Almost every product manufactured today is expected to connect to the internet, “Today, 49% of the world’s population is connected online and an estimated 8.4 billion connected things are in use worldwide.” (Rainie, Anderson, 2017). These devices pose new risks to the average consumer as easy exploits in these systems can allow bad actors to infiltrate a home. In 2022 The European Commission proposed the Cyber Resilience Act to address decaying security among consumer tech. The act requires incident reports and automatic security updates for hardware and software that connect to a network. With an end goal of making the manufacturers take responsibility for the products. I chose this policy because it is a landmark in cyber defense as was reported at the time, “This will impact not only the European Union. This will change the rules of the game globally, one way or another. Because they will copy us or because they will not have the tools to abide by our rules. This is good not only for the level of cybersecurity but for the competitiveness of Europe,” (Bertuzzi, 2022).

Growing cyber threats pose a serious threat to the European Union since they are a coalition of different countries with their own laws. As these threats grow to the global supply chain there has been an effort to close gaps in the EU’s security. There are open gaps in the security infrastructure across the continent. Partly coming from the range of consumer products being purchased but then abandoned by their manufacturers which leaves them open to breaches. This jeopardizes everyday consumers and companies that rely on these products. Part of the Cyber Security Strategy for the Europe Union is to reduce risks to the supply chain and the goal of The Cyber Resilience Act is to establish a universal standard across the union and thus protect the supply chain. The global supply chain is a vast network and there is no

guarantee that all the companies are operating with the same security measures, so the Resilience Act is a step in securing the Strategy laid out by the EU. This new approach will make cyber security at the forefront of every new product, “Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.” (Regulation (EU) 2024/2847). This is a consolidated front against the dangers of poor cyber security measures,”The world’s attention on the fight and prevention of cybercrime has risen after annual figures shown almost 113 billion dollar worth of costs and has hit one million victims every day.8 It is therefore compulsory that people, and especially children, should become more aware of the possible threat they face when life has become digitalized in every aspect.” (2016). Increasingly poor safety measures have led to skyrocketing costs. On the micro level this policy will help protect European consumers by mandating clear and effective security updates for hardware or software owned by the consumer. To make sure that companies comply, a longer process of risk assessment before any product is released is also conducted. Consumer products will be split into two categories: Class 1 and Class 2. Class 1 will be products that the company can audit internally then submit to the ENISA for approval. Class 2 will need an independent auditor for compliance “The initial list of class 1 products includes internet browsers, network management tools and specialised controllers. Class 2 products would be deemed to have a higher cyber risk. The initial list includes operating systems, general purpose microprocessors, network modems and routers, encryption software and even smart meters.” (Horn, 2022). Once this process is complete the product will get a CE mark and be ready for shelves, “A digital product with a CE mark could be freely sold across the EU. National authorities

might require non-conforming products to be withdrawn from the market. Importers and distributors would require their suppliers to have obtained CE marking on digital products" (Horn, 2022). These regulations will not just apply to home grown products but anything sold in the EU, especially products that have access to private data. Imported goods from American tech giants would still have to submit proof of compliance with the act or hire an independent auditor.

The European Union made history with these sweeping regulations on technology. This is a broad scope policy that pays little attention to the will of big tech industrialists in favor of regulation for the safety of its people. The appeal of a policy like this is that it forces companies to take an active role in the health and longevity of their products. This stops companies from producing and then abandoning hardware or software that people still use or can still collect sensitive data. When viewed as a counterpoint to American cyber policy, the effort to make a solid baseline approach across so many countries is commendable.

REGULATION (EU) 2024/2847 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847#document1

Bertuzzi L. (2022). Commission expects to set the world's cybersecurity standards for connected devices. EURACTIV

Commission expects to set the world's cybersecurity standards for connected devices – EURACTIV.com

Rainie, L., & Anderson, J. (2017). The Internet of Things Connectivity Binge: What Are the Implications?: Despite wide concern about cyberattacks, outages and privacy violations, most experts believe the Internet of Things will continue to expand successfully the nextf ew years, tying machines to machines and linking people to valuable resources, services and opportunities. Pew Research Center.

http://www.jstor.org/stable/resrep76739

European Crime Prevention Network, Cybercrime: A theoretical overview of the growing digital threat, 2016.

theoretical_paper_cybercrime_.pdf