THE CYBER RESILIENCE ACT - WHEN IS FREE AND OPEN SOFTWARE COMMERCIAL?

August Bournique

AUGUST BOURNIQUE

AMSTERDAM BASED CONSULTANT AND ATTORNEY

- California Licensed Attorney
- 11 Years of Litigation
- 4 Years of working with Tech non-profit and start up clients

DISCLAIMER: The presentation is general information and not legal advice about your specific situation

I am not your lawyer

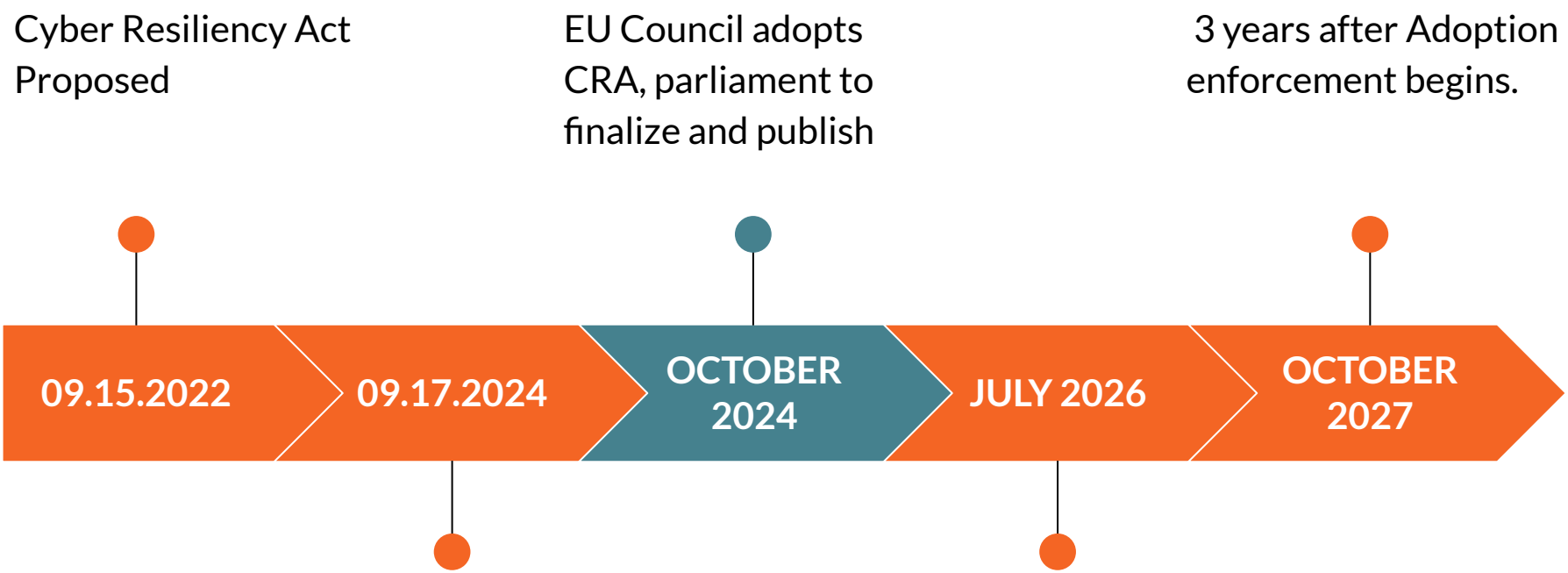
WHAT IS THE CYBER RESILIENCE ACT?

EU WIDE PRODUCT REGULATION (Regulation 2022/0272

- Products on the EU common market
- With a network component
- Few exceptions, most already regulated

STATED GOALS OF THE CRA

- Ensure manufacture of digital products that are private and secure throughout the product life cycle
- Transparency about product security to help consumers


Cyber Resiliency Act Proposed
EU Council adopts CRA, parliament to finalize and publish
3 years after Adoption enforcement begins.
09.15.2022
09.17.2024
OCTOBER 2024
JULY 2026
OCTOBER 2027
EU Council and Parliament “Approve” CRA
Reporting Requirement starts 21 months after Adoption

HOW WILL THE CRA REGULATE ?

REPORTING

- Manufacturer's must report breaches and exploited vulnerabilities
- Reporting to both ENISA & CSIRT - with follow up reports

STANDARDS & CERTIFICATION

- Technical documentation of compliance, update process, and end of life policy - all made public
- A "CE" mark. Products must be certified or self-assessed as meeting security and privacy standards throughout the product life cycle
- Scary fines & penalties

PROTECTIONS FOR FOSS

- “Non-Commercial” FOSS Excluded from CRA.
- Commercial FOSS only has to meet “General Product Standards”.

AND FOR FOSS?

OPEN SOURCE STEWARDS

- NGOs that work in an area or assist with a variety of projects. Linux Foundation EU, Apache Foundation etc.)
- Considered a “Manufacturer” by CRA (must report - with minimal liability)
- Work with regulators to write standards for FOSS products

SO WHAT'S FOSS?

(FOR THE CRA)

§ I - 18 - WHAT IS FREE AND OPEN SOFTWARE

“Free and open-source software is understood as software the source code of which is openly shared and the licensing of which provides for all rights to make it freely accessible, usable, modifiable and redistributable. Free and open-source software is developed, maintained and distributed openly, including via online platforms. In relation to economic operators that fall within the scope of this Regulation, only free and open-source software made available on the market, and therefore supplied for distribution or use in the course of a commercial activity, should fall within the scope of this Regulation…”

FREE AND OPEN SOURCE SOFTWARE UNDER THE CRA MUST:

- Share its source code openly, including on online platforms
- Offer a license where all rights are freely accessible, modifiable, usable and redistributable

THEN THE CRA DOESN’T APPLY TO FOSS UNLESS…

- It is distributed as part of commercial activity.

THE BIG QUESTION: WHAT'S "COMMERCIAL"?

§ I - 15 - WHAT IS COMMERCIAL

“[…] products […] supplied for distribution or use on the Union market in the course of a commercial activity [...defined…] by charging a price for a product […] by charging a price for technical support services [...beyond…] recuperation of actual costs, by an intention to monetise, by requiring [...] the processing of personal data for [sale] or by accepting donations exceeding the costs associated with the design, development and provision of a product. Accepting donations without the intention of making a profit should not be considered to be a commercial activity.

A COMMERCIAL FOSS PROJECT DOES ONE OR MORE OF THESE:

- Charges for the “Product”
- Charges more for “Technical Support” then it costs to provide
- Is intended to be “Moneised”
- Collects and sells user “Personal Data”
- Intends to profit from accepting Donations and succeeds

… WAIT THERE'S MORE

§ I - 18 - WHEN COMMERCIAL ISN'T COMMERCIAL

The mere circumstances under which the product [...] has been developed, or how the development has been financed, should therefore not be taken into account when determining the commercial [...] nature of that activity. [...F]or the purposes of this Regulation [...] to ensure that there is a clear distinction between the development and supply phases, the provision of products with digital elements qualifying as free and open-source software that are not monetised by their manufacturers should not be considered to be a commercial activity. [...] For instance, the mere fact that an open-source software product with digital elements receives financial support from manufacturers or that manufacturers contribute to the development of such a product should not in itself determine that the activity is of commercial nature.

WHAT DOES ALL THAT MEAN? NO ONE KNOWS YET, BUT…

- It appears that only the sale/monetisation of the final/complete product is commercial activity
- "Support" and "Contributions" from manufacturers for development is not commercial.
- Unless there's commercial intent
- §1 -17 notes that regulators need to "take into account the different development models" FOSS

… AND MORE

§ I - 18 - STILL MORE? THE FINAL BITS

In addition, the mere presence of regular releases should not in itself lead to the conclusion that a product with digital elements is supplied in the course of a commercial activity. Finally, for the purposes of this Regulation, the development of products with digital elements qualifying as free and open-source software by not-for-profit organisations should not be considered to be a commercial activity provided that the organisation is set up in such a way that ensures that all earnings after costs are used to achieve not-for-profit objectives. This Regulation does not apply to natural or legal persons who contribute with source code to products with digital elements qualifying as free and open-source software that are not under their responsibility.

SOME EXTRA PROTECTIONS

- Updates and new versions aren't themselves commercial activity -does this support "development phase" non-commerciality or work against it?
- Nonprofits can sell FOSS if earnings are used for charitable purpose
- Contributions of code to other's FOSS projects (even by companies) isn't regulated.

THE CRA IS A FOSS LOBBYING SUCCESS STORY

THE CRA USED TO BE TERRIFYING

- Originally FOSS “commercial” definition had no exceptions based on source of income (donation etc)

AN ONGOING PROCESS

- Open Source involvement in the CRA was not regular lobbying.
- Open Source Software Stewards are continuing the process of shaping the CRA by working with regulators.

WHAT SHOULD WE TAKE AWAY?

HARD LIMITATIONS

- Intention to monitise a product means the CRA applies
- Sales of final products mean the CRA applies
- Donations keep you outside the CRA

THE CRA COULD BE A WIN FOR FOSS

- Incorporated FOSS projects may feel pressure to be CRA compliant - this is an option to get paid
- The Steward model give a continued voice, how powerful will it be
- Might the CRA may end up as a model for other regulations of FOSS … NIS 2 even?

Resources

- CURRENT ACT
  https://data.consilium.europa.eu/doc/document/PE-100-2023-REV-1/en/pdf
- ENISA PAPER ON STANDARDS
  https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping
- MY WEBSITE
  https://bourniquelaw.com/