Possible Methods of Web Surveillance of Students at Tufts University and How Students Can Evade them

1 Abstract

Students at Tufts University are given many resources by the institution. However, many of these resources -- such as Tufts email, Tufts school computers, and Tufts Internet networks -- put students' data in the hands of the university in unnecessary ways. This paper outlines possible ways Tufts University could use its position as provider of these services to collect and monitor information about its students on computers in 2016, why undisclosed surveillance programs are a problem, and ways that students can evade these tactics.

2 Introduction

In 2014, Tufts University updated its surveillance camera policies and expanded its network of video security cameras.[1] The expansion of this program demonstrates one way that the monitoring of Tufts' physical campus is changing. The monitoring of students, however, is not limited to cameras, and extends even to forms of electronic communication and other computer-based activities.

This paper is meant to compile facts about some information about students' computer related activity Tufts has access to. Though it is possible that Tufts is not actively using this information, it is important that people know what information Tufts (or any other relevant institution) has access to, so that they can make informed decisions about what parts of their information is shared and in what places.

3 To the Community

In 1956, the FBI launched its COINTELPRO or counterintelligence program to monitor and disrupt the activities of several resistance movements in the U.S. This illegal program targeted popular leaders like Martin Luther King Jr.[2], contributed to the collapse of several political organizations, including the Black Panther Party, and resulted in the assassination of several political figures, including Fred Hampton, a revolutionary Black organizer.[3] The FBI, a federal agency, ran COINTELPRO, and while COINTELPRO was in operation, its

---

[1] "Video Security University Policy," *Tufts* University, 2014.
[2] "COINTELPRO and the History of Domestic Spying," *News and Notes*, NPR, January 18, 2006.
[3] "'The Assassination of Fred Hampton: How the FBI and the Chicago Police Murdered a Black Panther,'" *Democracy Now!* December 4, 2009.

activities were not disclosed to the public. The program did not end until the 1970's.[4] This is relatively recent history, and it is not hard to imagine similar counterintelligence or surveillance programs taking place in the present, especially given the nature of our "racist, xenophobic, authoritarian, climate science-denying, misogynistic, revenge-obsessed ego-maniac"[5] president elect.

As can be seen when examining COINTELPRO, surveillance programs have the potential to become unreasonably intrusive and deadly. This is because when institutions operate surveillance programs undisclosed to the public, there is no accountability for how the information they obtain is used. This is true of both the federal government and of other institutions, like Tufts University. I do not mean to suggest that Tufts is working to assassinate student organizers, but Tufts does have within its power the ability to monitor and store a lot of information about its students. While some of this is necessary to maintain academic records and to perform the expected functions of a university, it is clear that Tufts has access to information that does not serve these purposes, and that it is obtaining this information in ways not clearly disclosed to students.

4 Possible Methods of Surveillance

In the sections below, I will outline some of the major technologies that students use that make them vulnerable to web surveillance. This is not a comprehensive list, but a good starting point for thinking about what activities make students' information vulnerable to surveillance.

4.1 Tufts Email

Due to the nature of email, users should never have an expectation of privacy. According to Tufts University's online email policy, "Tufts cannot guarantee the security, privacy, and confidentiality of email. Users should not assume confidentiality of their email."[6] This alone should be enough to cause students to not trust email, and encourage them to suspect that university administrators can read their messages. I also had a conversation with a systems administrator in Halligan, and he confirmed that he, as a root administrator, has the ability to read emails.[7] He also added that he would not choose to do that unless he was asked to by an investigator, but the fact remains that certain Tufts employees have the power to read students' emails.

4.2 Tufts Wireless Networks

Tufts-Guest, Tufts-Wireless, and Tufts-Secure are all wireless networks provided by Tufts. Tufts-Guest can be accessed by anyone on campus, regardless as to whether or not they are

---

[4] "'The Assassination of Fred Hampton: How the FBI and the Chicago Police Murdered a Black Panther.'"
[5] Micah Lee, "Surveillance Self-Defense Against the Trump Administration," *The Intercept*, November 12, 2016.
[6] "Email Policy," *Tufts Technology Services*.
[7] Patrick Hynes, Personal Interview, 7 December 2016.

a student. However, that network is slow, has limited bandwidth, and is less secure than the other networks.[8] As a result, most students opt to use the Tufts-Wireless or Tufts-Secure wireless networks. In order to use these networks, students must register their devices, meaning that all of their wireless traffic is directly associated not only with their IP address, but also with their tufts.edu account.[9] This means that, when students use Tufts-Wireless and Tufts-Secure networks, Tufts University can easily associate their tufts.edu account (and therefore their identity) with whatever websites students access and whatever files students download.

4.3 Tufts Computers, Personal Computers, and Other Personal Devices

In buildings like Eaton Hall and Tisch Library, students can access computers owned by Tufts. These accounts, however, are Windows users accounts, meaning that any files saved to them can be seen by an administrative user, who in this case are Tufts employees.[10]

Saving files to a personal computer can protect them from being read by Tufts computer administrators. However, if that computer, or any other personal device like an iPhone, were to be detained by law enforcement, those files could be accessed unless they are properly protected.[11] Protection methods will be discussed in section 6.

4.4 Third Party Services

Tufts may also obtain student information through third-party online companies. Many popular services, like Facebook and Google, collect a lot of information about their users. They have access to the messages that users send back and forth between each other, photos that users post, as well as other kinds of personal information.[12] This in itself is worrying, but it is made relevant to Tufts because Tufts has its own police department. It is known that Facebook serves 81.41% of law enforcement requests for user data.[13] This means that, if a law enforcement agency is suspicious about a particular students activity on Facebook, perhaps they suspect that a student is organizing a nonviolent direct action, and want to see that student's Facebook posts, messages, or other information, Facebook provides that data the vast majority of the time. This is not unique to Facebook and similar social media companies. Cell carriers have responded to millions of law enforcement requests for call data, and also respond to requests for location information.[14] According to the *New York Times*, "cellular systems constantly check and record the location of all phones on their networks," and typically retain geographic information for a year or

---

[8] "Guest Wireless," *Tufts Technology Services*.
[9] "Tufts Secure Wireless," *Tufts Technology Services.*
[10] "Running with Administrator Privileges," *Microsoft Development Network*.
[11] Micah Lee, "Surveillance Self-Defense Against the Trump Administration."
[12] Lauren Williams, "Why There's No Such Thing As A Private Facebook Chat," *Think Progress*, May 8, 2014.
[13] United States Law Enforcement Requests for Data," Facebook, 2016.
[14] Peter Maass and Megha Rajagopalan, "That's No Phone. That's My Tracker."*The New York Times*, July 13, 2012.

more.[15] This shows that students' Facebook communication, phone communication, and location information is just a request away from being accessed by the university.

5 Known Cases

In November 2016, the *Tufts Observer* published an article about student experiences with wireless network monitoring at Tufts. One of the common experiences that students noted was that Tufts' internet usage policies and rules were vague, and that, as a result, the consequences of their (mis)usage of wireless networks were unexpected. For example, one student had the Internet disconnected from their devices, and another noted that private plans for her student group's protest were known by police despite the fact that neither she nor anyone in her group had posted the plans publicly. [16] Given that student activist groups have a tendency to use non-Tufts based channels of communication like Facebook to plan their direct actions, this example suggests a link between the information that Facebook has about students and the information that Tufts has about students, perhaps through Tufts University Police Department. The lack of disclosure of surveillance activities is a common complaint about many institutional surveillance programs, and can be seen in both of these examples.

One other common complaint about surveillance programs is that the people being monitored do not have a say in how the information that the institution secretly collects is used. I have personal experience with Tufts University blurring the lines between what information about me is private and what information about me is public. In March 2016, photos of my private dorm room were posted online. I did not take the photos and I did not give consent to them being posted on a semi-public online survey. Thought the survey was taken down after a professor helped me voice my complaint, this experience shows an example of the university collecting undisclosed data (in this case, photographs) about students and an example of them experimenting with ways that this data can be used. This collection and experimentation is being done without the knowledge of students.

6 Defenses

Below I will describe several methods students can use to evade the surveillance tactics described above. This is not a complete list of defenses, but a good starting point for better protecting students' information. It should be noted that they do not provide full privacy, but that better security practices can help to keep information more private than it might otherwise be.

6.1 Non-Web Based Communication

If a member of the Tufts community wishes to keep their online activity separate and inaccessible to anyone at the university, that activity should not be conducted on Tufts' wireless networks, and probably should not be conducted online at all. Communicating in

---

[15] Peter Maass and Megha Rajagopalan, "That's No Phone. That's My Tracker."
[16] Lauren Samuel, "Spinning the Web: Navigating Tufts' Wireless Networks," *The Tufts* Observer, Fall 2016.

person and away from electronic devices is the safest way to avoid computer- and internet-based monitoring.

6.2 Virtual Private Networks for More Secure Browsing

Virtual Private Networks, or VPNs, protect Internet traffic from surveillance on the public network.[17] This means that, if students use a VPN to connect to the Internet, Tufts systems administrators would be unable to see their Internet traffic.

Using a VPN comes with tradeoffs, however. It slows down the speed of students' Internet service and some VPNs monitor and save a user's browsing history. But if a student were mainly concerned about their Internet browsing being watched by administrators at Tufts, a VPN would help them avoid this.

6.3 Encryption

Encryption is a technique used to make information more secure, and when done correctly, greatly increases the chances that only the owner of the information and/or people of the owner's choosing can access the encrypted information.[18] It is a useful tool in evading surveillance.

6.3.1 Encrypted Devices

Saving personal files and information to personal computers makes that information more private than saving them to computers owned by the university. However, if law enforcement were ever to detain a personal computer (or phone), if it were not properly protected, they would be able to access any of the files saved on that device.[19] To prevent this from happening, it is important that students encrypt their devices. Encrypting their computer means that their files can only be accessed if the person who is trying to access them has the correct password. Without this password, law enforcement would be unable to extract information from their device.

6.3.2 Encrypted Communication

Instead of using services like Facebook Messenger or Gmail to communicate, students can use encrypted communication services to protect their data. Signal is free software application for Android, iOS, and Desktop that uses end-to-end encryption to protect user's data.[20] Because Signal uses end-to-end encryption, even if law enforcement were to request a user's Signal messages from the company, all Signal as the service provider would be able to provide is the time the user created their account and the last time the user connected to the Signal server. Because all information is encrypted, Signal would not even be able to

---

[17] "Choosing the VPN That's Right for You," *Electronic Frontier Foundation*, June 9, 2016.
[18] "What is Encryption?" *Electronic Frontier Foundation*, April 4, 2015.
[19] Micah Lee, "Surveillance Self-Defense Against the Trump Administration."
[20] "How to: Use Signal on iOS," *Electronic Frontier Foundation*, November 30, 2016.

provide the user's contacts, never mind the actual contents of their messages.[21] This makes it an ideal method for secure electronic communication.

7 Conclusion

Tufts has access to a lot of information about students that is not vital to carrying out its functions as a university. Thus, as students, it is important that we are aware of the history of past surveillance programs and the tendency of surveillance programs to lack disclosure and accountability. It is also important that we think carefully about what information about ourselves we are willing to allow the university to have access to. This is especially important for student organizers to consider. For example, at Tufts, secure communication is vital to forming labor unions, to addressing violations against bosses in the workplace, to communicate about direct actions, and to prepare for strikes. These are just a few applications; there are many other activities that Tufts has an interest in monitoring and knowing about. Understanding the technology that is being used to plan and communicate is essential to protecting information.

by: Elizabeth B.
Last Updated: December 2016

[21] Micah Lee, "Surveillance Self-Defense Against the Trump Administration."

Works Cited

"Choosing the VPN That's Right for You." *Electronic Frontier Foundation*. June 9, 2016. https://ssd.eff.org/en/module/choosing-vpn-thats-right-you

"COINTELPRO and the History of Domestic Spying." *News and Notes*. NPR. January 18, 2006. http://www.npr.org/templates/story/story.php?storyId=5161811

"Email Policy." *Tufts Technology Services.* https://it.tufts.edu/email-pol

"Guest Wireless." *Tufts Technology Services.* https://it.tufts.edu/guestwireless

"How to: Use Signal on iOS." *Electronic Frontier Foundation*. November 30, 2016. https://ssd.eff.org/en/module/how-use-signal-ios

Hynes, Patrick. Personal Interview. 7 December 2016.

Lee, Micah. "Surveillance Self-Defense Against the Trump Administration." *The Intercept*. November 12, 2016. https://theintercept.com/2016/11/12/surveillance-self-defense-against-the-trump-administration/

Maass, Peter and Megha Rajagopalan. "That's No Phone. That's My Tracker." *The New York Times*. July 13, 2012. http://www.nytimes.com/2012/07/15/sunday-review/thats-not-my-phone-its-my-tracker.html

"Running with Administrator Privileges." *Microsoft Development Network*. https://msdn.microsoft.com/en-us/library/windows/desktop/ms717801(v=vs.85).aspx

Samuel, Lauren. "Spinning the Web: Navigating Tufts' Wireless Networks." *The Tufts Observer*. Fall 2016. http://tuftsobserver.org/spinning-the-web-navigating-tufts-wireless-networks/

"'The Assassination of Fred Hampton: How the FBI and the Chicago Police Murdered a Black Panther,'" *Democracy Now!* December 4, 2009. https://www.democracynow.org/2009/12/4/the_assassination_of_fred_hampton_how

"Tufts Secure Wireless." *Tufts Technology Services.* https://it.tufts.edu/securewireless

"United States Law Enforcement Requests for Data," *Facebook*, 2016. https://govtrequests.facebook.com/country/United%20States/2015-H2/

"Video Security University Policy." *Tufts* University. 2014. http://publicsafety.tufts.edu/policies/video-security/

"What is Encryption?" *Electronic Frontier Foundation*. April 4, 2015. https://ssd.eff.org/en/module/what-encryption

Williams, Lauren. "Why There's No Such Thing As A Private Facebook Chat." *Think Progress*. May 8, 2014. https://thinkprogress.org/why-theres-no-such-thing-as-a-private-facebook-chat-3d590b7705b3#.43pt8n87m