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 social factor is a huge reason for change when it comes to implementing or changing a policy. Before, during, and after a policy is implemented, there is social commentary from citizens. This commentary is typically about the policy itself; how does it benefit or harm us, is it the best decision for most citizens. There are often controversial laws that some petition to have removed or protest out against prompting change. There are infinite opportunities of events that can occur because of making policy decisions. This is why voting for candidates to represent your ideas if so essential. Today I will be explaining how social factors have affected the Cybersecurity Information Sharing Act (CISA) as well as the Foreign Intelligence Act.

The rise in technology brought forth a new need for security prompting various policies to be put in place such as FISA and CISA. FISA was implemented to allow foreign intelligence information and share this information to develop stronger cybersecurity. Since its implementation there have been a few different revisions. A prime example of social factors dictating change came after the 9/11 attack on the world trade center. This act caused fear in citizens who called for more protection against terrorist threats. Following this the Patriot Act was implemented and as well PRISM and XKeyscore. The Patriot Act essentially allowed for the expanding of surveillance that could be done to better detect and prevent terrorism. PRISM allowed for digital data to be collected by the NSA. XKeyscore allowed for more in depth digital information without a need for authorization. Another example of this would be the Edward Snowden's revelations that occurred in 2013. This revelation was in regard to the surveillance practices of programs like PRISM and XKeyscore. The public was outraged about the types of information being gathered without our knowledge. In response to this was the USA freedom Act. This new act amended parts of the Patriot Act and FISA to address privacy concerns. For example, section 215 of the Patriot Act which allowed bulk data collection from the NSA of

telephone metadata. Search warrants would now be needed to collect telephone metadata, which induces caller information, location, and proximity data of other devices. Citizens value their own [privacy especially when it comes to our telephone data. When citizens feel as though our privacy rights are being violated, we demand new action. The USA Freedom Act also led to the creation of experts to advise on privacy concerns and public reports on FISA surveillance.

CISA was created to open communication about cyber-attacks between the government and businesses. In 2014 a cyberattack on Sony Pictures exposed employee information, unreleased films, and private communications. The hesitation between Sony to communicate with the government delayed response time to this attack. By opening the communication between the government and business development strategies against cyberattacks. This however creates fiction with the public with the fear of the government collecting unnecessary personal information from companies. To address this fear the Automated Indicator Sharing system was developed to anonymize the information being shared. There was also a huge concern with transparency from the public prompting the Cyber Incident Reporting for Critical Infrastructure Act which influenced reporting. CISA is required to report cyber incidents within 72 hours, opening transparency.

All in all, the social impact citizens have on America is enormous. The publics outrage over privacy concerns being one of the biggest factors that affects policies such as CISA and FISA. However, fear is also seen to be the driving factor in change to these acts as well. An example I provided earlier were the creation of new acts after the 9/11 attack. These attacks caused thousands to lose their lives and has been labeled a major event in American history. It is no surprise this attack caused fear and panic among the citizens for security to be tightened to prevent such a drastic event from recurring. As seen there have also been acts created in response

to previous acts created meant to enhance security. There is a fine line between security and privacy one that constantly plays a game of tug-o-war when it comes to public opinion vs the government. While security is also essential the social impacts policies have on citizens play a large role in their success.

References

"Pros and Cons of the Cybersecurity Information Sharing Act of 2015." **ACE USA**, ACE USA, https://ace-usa.org/blog/research/research-technology/pros-and-cons-of-the-cybersecurity-information-sharing-act-of-2015/.

Maranzani, Barbara. "How Watergate Changed America's Intelligence Laws." **History**, A&E Television Networks, 16 Oct. 2018, https://www.history.com/news/how-watergate-changed-americas-intelligence-laws.

Woods, Michael, et al. "The Prospects of Cybersecurity Information Sharing Act (CISA): Lessons from the USA." **Cybersecurity**, vol. 9, no. 1, 2023, p. tyad003, https://academic.oup.com/cybersecurity/article/9/1/tyad003/7100879.

Goitein, Elizabeth. "A Surprising Senate Vote Signals New Hope for Surveillance Reform." **Brennan Center for Justice**, Brennan Center for Justice, 13 June 2023, https://www.brennancenter.org/our-work/analysis-opinion/surprising-senate-vote-signals-new-hope-surveillance-reform.

Lathrop, Ian. "Cybersecurity Information Sharing Act of 2015: Balancing Security and Privacy." **Hastings Law Journal**, vol. 13, 2020, https://hastingslawjournal.org/wp-content/uploads/I-Lathrop_13-TRANSMIT.pdf.

"Shared Responsibility: Public-Private Cooperation in Cybersecurity." **Center for Strategic and International Studies (CSIS)**, CSIS, https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity.