The 2018 Japanese Cybersecurity Policy contained details regarding an array of ethical issues created by rising technologies, governmental and private sector oversight, and data protection and privacy. It also led to considerations regarding the cost of implementing the changes this policy suggested. One policy Japan embraced with this new Cybersecurity Policy was a know as Public-Private Partnership, or PPP.

In essence, PPP is the cooperation of public sector critical infrastructure agencies, and elements of the Japanese government responsible for handling cybersecurity matters. This includes anything from analyzing current cybersecurity measures to exercises testing those measures, and the public sector's response to a simulated cyber-attack. While these PPP exercises have taken place since 2006, the 2018 Cybersecurity Policy mandated them as official government policy between the public and private sectors (Watanabe, 2019).

Two challenges posed against PPP was an issue regarding dependencies between critical infrastructure sectors, and increases in cyber incidents that occur after natural disasters. Using a report from 2007 as an example, they found that entities involved in finance, communication, and even governmental entities had huge dependencies on the energy sector. If a cyber incident or natural disaster impacted the country's electric grid or electric companies, it could have a cascading effect on those entities that remain dependent on it. This raised huge ethical concerns regarding sector interdependency and prior to the 2018 policy, PPP was continuously worked upon, and improved (Watanabe, 2019). Some saw this as government overbearing and intruding

into private sector affairs, but the potential security implications far outweighed any ethical concerns regarding government cooperation with private sectors.

Part of the new cybersecurity policy also impacted protections on personal information. The policy utilized the amended Act on the Protection of Personal Information (APPI), which was introduced in 2005, and amended in 2015. Referring to the amended APPI for guidance, it helped to further define "personal information" and control how entities handled transactions regarding personal information, as well as punishments for misuse of personal info, which has been a hotly debated ethical cyber issue worldwide (Shiraishi & Hirano, 2020). While more clearly defining what is considered personal information and forcing both businesses and agency to answer to the established Personal Information Protection Commission, it included some concerning exemptions, which were also included in the 2018 policy. Exemptions for broadcasting entities, writers, and universities were fine, as well as the loosely defined "political bodies", but allowing exemptions for "religious bodies" was a concerning inclusion. This also closed the door on non-university educational bodies being exempt from this rule (Inoue, 2018).

Personally, I think this the policy comprehensively covered ethics and rights of individuals, and entities well. It helps define what needs to be protected, works with and boosts the capabilities of entities that protect that information, and as stated in my last paper, promotes individual measures and education on cybersecurity (Cybersecurity Strategy Headquarters, 2018). It does all this without infringing on individual rights with regards to cybersecurity, at least on the surface. Of course, there is some concern with government agencies working with and having oversight into how private infrastructure entities promote their own security. Given how interdependent the private sectors of Japan are on one another, it's clear this extra cooperation between them and the government can be a positive force.

***Works Cited:***

Cybersecurity Strategy Headquarters (2018) Cybersecurity strategy—Japan, 27 July, 2018. https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf. Accessed 15 Feb 2021

Inoue, Y. (2018). Privacy and libraries in the case of Japan. IFLA Journal, 44(3), 223–228. https://doi.org/10.1177/0340035218785391

Shiraishi, K., & Hirano, M. (2020, February 24). *Cybersecurity in Japan*. Lexology. Retrieved March 21, 2023, from https://www.lexology.com/library/detail.aspx?g=5a1b0e44-9f84-432e-9bed-88523b2ebb6a

Watanabe, K. (2019). PPP (Public-Private Partnership)-Based Cyber Resilience Enhancement Efforts for National Critical Infrastructures Protection in Japan. In: Luiijf, E., Žutautaitė, I., Hämmerli, B. (eds) Critical Information Infrastructures Security. CRITIS 2018. Lecture Notes in Computer Science(), vol 11260. Springer, Cham. https://doi-org.proxy.lib.odu.edu/10.1007/978-3-030-05849-4_13