When a consumer purchases a device that connects to the internet, there can be the reasonable fear that this device could become compromised. Coupled with the fact that some companies abandon products in use, there can be a lot of danger to the consumer. When breach happens it can be hard to seek restitution for the average consumer, so when the Cyber Resilience Act was put into effect the idea was to protect these people on a standardized basis across all of the EU. Now, this was not purely a magnanimous gesture as economic and social cohesion being distributed by patchwork laws costs money,"If enacted, the CRA would allow, among other things, the banning of devices with digital elements that do not meet the requirements of the EU market. Given that the CRA may also apply to non-EU manufacturers' digital products once placed on the EU market, the CRA could have an impact on cybersecurity standards for such products beyond the EU borders. Indeed, non-EU operators might find it convenient to follow the CRA's rules as a default framework for their global operations instead of developing different products or processes for different markets." (Burri, Mira & Zihlmann, Zaira. 2023). The wide ranging effect of this policy is almost global as there are very few markets that do not engage with the European economic bloc. This almost preemptive control of the free market could be seen as oppressive to some laissez faire maximalists that argue that regulation reduce competition," ….. regulation of industry structure by a monopolistic authority that may reduce competition as centralized control of prices and profits may dampen the signals and incentives for would-be

challengers to enter markets. The experience of “antitrust” law, for example, suggests that rather than enhancing competition, regulation often acts as an impediment to it.” (Pennington M..2017). All calls for the sanctity of free market capitalism against this act would on its face be accepted as anti consumer bias, so most ethical considerations will,and should, always favor the consumer, with supply chain security being a positive after effect. Meaning that classical liberal market economics has little weight in discussion of ethics or the wellbeing of consumers. It is well documented that companies will traffic in the data of their users for profit, this makes it so the modern buyer cannot expect to have any right to privacy. To address these privacy concerns The Cyber Resilience Act carves out protections that ensure that devices that store data will have to be protected by the manufacturer, “Security requirements relate….., protecting data confidentiality, integrity, ……. and reporting vulnerabilities and incidents. Digital products should be secure “by design” and “by default” and vulnerabilities should be quickly detected and eliminated. Products should also have security updates installed automatically and separately from functionality updates throughout the product's lifecycle.” (M. Kikelj & I. Sabic, 2024). Extension of the protection over the life of the product will be a massive boon for the consumer as the expansion of the internet of things has made its way to many household products that are forgotten about. These protections set the standard for consumer protection goals world wide, with the U.S lagging far behind. There is a concern when it comes to smaller companies or open source software developers being met with

steep costs or legal battles from downstream use of their product, “Some commentators argue that these laws are the “death of open source.” According to this logic, there is no way for downstream providers to meet their compliance obligations under the CRA and the PLD, at least without satisfactory representations, warranties, and indemnifications from OSS providers. This regulatory uncertainty poses a challenge to the sustainability and growth of open-source initiatives.” (Liane Colonna, 2025). This concern was responded to with quick revisions to the policy but not all needs were met and uncertainty still looms. Ethical considerations are a major part of cyber security, but every policy is a balancing act to protect and not hurt consumers. This won't always be guaranteed on the first draft.

Burri, Mira and Zihlmann, Zaira, The EU Cyber Resilience Act – An Appraisal and Contextualization (February 17, 2023). Zeitschrift für Europarecht (EuZ), 2/2023, B1-B45, Available at SSRN: https://ssrn.com/abstract=4375552

Pennington M. ROBUST POLITICAL ECONOMY AND THE PRIORITY OF MARKETS. Social Philosophy and Policy. 2017;34(1):1-24. doi:10.1017/S0265052517000012

M. Kikelj and I. Sabic, "Strengthening the Digital Ecosystem: Effects of the Cyber Resilience Act (CRA) on Open-Source Software," 2024 IEEE International

Conference on Cyber Security and Resilience (CSR), London, United Kingdom, 2024, pp. 557-561, doi: 10.1109/CSR61664.2024.10679481.

keywords: {Technological innovation;Ecosystems;Collaboration;Europe;Security;Computer crime;Open source software;Cybersecurity;Cyber Resilience Act (CRA);Due diligence;European Union;Open-source software;security requirements},

Liane Colonna,

The end of open source? Regulating open source under the cyber resilience act and the new product liability directive,

Computer Law & Security Review,

Volume 56,

2025,

106105,

ISSN 2212-473X,

https://doi.org/10.1016/j.clsr.2024.106105.

(https://www.sciencedirect.com/science/article/pii/S0267364924001705)