European Cyber Resilience Act: Why Universities Should Care

Anne-Marie Scott, Board Chair

DINI Conference, October 2023

Apereo Foundation

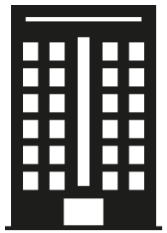
- Formed 2012 (date back to 1999)
- Non-Profit (New Jersey 501 c.3)
- Global Membership Organisation
- Elected Board of Directors
- Partnerships
  - ESUP-Portail (France)
  - LAMP (USA)
  - AXIES (Japan)

Mission

"…**collaborate** to foster, develop, and sustain open technologies and innovation to support learning, teaching, and research."

apereo Foundation

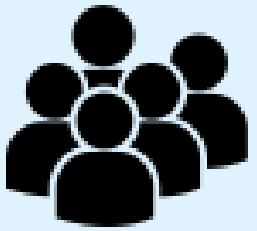
Educational Institutions



Commercial Affiliates

Apereo Foundation

Shared Services

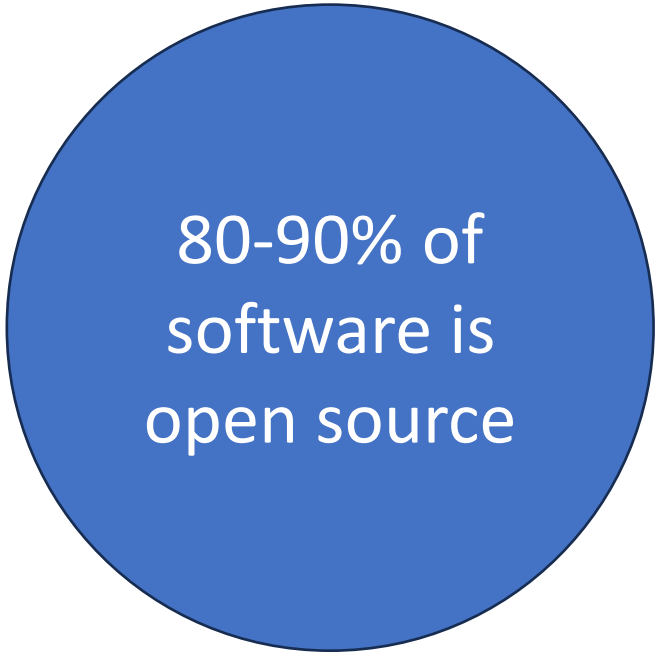


Software Communities

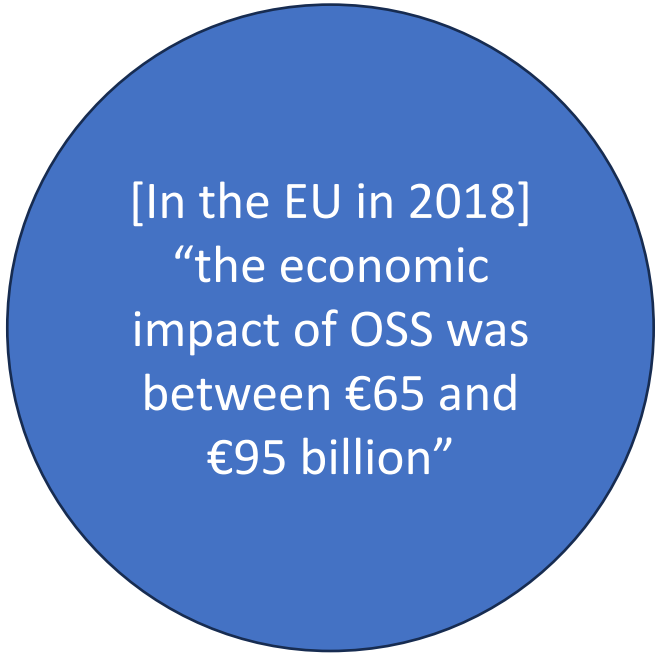
Projects

apereo Foundation

Open source: Cooperation for economic benefit



(Forrester Research)



(European Commission)

Background to the CRA

The European Commission has proposed a new legislation intended to improve the state of cybersecurity for software and hardware products made available in Europe.

- Draft legislation is now in the political process in the EU Parliament and Council

The initial draft of the **Cyber Resilience Act** (“CRA”) would:

- Improve the security of all products with digital elements made available in Europe
- Require that all manufacturers take security into account across both their development processes and the lifecycle of their products once in the hands of consumers
- Require that manufacturers apply the CE Mark to their products to indicate conformance to the requirements of the CRA

Additional Details

- Applies to all software whether embedded in cyber-physical systems, packaged software, or SaaS
- Process requirements:
  - Mandates the use of SBOMs, security patches, user ‘call home’ functionality
  - Requires support of products for no less than 5 years
  - Restricts publication of unfinished software for testing purposes
  - Imposes process and documentation requirements on a per-release basis
- CE Mark requirements:
  - Three tiers of product types, with increasing compliance obligations for ‘critical’ and ‘highly critical’ products
    - Critical and Highly Critical systems must use external audits for release certification

Who does it affect?

Anyone making software available (*downloadable*) on the extended single market:

- Developers
- Providers of software
- Providers of digital services
- Online marketplaces & repositories

Cyber Resilience Act and Open Source

Recital 10

In order not to hamper innovation or research, free and open-source software ***developed or supplied outside the course of a commercial activity*** *should not be covered by this Regulation.*

“Commercial Activity” Definition (Blue Guide)

Regularity

- Is there a regularity of supply? I.e. does your project release on a regular, repeated cadence?

Characteristics

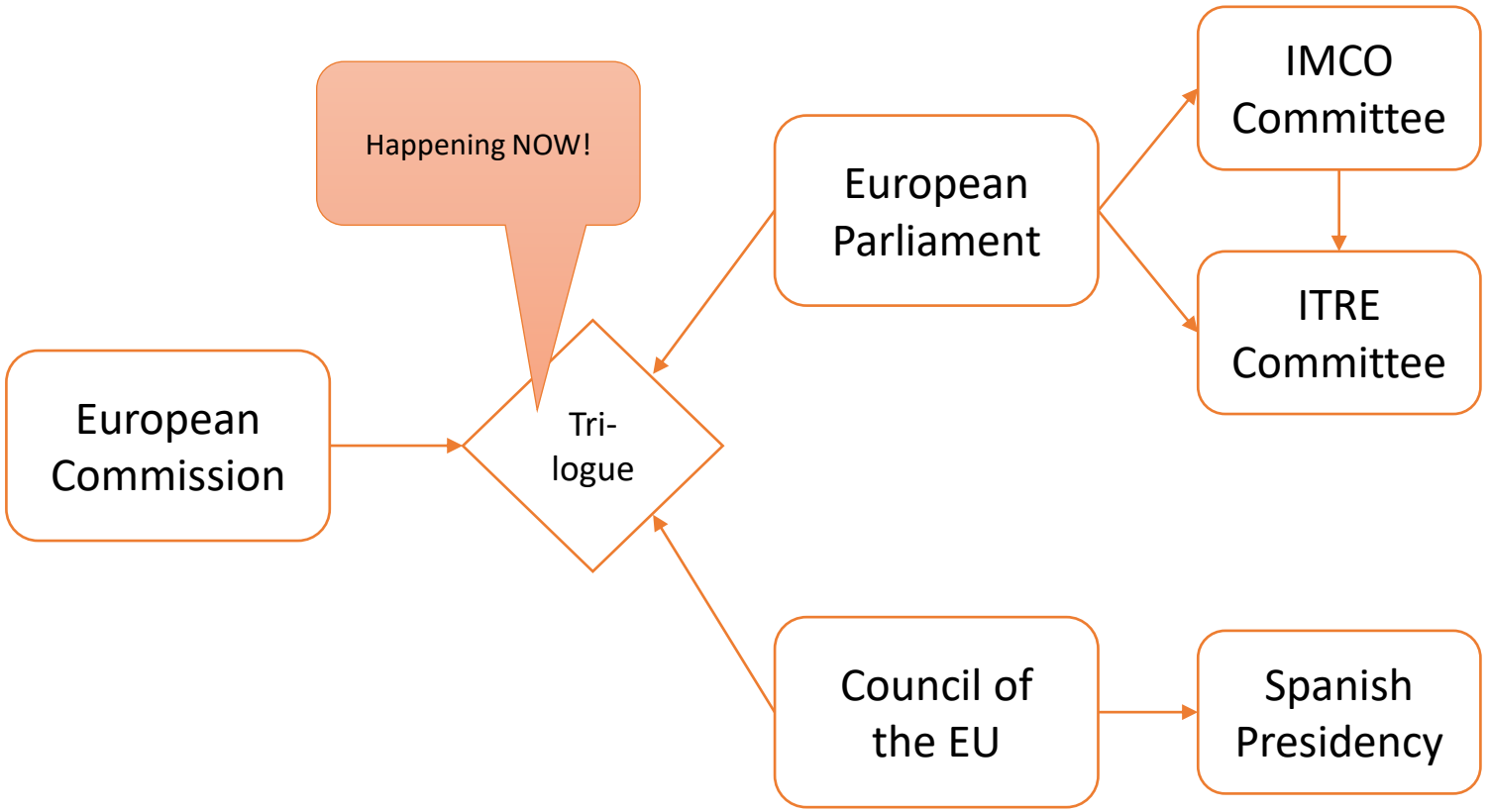
- Is your open source project of commercial quality?

Intentions

- Do you intend for your open source project to be used in a commercial setting?

In reality, this exclusion will only support hobbyists and charities

Legislative Process



CRA: Current Status

- European Parliament ITRE (lead) and IMCO committees have drafted amendments
- The IMCO amendments seem positive for open source
- The discussions and drafted amendments of ITRE are very worrisome
- Commission remains adamant that open source must be regulated consistently as per the New Legislative Framework and Blue Guide, so outcome of trilogue is worrisome

apereo Foundation

CRA: Current Status

The ITRE Committee has reached the firm conclusion: **most open source projects and all open source foundations should be responsible for CE Mark conformance**.

- This is intentional.
- This is not a misunderstanding.

Rationale:

- Expensive for European SMEs to implement the CRA
- Reduce the financial burden on the EU economy by putting OSS projects, OSS Foundations in charge of conformance
  - Assumes that CE Mark conformance is transitive

apereo Foundation

ITRE Draft: Problem 1

Any open source project which has committers who are employed by a commercial entity will be deemed to be a commercial activity

Why is this a problem?

- This would encompass virtually every meaningful open source project on the planet
- Set perverse incentives for struggling projects to reject people or contributions from the companies that use their software
- Companies may ban their employees from participating in or contributing to open source projects

ITRE Draft: Problem 2

Any project which accepts recurring donations from commercial entities will be deemed to be commercial

Why is this a problem?

- Open source sustainability is a serious problem
- Projects will be incented to decline donations that could have otherwise been used to support their work

ITRE Draft: Problem 3

Publication of intermediate builds, milestones, etc. must be restricted to a particular geographical area, limited in time, and with use restricted to testing only.

Why is this a problem?

- The publication of integration builds under open source licenses has been considered best practice for over 30 years.
- These are often made available indefinitely for regression testing purposes
- This will essentially make open source development best practices prohibited

ITRE Draft: Problem 4

All exploited vulnerabilities must be reported to ENISA within hours, regardless if a fix is available

Why is this a problem?

- Breaks accepted best practices for coordinated vulnerability disclosure
- For unpatched vulnerabilities, runs counter to best practices to limit disclosures to only those able to contribute to the fix
- Creating a central repository of unpatched vulnerabilities will not make software more secure
- Creates a terrible precedent for other governments to follow

Impact Analysis

In order to comply, projects, communities, and foundations will have to:

- Develop, document, and implement policies and procedures for every project, incl. all of the following:
  - development and post-release security requirements set forth in Annex I, including providing notification and update mechanisms.
  - user documentation requirements set forth in Annex II
  - product technical documentation set forth in Annex V
  - determine whether third party libraries used by each project are CRA compliant

- For each project release, prepare the project-specific documentation required by Annex V
- Determine for each project whether it meets the definition of ‘product with digital elements’, ‘critical product with digital elements’, or ‘highly critical product with digital elements’.
- For each single project release, document that the relevant CE mark process is followed...

Impact Analysis

Core objective of the proposed legislation is to extend the CE Mark regime to all products with digital elements sold in Europe, coupled with revisions to Product Liability Directive to extend to software products.

Assumption:

- Process will be applied to OSS made available under OS licenses and provided free of charge, ostensibly under licenses which **disclaim any liability or warranty**.

Concern:

- CRA could fundamentally alter the social contract which underpins the entire open source ecosystem: open source software provided for free, for any purpose, which can be modified and further distributed for free, but without warranty or liability to the authors, contributors, or open source distributors.

Potential Consequences

Non-European producers of open source code don't permit its use in Europe

- A reasonable and rational response not to accept statutory responsibility obligations for something you **make available for free.**
- Severing the EU's access to open source would cripple its innovation economy

Commercial intermediaries charge for "compliant" code

- Commercial third parties make non-EU open source code available in ways that adhere to the CRA, **at a cost.** Europe pays for what the rest of the world gets for free.

European producers of open source will be at disadvantage relative to their international peers

- Since they cannot avoid the responsibility obligations, they will be forced to accept them as part of their operations.
- For some projects, it would probably be simpler to just terminate the project and pull its source code off of the internet.

Potential Consequences

None of the package distribution sites are in a position to accept responsibility for the packages they make available

- Popular package repository sites restrict access from the EU

Force European businesses to stop contributing to open source projects

- At the moment, it is generally understood that **the risk** that contributions to open source may incur responsibility to the company **is low**.
- **The CRA changes that equation** and as a result European companies may curtail their open source collaborations
- Extremely damaging to the innovation economy in Europe
- Runs counter to numerous European-wide strategies e.g. digital sovereignty, Industrie 4.0 etc

Potential Consequences for Universities

- **The software you rely upon is no longer available**
  - Non-EU open source software projects exclude the EU from use
  - Some projects are removed from the web entirely to avoid unsustainable compliance costs.
  - Alternative solutions will need to be sourced / built and migration costs incurred.
- **Costs increase**
  - Institutional fees for commercial software products that include open source software increases to cover required re-factoring in response to the CRA

Potential Consequences for Universities

- **Collaboration becomes more complex and difficult**
  - Disincentivises collaborating with commercial partners e.g. industrial partners in research projects
  - EU / non-EU university collaborations, where different software components are available in different jurisdictions.
- **Open research becomes harder**
  - Developing software for research purposes is harder because some open source packages are no longer available within the EU.
  - Potential compliance costs for releasing open source software as a research output make it harder to support open science and scholarship.

Potential Consequences for Universities

- **Academic curriculum is affected**
  - Code bases, software development tools, and data analysis technologies that you rely on for learning and teaching activities become inaccessible or are removed from the web.
  - Academic curriculum will need to be redeveloped.
  - Potentially narrowing effect on curriculum in key areas such as computer science, AI, digital humanities etc?

Potential Consequences for Universities

- “Public sector” exemptions may provide some exclusion for software published as an output of a research project, or software built and used within educational institutions.
  - How this works when industry / non-EU partners are involved is unclear
- **It will not exempt open source projects that you likely rely upon**
  - WordPress / Drupal / Jupyter
  - Dspace / OJS
  - PhP / Python
  - Docker / Kubernetes
  - MariaDB / Mongo / Postgres

What to do?

- Consult your legal experts!
- Quantify the potential impact on you
  - Many open source organisations have published open letters
- Speak to appropriate political bodies to represent your concerns

apereo Foundation

Useful References

- Cyber Resilience Act (Wikipedia)
- The CRA should support open practices of open source and the development of European Open source to the advantage of small and medium size entreprises (SMEs) (Eclipse Foundation)
- Will the Cyber Resilience Act help the European ICT sector compete? (Linux Foundation)
- The European Cyber Resilience Act (more technical article from a member of the security team at Eclipse)

The Big Picture

We are seeing the start of the regulation of the software.

This is a good thing, but it is new, and the process is imperfect.

Future Collaboration Challenge

- Universities may not be well understood as “digital businesses” by regulators
  - How will you represent yourselves to regulators?
  - How will you make it easy for regulators to consult with you?
  - How will you make it easier to evaluate the impact of regulatory change on individual institutions, and on the sector?

"The Open Policy Alliance is designed to bring non-profit organizations together to participate in educating and informing US public policy decisions related to Open Source software, content, research, and education.

Responding to increased demand for public dialog and thoughtful stakeholder engagement in these adjacent and related "open domains."

apereo Foundation

Questions?

- https://apereo.org
- Anne-marie.scott@apereo.org