Lashanti Gladney

Cyber Policy

For my analysis I will be focusing on the Cybersecurity Information Sharing Act as well as the Foreign Intelligence Surveillance Act, specifically on how they relate to the digital tracking of online consumers. While also discussing programs such as PRISM, XKeyscore, and the Five Eyes Alliance.

The Cybersecurity Information Sharing Act (CISA) allows for the sharing of data relating to cyber threats between companies and the government. The Foreign Intelligence Surveillance Act (FISA) was created to regulate foreign intelligence information. Both acts tie into one another as they are centered around the sharing of information. This also has contributed to what has made both controversial acts. Today I will be focusing on the policy implications of these acts, and why they have sparked controversy. I will also ensure to discuss how policy makers have addressed these concerns, and the ramifications associated with those decisions.

To begin the main issue civilians were found to have as it relates to CISA and FISA was the personal data being shared. The intention of these acts was to gather threat intelligence however, in this process some personal information about citizens could be included in the mix. This was mainly a concern with CISA, companies such as Microsoft, Google, Facebook, and many more are included among those who share threat information with the government. These companies hold personally identifiable information such as social security numbers, birthdays, demographics, as well as personal banking information and more. This is information many do not know or want to be shared with the government. FISA escalates these worries on a national level with the monitoring of citizens digital activities crossing the line between gathering information for intelligence and gathering everyday information.

The aforementioned promoted the need for provisions. Provisions were added to combat the issues associated with the amount of data collected one being the removal of personally identifiable information that isn't related to cyberthreats in the data sharing process. This also ties into another provision that restricts the type of information that companies are to share with the government. There are also annual reports to congress to monitor the effectiveness of the program as well as to continuously improve upon the act where needed. To address the privacy

concerns that arose with FISA other acts were brought forth for example the USA Freedom Act, that requires the government to request specific information about a target when it comes to collecting communication data. This aids in the mass collection of telephone data from all citizens in the name of security without just cause. There was also a section included giving companies the freedom to reveal when the government requests this information and how many times. There was also the FISA amendments Act of 2008 that requires intelligence agencies to obtain official court permission for communications information of civilians, similar to how a warrant works. These implementations were not without pushback however, as the government viewed the data they collected as being most valuable to counter cyberattacks and new provisions to restrict what data could be collected impeded their efforts.

The government had programs such as PRISM, XKeyscore, and the Five Eyes Alliance under CISA and FISA. The public being made aware of these programs specifically is what caused the most outrage about privacy concerns. PRISM was devised under section 702 of FISA which essentially allows the government to collect digital information from companies inside and out of the United States. XKeyscore allowed for the collection internet data including emails, search history, and more under the same section as PRISM. The information gathered from these two programs are then funneled into the Five Eyes Alliance which shares collected data of United States Citizens to other countries; The United Kingdom, Canada, Australia, and New Zealand are all among them. The reforms mentioned above impact these programs directly, although these countries are seen as being allies of the U.S the privacy concern of citizens still exists as the question of what these other countries will be doing with the data collected emerges.

Overall, there are various perspectives that arise when discussing CISA and FISA in terms of national security. On one hand there are privacy concerns from citizens about thew mass

collection and sharing of data. While on the other hand the government sees these concerns not being as concerning enough to want to get rid of their surveillance programs completely. To meet in the middle there have been added provisions to reassure citizens of their digital privacy and safety while also allowing for the government to stay vigilant.

Sources Cited

Council on Foreign Relations. "FISA's Current Controversies and Room for Improvement (Part Two)." *Council on Foreign Relations*, 2021, www.cfr.org/report/fisas-current-controversies-and-room-improvement-part-two.

Holt, Keith "Cybersecurity and Information Sharing: Legal challenges and solution" Harvard law review, Vol. 133 no. 5, 2020,

https://www.jstor.org/stable/10.5325/harvlarrev.133.5.1230.

Senate Report 114-32. "Cybersecurity Information Sharing Act of 2015." *U.S. Government Publishing Office*, 2015, www.gpo.gov/fdsys/pkg/CRPT-114srpt32/pdf/CRPT-114srpt32.pdf.

Zeng, Tong. "Reforming Section 702 of the Foreign Intelligence Surveillance Act for a Digital Landscape." *Harvard National Security Journal*, vol. 10, 2019, pp. 59-82. https://harvardnsj.org/2019/10/reforming-section-702-of-the-foreign-intelligence-surveillance-act-for-a-digital-landscape.