THE CYBER RESILIENCE ACT AND OPEN SOURCE PROJECTS

M. August Bournique

M. 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

THE CYBER RESILIENCE ACT

Regulation (EU) 2022/0272 (2024)

EU WIDE DIGITAL PRODUCTS AND CYBERSECURITY REGULATION

NIS 2 Framework (2023)
ENISA Standards (Draft 2024)
EU Product Liability Directive (2024)

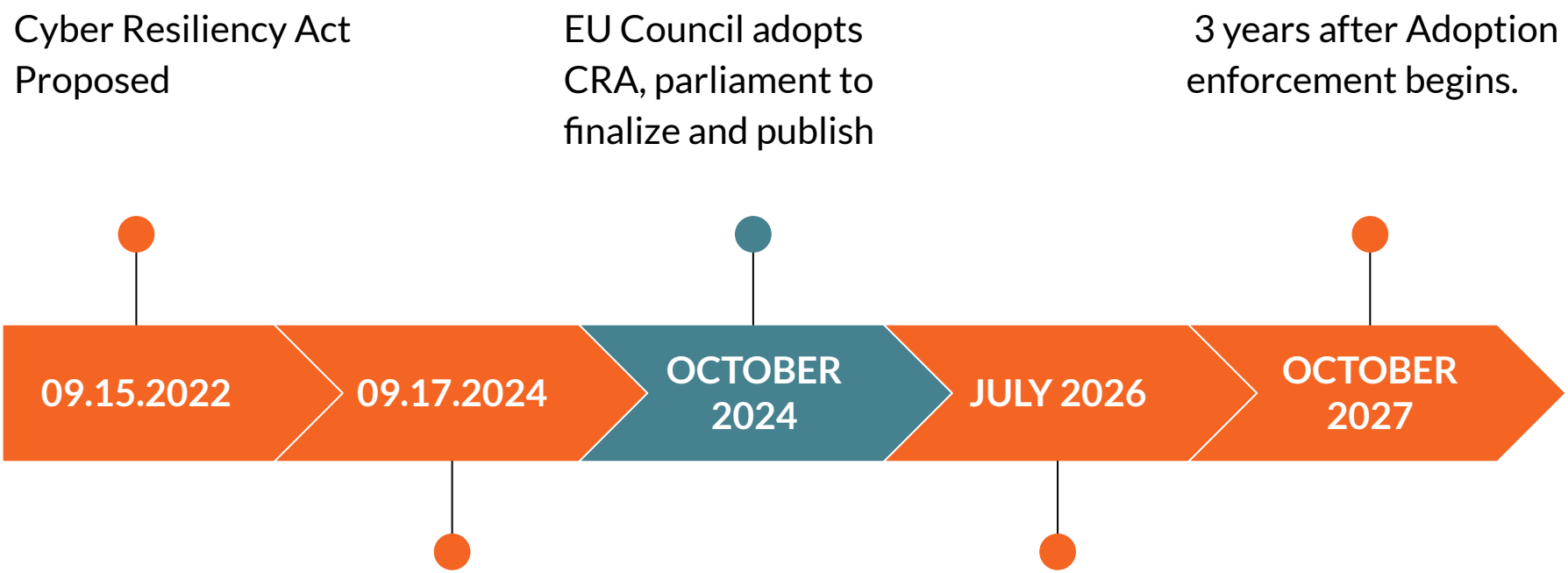
WHAT IS THE CRA?

EU WIDE PRODUCT REGULATION

- 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

Cyber Resiliency Act Proposed

EU Council adopts CRA, parliament to finalize and publish

3 years after Adoption enforcement begins.

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

THE REALITY OF THE CRA

UNSTATED GOALS

- Show public action on security & privacy
- Force large tech actors to consider privacy and security
- Without harming EU Manufacturing

ENFORCEMENT AND SCOPE

- Proposed scale of regulation is vast
- Primary regulator (ENISA) has around 100 employees
- CRA self-assessment/certification are self-regulation

WILL THE CRA APPLY TO MY OPEN SOURCE PROJECT?

FOSS UNDER THE CRA

DEFINITION OF FOSS

- Software that has publicly available code
- Offered under open license

PROTECTION A: IS MY PROJECT A PRODUCT?

FOR THE CRA A PRODUCT IS:

- Is software or a physical good
- With a networking component

FOR THE CRA A PRODUCT IS NOT:

- Contributing to another's FOSS project
- A service, including software as a service (that may face other regulation)
- Hosting a code repository
- A ISP or IXP
- An individual or company

PROTECTION B: IS MY PRODUCT COMMERCIAL?

CRA ONLY APPLIES TO "COMMERCIAL" FREE AND OPEN SOFTWARE

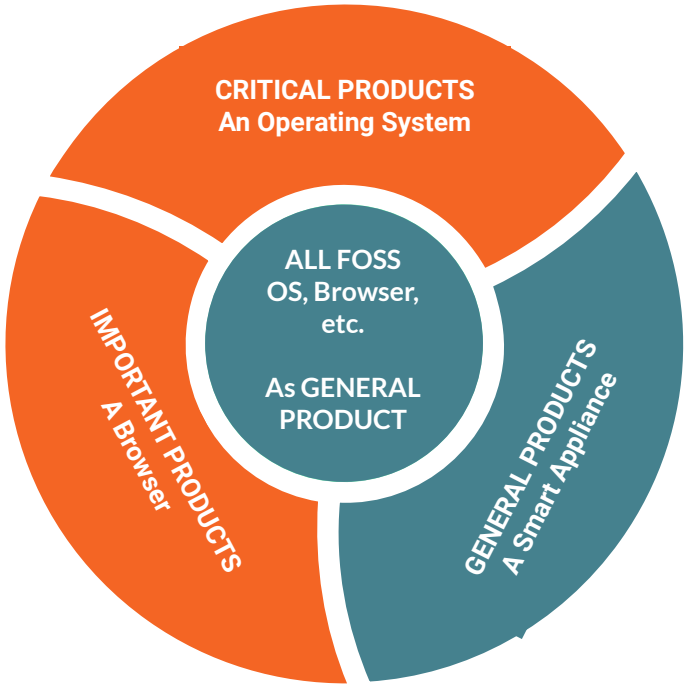
A COMMERCIAL FOSS PROJECT:

- We still don't know exactly what it is … but …
- It's directly monetized
- More than receiving donations
- More than a contract or two for specific features or maintenance

WHAT IF SOMEONE USES MY PROJECT COMMERCIALLY?

COMBINED FOSS & COMMERCIAL PRODUCTS

- The CRA doesn't apply to FOSS included in another commercial product
- Manufacturer of product including FOSS elements must do due diligence
- Unless the FOSS developer had "Commercial Intent"



WHAT IF MY PROJECT IS COMMERCIAL?

- Commercial FOSS projects only have to meet the standard for a “General Product” (Self Assessment) regardless of purpose.
- You can afford a lawyer

OTHER PROTECTIONS:

YOU'RE JUST A LIL' GUY

- Small, Medium and Micro Enterprises (less than 250 persons/€50M turnover (per 2003/361/EC) have lower requirements and fines.

OPEN SOURCE SOFTWARE STEWARDS

- NGOs that assist FOSS projects.
- May work with regulators to produce domain specific standards
- Subject to lesser sanctions for mistakes in reporting etc.

THE TEXT vs. REALITY

WHAT TECH PEOPLE MISS ABOUT LAW

- Legal Code is not the same as “Code”
- Enforcement and understanding of law is constantly evolving
- At scale law almost always avoids absurd results

QUESTIONS FOR A RISK-BASED APPROACH TO THE CRA

- Are OS projects the CRA’s regulatory target?
- What can an one due to avoid being subject to regulatory scrutiny?
- What is the record of enforcement for similar regulations?

A RISK ASSESSMENT

THE OS DEVELOPER & THE CRA

Gets some corporate donations.
Has a support contract or two

Relax! Only be concerned if:

- Your project is making money
- Your project is collecting private data
- Your project is a tempting target

Still worried…

- Review your income, costs, security and privacy policies.
- Start documenting security efforts
- Watch for Regulator and Steward actions
- Review your reporting process

Resources

WHAT TECH PEOPLE MISS ABOUT LAW

- CURRENT ACT
  https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html

- ENISA PAPER ON STANDARDS
  https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping

- MY WEBSITE
  https://bourniquelaw.com/