. With such a small portion of the public across the world falling into the 'sympathizer' or 'extremist' bucket, it is difficult to statistically represent patterns with the unpredictability of human nature. Who draws the line between what is intellectual curiosity and knowledge seeking against psychopathy derived from undying loyalty to an evil cause? Particularly

in a library setting, where the terrain is not whittled down by hyper specific filters, and no sense of intent can be derived without forms of verbal or written expression. What the motion describes is the government asking for the ability to speculate without cause, and that is simply not acceptable. There are many cases over the past 20 years, as this debate of privacy has raged on, where librarians and the ALA have stood against government surveillance. As far back as 1987, there was an FBI program called the *Library Awareness Program*, where FBI personnel were responsible for recruiting librarians to act as spies in order to infiltrate and relay information that *might* relate to Soviet intelligence gathering. This was opposed aggressively by the ALA, and deemed a gross appropriation of a librarians' duties - An excerpt: "I find it amazing that a librarian could be supposed to recognize someone who is a national of a foreign power. Does anyone with an accent come under suspicion" [9]. Research indicates that the motion at hand rose to commercial prominence after the initiation of the Patriot Act, but it is really a war the government has been fighting, secretly, against its citizens for some time.

In reference to the readings combined with this week's asynchronous material, we delve into the 'Nothing to Hide' argument, which has become a prevalent rallying cry for a pro-surveillance state. The argument of a 'nothing to hide' mentality positions itself as a necessary tradeoff between privacy and safety, where one should turn a shoulder to the possibility of embarrassing data or behavioral patterns being analyzed or fed into a machine in obtainment of a greater good. If one truly believes that they are doing nothing wrong, they should have no issue sharing their personal data, no matter how intimate. This gets into a key point about privacy. People are not unwilling to share data that they don't deem sensitive - We do this all the time in contractual settings where we are trading some non-personal information for access to a functional utility. However, people do feel hesitancy to share information that could lead to the systematic management and disruption of their persona - "affect[ing] social structure by altering the kind of relationships people have with the institutions that make import decisions about their lives" [3]. As the article mentions, proponents for the argument may counter that Americans are seizing their rights when interacting with companies and should have no reasonable expectation of privacy. This contractual agreement between third parties

and American citizens opens the door, as ruled by the Supreme Court [3], for the government's unlimited and unrestricted access to personal identifiable information (PII) with no regard to oversight. This leads way to our next point about chilling effects.

My final point will be broad in nature, focusing not only on the chilling effects of a surveillance state, and the potential economic impact of suppression of Free Speech and intellectual curiosity, but also about the infrastructure with which our data is being stored, with or without or explicit consent. As Solove notes [3], surveillance of legal activities (normal day to day routines), can inhibit one's' willingness to engage in them. This works in unison with the point above about the alteration of our own unique social structure. More harmful, however, would be the resulting reduction of viewpoints and the unintended muzzling of freedom derived from a position of fear. A country founded on and evolved from differing perspectives may unintentionally be muting and stripping the voice from active members of our democracy. The direct economic response to such a situation would be impossible to quantify, but the suppression of ideation could, in theory, lead to a decline in innovation. Moreover, we continue to analyze the Solove article, and note issues with the concept of having nothing to hide. Fragments of collected data can be aggregated, and predictive analytics can have their run at predicting future decision making at an intricate level. You would not only be subscribing to government surveillance on your past, but also probability distributions of your future actions. We touch on machine learning in relation to National Security again below, but there are obviously some hazards and issues of control & power present in that landscape. Lastly, we discuss the issues of unified storage of some of our most pertinent private information. As we have seen in recent years, particularly with the Equifax breach, there is real cause for concern with the widespread collection of vital information, whether it be financial or not. What we need to know, as American citizens, is that, beyond reasonable doubt, our data is secure. Disregarding government mistrust derived from the Snowden revelations, it is difficult to ponder the scale and impact of a data leak from a government intelligence agency that impacts the American people in totality.

Main points w/ factual representative evidence:

Author: Nishita S.

Many librarians today argue about their increasing concern on the privacy and confidentiality about their patrons. There have been numerous debates on the same. Yet, the question “Should should be required to maintain limited historical patron records to assist law enforcement and intelligence agencies to identify US persons who are likely to become radicalized by a terrorist organization?”, remains unanswered.

In my opinion, the answer should be “No”. No, libraries should not maintain any patron records or if maintained, should not make the same accessible to any third party.

American Library Association has stated privacy as one of its core values. In order to support privacy at its core, library professionals are committed to facilitating and not monitoring access to information within any library premise. Maintaining privacy in any library setting is important to ensure that individuals can seek, read and learn based on their choices and preferences without the fear of being judged, punished, damage their reputation or embarrassed. Altering this privacy arrangements within libraries can force readers to practice their first amendment right to read and also destroy the main motive of libraries - free access to information (Advocacy, Legislation & Issues, 2018).

Most readers may argue that most libraries maintain information on how accesses what book along with some personally identifiable information, for example, name email id, etc. However, information if maintained should remain confidential, ensuring libraries grow as a center of free access to information and knowledge along with freedom of inquiry (Advocacy, Legislation & Issues, 2018).

Earlier in this debate we discussed about the analogy, “Finding a needle in the haystack”, where we refer to the needle being those few who pose a threat to national security. However, it is also important to consider how this continuous monitoring of individuals without any prior strong evidence can draw us to conclusions and patterns which are not true or how some may call it “false positive”.

This draws me to talk about incidents from a Bollywood movie - “New York”. The movie discusses the story of three students studying in New York, one of who was detained as a terrorist after the 9/11 attacks. After thorough investigation, it was discovered that the

student was not guilty and had conducted a research on The World Trade Center as a part of his curriculum. The aftermath of this detention resulted into the student joining a terrorist organization on release from the detention center in order to answer the impeachment of his rights and privacy.

This incident summed up with statistics from Guantanamo Bay Detention Center can be terrifying. Evidence shows that only 6 out of 166 prisoners at the Guantanamo Bay Detention Center face formal charges and around 30% of the released prisoners from this detention center go back to battle after release (Postel, 2018) (Sherman, 2017).

Now consider, all these numbers and scenarios with respect to the monitoring of patrons at a library and try finding answers to the following questions. What are the odds of librarians intercepting wrong information about patrons? What is the possibility of an individual learning about arms or ammunition for educational or recreational purposes? What is the possibility of these patterns and monitoring resulting into monitoring and eventually, detention of innocent individuals? Lastly, what is the probability of these innocent individuals then returning to battle to seeks answers against this injustice?

Most of us might agree, that people of who seek information on terrorism are not necessary likely to become terrorism. I agree, the above-stated scenario may seem rare, maybe one in a million such case might take place. But is it fair, if we give birth to even one such terrorist due to lack of evidence and based on unreasonable data from their personal preferences of readings and books? Assuming an individual’s motive based on their reading preferences make no sense and additionally, waste legal resources as well as poses a threat to people’s knowledge on current affairs and events (Advocacy, Legislation & Issues, 2018).

Most of us have witnessed the after effects of Edwards Snowden revelations about NSA. Researchers have argued about the aftermath of widespread government surveillance and how it has encouraged meekness and conformity. Aftermath of monitoring and maintaining patron records can have similar effects. If we think someone is watching our actions, we are bound to not perform certain actions in order to avoid been looked at suspiciously (Guo, 2016). Evidence shows a 20% decrease in page view of Wikipedia articles on terrorism or related activities after NSA document leaks (Guo,

2016). Library being the hub of learning and education, one can only imagine the decrease in patrons urge to seek information if they knew they are being monitored. This might also result in uninformed citizens (Guo, 2016).

Another important argument that I would like to shed light upon is the linear relation between freedom of thought, freedom of speech and freedom of inquiry. Many librarians from their experience have stated that the above-stated rights go hand-in-hand and restraining rules on freedom of inquiry may have direct repercussions on freedom of speech and freedom of thought and that such repercussions of people deterring from learning and inquiring about important policy matters can also pose a threat to democracy (Guo, 2016) (Roberts, 2015).

2 questions to ask the other side:

1. If the government were allowed to act and react to circumstance without a semblance of transparency and no bounds to their reach, what would be the economical impact, long term, of a fallout/decline of innovation resulting from a lack of intellectual curiosity? Would culture adapt, or would heightened restrictions and fear of generalization/stereotypes lead to a decline in the digital era/age of information?
2. What dangers arise with arbitrary assignment of ‘dangerous content’, and who is deciding which content has a causal relationship with terrorist activity? Is it possible that illogical relationships will be formed between specific content and behavioral classification?

3 questions likely to be asked w/ answers:

1. The idea that an objection to government overreach is not American is an obvious counterpoint. Why would people willingly refuse to assist government officials in keeping the general American public safe - a point of view the opposite side of the spectrum might pose. The issue is not in the legal and lawful search of individuals who are deemed to have terrorist ties or are known sympathizers is not, in and of itself, unlawful. If you see something, you should say something, as the post 9/11 slogan goes. But even that slogan, as presented

by the Department of Homeland Security, is accompanied by its own set of rules, namely discouraging physical appearance as a regressor of an unsafe environment. The practice of collecting every single American's personal and private data in order to build user profiles on terrorist candidates, and probabilistically determine those ties in order to conduct predictive psycho-analysis as a countermeasure isn't only a violation of privacy, but it is an unethical injection of bias/variance into machine learning models. Turning to machine learning for probability densities against known classes, in this case terrorist vs innocent, is a practice that is utilized by the NSA in Pakistan (I've cited the sources below but can't find any academic resources pertaining to 'Skynet' and the NSA's use of the below). Random Forests are mainly used to fit a model which approximates a function between psychographics, demographics, behavioral patterns, etc. against known class representations. The issue, as is noted in the reference, is that the models tend to overfit due to severe class imbalance. What this leads to is cases of false positives, eg. innocent people are classified as terrorists and are thus subject to military operation. Although the false positive rate is miniscule, in a country with a population as large as Pakistan, there are still unacceptable civilian casualties. In our perspective, although slightly beside the point, widespread collection of user data in this instance might not only be an overreach, but could potentially, even if accidentally and done with notions of the greatest good in mind, be classified as a war crime [4,6]. It could also be a case, as we reference our past assignment, of a spinoff of the principal agent problem, where a machine is ultimately providing analysis that is leading to human action, which will impact the known principal [5].

2. *"Etzioni is right to critique those who argue that privacy is an individual right that should trump social interests. The problem, however, is that utilitarian balancing between individual rights and the common good rarely favors individual rights—unless the interest advanced on the side of the common good is trivial. Society will generally win when its interests are balanced against those of the individual"*

[3] - This is likely the main counterpoint to our argument against the motion. We touch upon this directly above, but the idea that terrorism and counter surveillance is looked at as an individual vs societal issue, and our culture generally leans toward a deontologist paradigm, means that we might be willing, in theory, to sacrifice our freedoms in order to ensure our safety. Our argument would be that the interest being advanced at the expense of our privacy is, in fact, trivial. For example, the referenced New York Times (opinion) article suggests that the enhanced data collection techniques are backed without a semblance of evidence that they work. They note that NSA has failed to show that a single terrorist attack has been thwarted via the use of phone taps [12]. Instead, most thwarted attacks are the result of more traditional techniques, such as government informants and social media analysis. A white house panel in 2015 conceded that they had no actual records of phone surveillance leading to any disruptions of terror plots [13]. This extends beyond the original motion but contributes evidence to the position that mass surveillance may not coincide with heightened security.

3. Most of us might say that a law-abiding citizen of the country has “Nothing to Hide” and should not fear anything. Such surveillance practices are only meant to monitor and keep an eye over those who pose a threat to national peace and dignity. However, one important specification that we miss while making this argument is that these surveillance and monitoring activities do not only monitor an individual when they access or inquire about topics like terrorism or murders. In fact, irrespective of the information that you access you are going to be watched. Now, consider you have been accessing and reading you information related to your sexual preference and are being watched by the library staff and detailed for even the minutest of the information. For example, “Which book did you access?”, “How long did you read the book for?” etc. In many countries, even today people do not openly disclose their sexual preferences or sexuality. Now imagine, an individual reading on rules and regulations about a particular community, say, LGBT community, and is being watched by the library staff to

ensure record-keeping. Wouldn’t it result into an embarrassing situation for the patron? Or wouldn’t this harm his/her reputation in a society where people defame such references? It could also cause him to refrain from accepting his own choices and learning about them, from the fear of being judged. Though such situations may not be harmful in certain societies but is surely something some may hide in less liberal societies. Another argument made in this motion can be, “What harm can it possibly cause if this data was captured/monitored by a few?”. Agreed, it might not be devastating if the data was restrained in ownership of only a few. But into today's tech-savvy and insecure era, who can ensure confidentiality of this data? With examples of data breaches of not only private but also government data being encountered everyday no individual can be secured if such data gets leaked in a socially unliberal society. This summed up with the fear of being exposed, judged and harmed falsifies the analogy of “Nothing to Hide”.

References:

[1]Staff, L. (2017, October 10). Fourth Amendment. Retrieved from https://www.law.cornell.edu/constitution/fourth_amendment

[2]The Freedom to Read. (2018, May 22). Retrieved from https://americanlibrariesmagazine.org/2016/03/15/freedom-to-read/

[3]S., & J., D. (2007, July 12). 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565

[4]Christian Grothoff & J.M. Porup. (2016, February 16). The NSA's SKYNET program may be killing thousands of innocent people. Retrieved from http://arstechnica.co.uk/security/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people

[5]Staff, I. (2018, January 23). Principal-Agent Problem. Retrieved from https://www.investopedia.com/terms/p/principal-agent-problem.asp

[6]Zetter, K. (2017, June 03). So, the NSA Has an Actual Skynet Program. Retrieved from https://www.wired.com/2015/05/nsa-actual-skynet-program/

[7]Egelko, B. (2012, January 30). FBI checking out Americans' reading habits / Bookstores, libraries can't do much to fend off search warrants. Retrieved from https://www.sfgate.com/politics/article/FBI-checking-out-Americans-reading-habits-2826830.php

[8]Roberts, D. (2015, June 05). NSA surveillance: How librarians have been on the front line to protect privacy. Retrieved from https://www.theguardian.com/world/2015/jun/05/nsa-surveillance-librarians-privacy

[9]The FBI library awareness program: An analysis. (n.d.). Retrieved from https://www.tandfonline.com/doi/abs/10.1080/02684529208432158?journalCode=fint20

[10] Postel, T. (2018). How Guantanamo Bay's Existence Helps Al-Qaeda Recruit More Terrorists. [online] The Atlantic. Available at: https://www.theatlantic.com/international/archive/2013/04/how-guantanamo-bays-existence-helps-al-qaeda-recruit-more-terrorists/274956/ [Accessed 27 May 2018].

[11] Sherman, A. (2017). How many released Guantanamo prisoners re-offend?. [online] Politifact. Available at: http://www.politifact.com/florida/statements/2017/jan/25/cory-gardner/how-many-released-guantanamo-bay-prisoners-commit-/ [Accessed 27 May 2018].

[12]Opinion | Mass Surveillance Isn't the Answer to Fighting Terrorism. (2017, December 21). Retrieved from https://www.nytimes.com/2015/11/18/opinion/mass-surveillance-isnt-the-answer-to-fighting-terrorism.html

[13]NSA program stopped no terror attacks, says White House panel member. (n.d.). Retrieved from https://www.nbcnews.com/news/world/nsa-program-stopped-no-terror-attacks-says-white-house-panel-flna2D11783588

[14] Advocacy, Legislation & Issues. (2018). *Privacy*. [online] Available at: http://www.ala.org/advocacy/privacy [Accessed 27 May 2018].

[15] Guo, J. (2016). *New study: Snowden's disclosures about NSA spying had a scary effect on free speech*. [online] Available at: https://www.washingtonpost.com/news/wonk/wp/2016/04/27/new-study-snowdens-disclosures-about-nsa-spying-had-a-scary-effect-on-free-speech/?noredirect=on&utm_term=.a975f68edde8 [Accessed 28 May 2018].

[16] Roberts, D. (2015). *NSA surveillance: how librarians have been on the front line to protect privacy*. [online] The Guardian. Available at: https://www.theguardian.com/world/2015/jun/05/nsa-surveillance-librarians-privacy [Accessed 28 May 2018].