Adish Betawar

AMS 1B

Prof. Frank

5/10/2016

A Revisitation to Our Aerial …(Friend/Foe)?

In my previous paper that I wrote in the fall, meaning during the days of AMS 1A, I talked about the dangers about the use of UAVs, to survey civilian population for suspicious activities. In that paper, I discussed some of the minor political hotspots of this problem as well as how some organizations are fighting to ensure that we allow us to maintain our continued use of privacy. Now as we forward to the present, we see that the situation of drones and other UAV automatons are still posing a rather questionable debate wether or not it is a good thing or a bad thing.

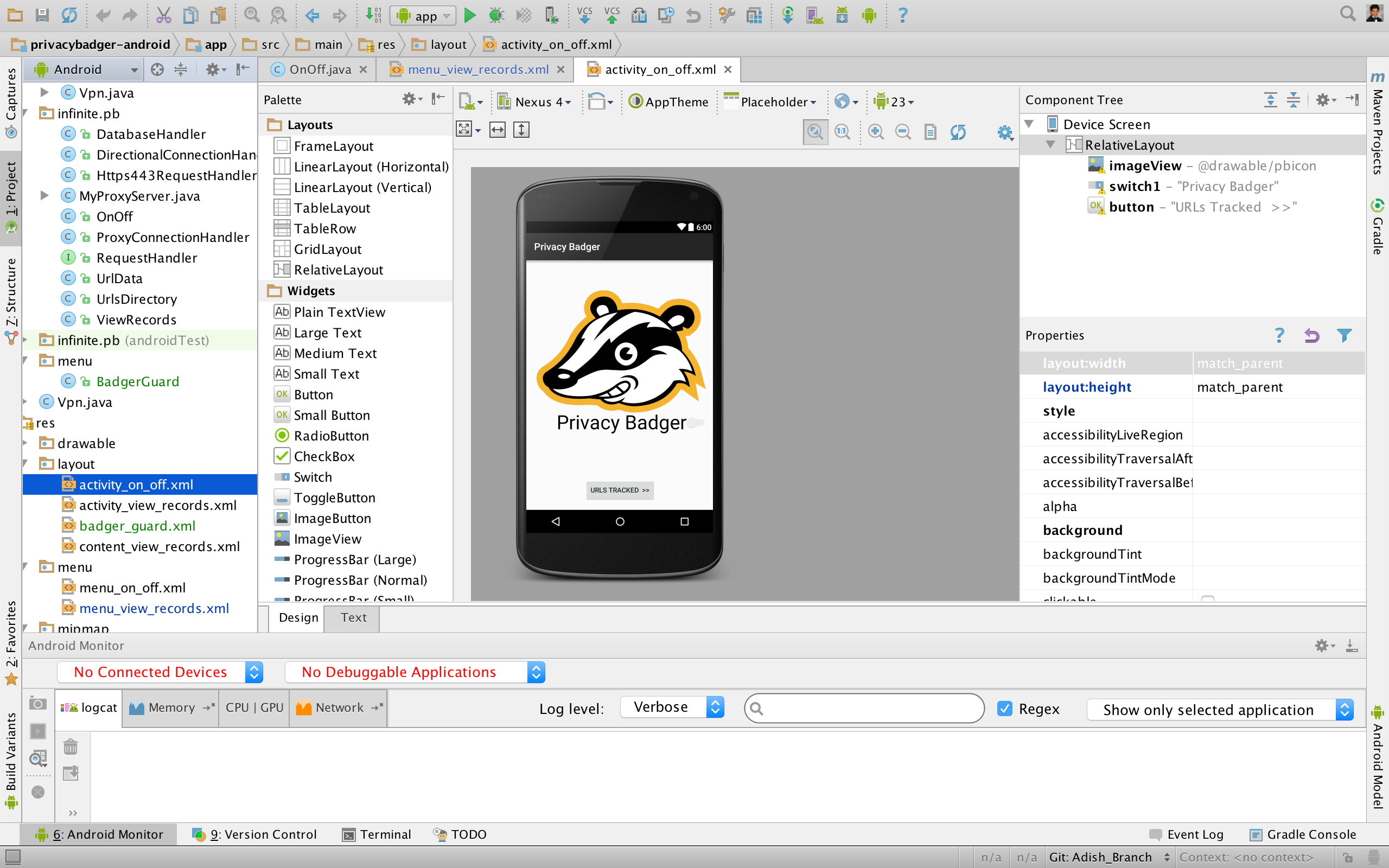
As we all know, there is no written law guaranteeing our right to privacy. A great number of organizations have addressed this problem through a variety of approaches. The American Civil Liberties Union, or the ACLU for example, has repeatedly addressed this problem through a theoretical approach by embarking on campaigns in order to try and limit the use of these UAVs. Their most recent success for this organization was in New Jersey, where they organization was able to urge the courts to pass a new law to allow police to acquire a warrant if they want to survey an individual with the use of domestic drones.

While the ACLU does address the issue with regard to civil rights and privacy, it seems that they are only concerned with the short term goal of more privacy for the people. They don’t seem to know what seems to be more important for the long term. I would say this because just because we win some privacy today it doesn’t mean that our safety will be any less significant then it was before. While this organization worked through court cases and inspire public support for this and other issues pertaining to civil rights, another organization, the Electronic Frontier Foundation, goes on the direct route to solve our problems.

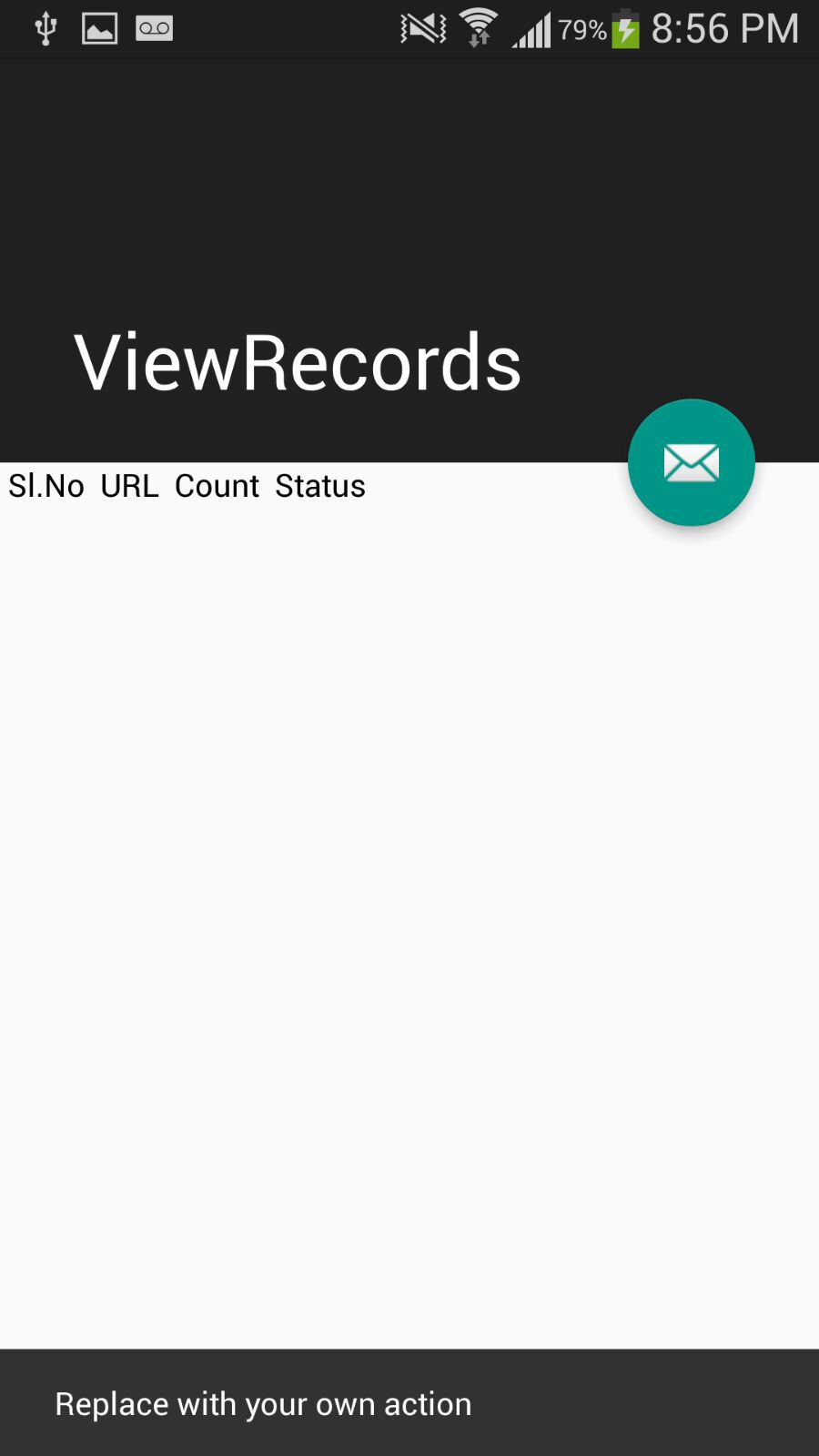
Another organization that addresses the problems of civilian surveillance with the use of UAVs is the Electronic Frontier Foundation, or the EFF. They go on the offensive when addressing this problem as well other internet related problems. They have developed numerous pieces of software that we can use to protect ourselves on the internet as well as from limited hardware. They are currently trying to develop a kit that can help us mask our identities from UAVs to a certain extent. The EFF also has compiled a rough map of approximate zones of UAV activity authorized by the U.S government for other kinds of things. In case you did not read my previous paper, I primarily worked with the EFF and their direct approach for tackling the problem.

As mentioned in the paragraph above, I primarily worked wth the EFF. The reason why I went along with them was because the ACLU could not honor my request for a service project during that time. My role at that time was to sort through papers and do some office work. I admit, not the best kind of service ever but I did get to see some insight into the problem. The EFF has kept tabs on certain different drones operating within the United States, both military as well as scientific. I took a look at it and realized that they were trying to develop a program that could potentially ‘arm’ civilians in a way to be aware about which drone is tracking them and which ones are not. From that list, six of the eight or more drones that I looked at were currently active. When I checked their website with that same chart, five of those drones are currently marked active. This led to my most important inference from my experience. The most important inference that I made while was that not only do they actively work to support digital rights for people, but they also help to develop tools to engage with the audience so that they can be protected on the web.

The use of UAVs for domestic surveillance proves to be both a social and political issue with the American public. The problem with domestic surveillance with the use of UAVs can be linked to Political and social inequality within our society. At first glance, I thought that the cause of this problem comes from the post 9/11 paranoia that feeds the government with more excuses to get citizens to give up more of their already bare minimum amount of privacy that they have to ensure the safety of the nation for another day.

Benjamin Franklin once said, “Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety”(Wittes 2). The quote suggests that one of our founding fathers would never want our population to become a bunch of sell outs who would let government agencies survey the population with little to no awareness from the public just like that. The political side of the inequality argument comes from the fact that although organizations such as the ACLU and the EFF try their best to try and urge the courts to impose limits on the use of UAVs, with more and more world leaders stockpile on nuclear weapons (e.g North Korea), it only makes sense to surrender some privacy rights for the sake of national security. Besides, according to Pew Research, it appears that more Americans approve of the use of Drones for government and consumer use, but not so much for surveillance (Dorr, Les, and Alison Duquette 44), which must be due to the numerous benefits that Drones provide in general. Overall, the Domestic surveillance by UAVs shows just how far our local and federal government will go to try and protect their citizens at the cost of targeting a new groups of people who could fit the criteria of being considered as a potential target("Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft.” 44).

Coming up with a rudimentary solution to this particular problem was difficult, especially since according to the basics of networking protocols, you cannot connect to a host device directly because you have to get permission from the master controller in order to do so. So a direct approach was not possible, and since I really don't like simple things like flyers or pamphlets, I decided to do something else. Thankfully, I do have some experience with computer programming thanks to my academic minor. So I was able to somewhat help the organization that I was working with directly on a current ongoing project. I worked with my organization on an Android application that they are currently making. The project’s name is Privacy Badger and the primary intention of this application is to help users mask their identity when surfing the web. The application uses a series of encryption algorithms that scrambles your messages every time you send a request (tap on a link to go to another web page). A picture of the application in development is given in the previous page. To try and fit the application to my own needs, I manipulated some of the source code to fit the intentions behind my topic. In doing so, I made the application fit the smaller picture of a the larger issue. You can see the application running in this picture down below. The application was written primarily in Java, since that is the language that android mostly uses.

****

Although it may not seem much from first glance, the EFF’s intention of potentially releasing the application is genuine because as per their knowledge, the application links to inequality both directly and indirectly because since we live in the Bay Area, the passageway of the EFFs message would only work to the extend of the number of people who own smart gadgets. This would link to economic inequality because there are groups who do not own smart gadgets such as iPhones, and simple laptops. Another downside to the strategy would be that as these solutions are largely embedded deeply in the world of the computer scientist, the average consumer would not know about what these protocols do and might discard the message and continue on using what he or she has been doing for the longest time. I focus on the downsides mostly because that is how the EFF gets down to business to try and convince their audience that their methods are partial solutions to the problem.

Overall, civilian surveillance by UAVs, otherwise known as Drones are still new and many Americans are divided on the issue. It has only been a couple of years since the military started using these kinds of drones in our own airspace conducting surveillance. In my previous paper I suggested that we could focus on the more domestic use such as delivery drones thanks to Amazon air, or for scientific research. The debate is still ongoing and I can only hope that this is not just another added instrument of paranoia put into place by the NSA to make us feel like we are being watched all the time. It does bring up the question though, with all the different methods of surveillance (not only limited to drones and other unmanned machines), is our society almost voluntarily headed towards the police state as depicted in George Orwell’s novel 1984?

# Works Cited

"ACLU-NJ Cheers Passage of Drone Privacy Bill in Assembly, Urges Senate to Follow Suit With a Yes Vote." 14 May 2015. *aclu.org.* American Civil Liberties Union. 24 October 20215. <https://www.aclu.org/news/aclu-nj-cheers-passage-drone-privacy-bill-assembly-urges-senate-follow-suit-yes-vote>.

Blitz, Marc Jonathan, et al. "Regulating Drones Under the First and Fourth Amendments." 5 March 2015. *ssm.com.* William & Mary Law Review, Forthcoming. Print. 26 October 2015. <http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2574378>.

Dorr, Les, and Alison Duquette. "FAA Fact Sheet – Unmanned Aerial Vehicle (UAV) UAV." FAA Fact Sheet – Unmanned Aerial Vehicle (UAV) UAV. Unmanned Aerial Vehicles, 14 Dec. 2012. Web. 10 May 2016. <http://www.hse-uav.com/faa\_fact\_sheet\_unmanned\_aircraft.htm>.

Farber, Hillary B. "EYES IN THE SKY & PRIVACY CONCERNS ON THE GROUND." *Scitech Lawyer* 11.4 (2015): 6-9. Print. 26 October 2015. <http://search.proquest.com/openview/9e65b2ffc3f7a94d1fd00e9e322ca316/1?pq-origsite=gscholar>.

Heatherly, Michael C. "Drones: The American Controversy." *Journal of Strategic Security* 7.4 (2014): 25-37. Print. 23 October 2015. <http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1387&context=jss>.

"Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft." n.d. *aclu.org.* American Civil Liberties Union. Web. 12 October 2015. <https://www.aclu.org/report/protecting-privacy-aerial-surveillance-recommendations-government-use-drone-aircraft?redirect=domesticdronesreport>.

RIC, Bartsch. "Unmanned and Uncontrolled: The Commingling Theory and the Legality of Unmanned Aircraft System Operations." *Aeronautics & Aerospace Engineering* 4.1 (2015). Print. 26 October 2015. <http://www.omicsgroup.org/journals/unmanned-and-uncontrolled-the-commingling-theory-and-the-legality-of-unmanned-aircraft-system-operations-2168-9792-1000140.pdf>.

Stanley, Jay. "Five Reasons Armed Domestic Drones Are a Terrible Idea." 27 August 2015. *aclu.org.* American Civil Liberties Union. 24 October 2015. <https://www.aclu.org/blog/free-future/five-reasons-armed-domestic-drones-are-terrible-idea>.

—. "The Coming Clash Over Drones." 10 September 2015. *aclu.org.* the American Civil Liberties Union. 25 October 2015. <https://www.aclu.org/blog/free-future/coming-clash-over-drones>.

—. "The Precarious State of the Private-Sector Drone Industry." 9 September 2015. *aclu.org.* American Civil Liberties Union. Web. 21 October 2015. <https://www.aclu.org/blog/free-future/precarious-state-private-sector-drone-industry>.

Wittes, Benjamin. "What Ben Franklin Really Said." What Ben Franklin Really Said. The Lawfare Institute, 15 July 2011. Web. 10 May 2016. <https://www.lawfareblog.com/what-ben-franklin-really-said>.

Zuckerman, Laura, and Thomson Reuters. "Idaho Restricts Use Of Drones By Police Amid Privacy Concerns." The Huffington Post. TheHuffingtonPost.com, 11 Apr. 2013. Web. 29 Apr. 2016. <http://www.huffingtonpost.com/2013/04/12/idaho-drones\_n\_3066045.html>.