The EU regulating (open source) software

the proposed Cyber Resilience Act and Product Liability Directive

Benno Overeinder, Bastiaan Goslings and Robert Carolina

European Commission intends to regulate *products with digital elements* (≈ all hardware & software)

Slide image source: CONNECT University, CC BY 4.0
CE marking
TL;DR: this affects FOSS too

1. What?
2. How?
3. Now what?
Scope

Products with digital elements:

- **Hardware products** and components placed on the market separately, such as laptops, smart appliances, mobile phones, network equipment or CPUs

- **Software products** and components placed on the market separately, such as operating systems, word processing, games or mobile apps

1. The definition of “products with digital elements” also includes *remote data processing solutions*.

Not covered:

- Non-commercial projects, including *open source* in so far as a project is not part of a commercial activity

- Services, in particular cloud/Software-as-a-Service – *covered by NIS2*

Outright exclusions:

- Certain products sufficiently regulated on cybersecurity (cars, medical devices, *in vitro*, certified aeronautical equipment) under the new and old approach

Slide image source: CONNECT University, CC BY 4.0
Obligations of manufacturers

Assessment of the risks associated with a product

- (1) Product-related essential requirements (Annex I, Section 1)
- (2) Vulnerability handling essential requirements (Annex 1, Section 2)
- (3) Technical file, including information and instructions for use (Annex II + V)

Conformity assessment, CE marking, EU Declaration of Conformity (Annex IV)

Continued compliance with vulnerability handling essential requirements throughout the product life time (Annex I, Section 2)

Design and development phase

Maintenance phase
(5 years or across product lifetime, whichever is shorter)

Obligation to report to ENISA within 24 hours:
- (1) exploited vulnerabilities
- (2) incidents having an impact on the security of the product

Reporting obligations to continue

Slide image source: CONNECT University, CC BY 4.0
Which conformity assessment to follow?

<table>
<thead>
<tr>
<th>90% of products</th>
<th>10% of products</th>
<th>Highly critical</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default category</strong></td>
<td><strong>Critical “Class I”</strong></td>
<td><strong>Critical “Class II”</strong></td>
</tr>
<tr>
<td>Self-assessment</td>
<td>Application of a standard or third party assessment</td>
<td>Third party assessment</td>
</tr>
<tr>
<td>Criteria: n/a</td>
<td>Criteria: • Functionality (e.g. critical software) • Intended use (e.g. industrial control) • Other criteria (e.g. extent of impact)</td>
<td>Additional criteria: • Used by NIS2 entities • Resilience of supply chain</td>
</tr>
</tbody>
</table>

**Examples:**
- Photo editing, word processing, smart speakers, hard drives, games etc.
- Examples (Annex III): Password managers, network interfaces, firewalls, microcontrollers etc.
- Examples (Annex III): Operating systems, industrial firewalls, CPUs, secure elements etc.
- Examples: n/a (empowerment to future-proof the CRA)

To be amended/specified via delegated acts.
New Legislative Framework

- Manufacturers, authorised representatives, distributors and importers
- Notified bodies
- Notifying authorities
- National accreditation bodies
- Market surveillance authorities

Third party assessment

- "Lift Institute" (e.g. NL: RDI?)
- "TÜV"
- "DEKRA"
- (your favorite here)
Tentative timeline

- **2022**
  - Proposal (15 Sept. 2022)

- **2023**
  - EP elections (May 2024)
  - Standardisation request
  - Application of Art. 11 (EIF + 12 months)
  - DA specifying Annex III definitions (EIF + 12 months)

- **2024**
  - Application of all other provisions (EIF + 24 months)
  - Evaluation report (EIF + 36 months)

- **After entry into force (“EIF”)**
  - ENISA report on cybersecurity risks (Art. 11 + 24 months)
  - Publication of harmonised standards

---

Slide image source: CONNECT University, CC BY 4.0
A simplified example of smartphones (hardware)

As a rule, whoever places on the market a “final” product or a component is required to comply with the essential requirements, undergo conformity assessment and affix the CE marking.

Developed by the manufacturer placing the smartphone on the market:

Developed by upstream manufacturers for integration into the “final” product:

Placed on the market separately for users to buy and integrate:

Copyright: turbodesign / PIXTA

Slide image source: CONNECT University, CC BY 4.0
A simplified example of smartphones

As a rule, whoever places on the market a “final” product or a component is required to comply with the essential requirements, undergo conformity assessment and affix the CE marking.

Developed by the manufacturer

Developed by upstream manufacturers for integration into the “final” product:

Placed on the market separately for users to buy and integrate:

source: LWN.net: Development statistics for 6.3

(Parodied) slide image source: CONNECT University, CC BY 4.0
TL;DR: this affects FOSS too

1. What?
2. How?
3. Now what?
“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. [..]”

- recital 10

FOSS out of scope?
“Commercial activity”? 

“[..] a commercial activity might be characterized not only 
1. by charging a price for a product, but also 
2. by charging a price for technical support services, 
3. by providing a software platform through which the manufacturer monetises other services, or 
4. by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software.”

- recital 10
Risks arising from the proposal’s chosen open source exception

Expansive interpretation of “commercial activity” leads to narrow scope of exemption

- Disincentive to professionalise development and curation
- Incentive to move away from open source non-profit model
- Harming product diversity and reducing innovation
The Blue Guide guidance on the NLF from 2022 did not actually consider standalone software as a product.

See: 2022/C 247/01 The ‘Blue Guide’ guidance on the implementation of EU product rules
Further reading

• Content of today’s presentation was sourced from the joint response with ISC, CZ.NIC and NetDEF

broader FOSS perspectives on the CRA:
• Responses by Open Source Initiative, Open Forum Europe
• many others! See “the ultimate list of reactions to the CRA” by Simon Phipps

on the limitations of “supply chain”-thinking:
• “I am not a supplier” by Thomas Depierre

on the lack of standards and audit capacity required:
• “The EU's new Cyber Resilience Act is about to tell us how to code” by Bert Hubert
TL;DR: this affects FOSS too

1. What?
2. How?
3. Now what?
The EU Cyber Resilience Act

Feedback provided by the RIPE NCC
Good intentions?

• Improve cybersecurity in the EU
• Harmonisation and legal clarity for manufactures when placing products on the EU market
• Risk-based approach
• Security-by-design principle
• Clear information for users
Feedback requested by EC

• RIPE NCC submitted a response on 23 January 2023:
  - What does this mean, in terms of scope, definitions, necessity & proportionality?
  - How does it affect RIPE NCC services and infrastructure?
  - What are the concerns within the RIPE community at large?

https://t.ly/upBl
As the Regional Internet Registry for Europe, the Middle East and parts of Central Asia, the RIPE NCC welcomes the opportunity to give feedback on the European Commission's proposed Cyber Resilience Act. In the attached document, we explain how we foresee the Cyber Resilience Act impacting the RIPE NCC's own operations and services, and areas in which we believe further clarity is needed. In addition, we include viewpoints from the wider RIPE community, which is made up of technical operators, open-source developers and others responsible for maintaining much of the Internet's technical infrastructure within Europe and beyond.
Community concerns

- Welcome the exemption for open source software in recital 10, however it is too limited
  - Only when “developed or supplied outside the course of a commercial activity”
  - Terminology of the New Legislative Framework does not fit the way open source software is developed and published (‘manufacturer’, ‘placing on the market’)
  - Potential impact of compliance costs for small entities, individual developers - will harm innovation within the EU
  - Emphasis should be put on usage of the product, not on the type of license
‘For the CRA to reach the goal of reducing product vulnerability, it also needs to reduce vulnerability in open-source software – an aim the RIPE NCC strongly supports. The lack of clarity surrounding the notion of “commercial activity” referred to in Recital 10 however, is what creates uncertainty for, and risks placing undue regulatory burden on, those from the community who contribute to open-source software and its security without the intent of making a profit as a result of its later use.’

Now: discussion in council, parliament
Current status

- Council compromise text for OSS in recital 10 reached - improved text

- European Parliament
  - ITRE (Industry Research Energy) lead committee; draft report strengthens exclusion of OSS for non-commercial purposes
  - ITRE technical meetings to discuss proposed amendments currently ongoing
  - Reach out to MEP’s to state concerns
Questions

bgoslings@ripe.net
This Regulation applies only to products with digital elements made available on the market, hence supplied for distribution or use on the Union market in the course of a commercial activity. The supply in the course of a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services when this does not serve only the recuperation of actual costs or pursues a profit or the intention to monetise, by providing a software platform through which the manufacturer monetises other services, or by requiring as a condition for use, the processing of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software. The circumstances under which the product has been developed, or how the development has been financed should not be taken into account when determining the commercial or non-commercial nature of that activity. Taking account of the above-mentioned elements determining the commercial nature of an activity, only free and open-source software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable, supplied in the course of a commercial activity and therefore placed on the market should be covered by this Regulation. For the same considerations, products provided by public administration
Amendment 8
Proposal for a regulation
Recital 10

Text proposed by the Commission

(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. This is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable. In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software.

Amendment

(10) In order not to hamper innovation or research, only free and open-source software supplied in the course of a commercial activity should be covered by this Regulation. In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software. Where free and open-source software has been developed or supplied outside the course of a commercial activity, manufacturers that incorporate such software in their products with digital elements should take all the necessary steps to ensure the compliance with this Regulation.
Last week: FOSS related amendments in ITRE

Slide image source: European Parliament
Last week: FOSS related amendments in IMCO
The proposed Product Liability Directive (PLD)

What would it do?

Robert Carolina, General Counsel
Internet Systems Consortium
RIPE86, Rotterdam, 22-25 May 2023
Robert Carolina

- Lawyer (England & US)
  - General Counsel, ISC (2020- )
  - Author, CyBOK Law & Regulation (www.cybok.org)
  - Practitioner, law & regulation of ICT; law & ethics in cyber security
- BA (Dayton, 1988)
  - Juris Doctor (Georgetown, 1991)
  - LL.M (London School of Economics, 1993)

- Royal Holloway University of London
  - Senior Fellow, Law & Regulation module leader, Information Security Group, (1999- )
Hypothetical: 7 persons, 2 pieces of software, 1 car, 1 victim, all fictitious
Hypothetical – the story

- Firefly Ltd (Freedonia) develops and supplies "OpenSesame" cryptographic authentication software package.
- Einstein Motors Inc (California) adopts BravoDrive as fly-by-wire solution in automobiles they manufacture.
- Exotic Imports Ltd (Ireland) imports Einstein Sedans from California

- Jim Johnson (Ireland) purchases an Einstein Sedan from Exotic Imports.
- Denis Dastardly (Ruritania) exploits a flaw in OpenSesame. He remotely hacks Johnson’s sedan and accidentally commands the car (in Ireland) to swerve & crash into Victor Victim.
- Victor Victim suffers life-altering injuries.
- Dastardly has no money. He dies in a paragliding accident.
Hypothetical – the supply chain

California

Einstein Motors Inc
- Manufactures Car incorporating BravoDrive

Exotic Imports Ltd
- Imports and Sells Car

Bravo Bits Ltd
- Writes BravoDrive (software) including OpenSesame

Firefly Ltd
- Writes OpenSesame (software)

England

Johnson
- Purchases Car

Ireland

Victim
- Hit by Car when hacked by Dastardly - No commercial relationship

Freedonia

Ruritania

Dastardly
- Hacker - No commercial relationship - No assets - Died in paragliding accident
Hypothetical – the forensic export report

- The vulnerability
  - OpenSesame source code included a subtle coding error – a single misplaced semi-colon. This created a vulnerability in the (otherwise standard) cryptographic authentication protocol.

- Firefly normally has a strong reputation for secure coding, but this Q/A programme was poorly managed.

- Dastardly discovered the weakness independently. This was a zero day exploit.
## Legal analysis: the law today

If Victim brings a lawsuit in Ireland against...

<table>
<thead>
<tr>
<th>If Victim brings a lawsuit in Ireland against...</th>
<th>Negligence (common law)</th>
<th>Strict Liability Defective Product (EU 85/374)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Duty of care to victim (foreseeable, proximity)</td>
<td>Acted unreasonably (negligently)</td>
</tr>
<tr>
<td>Johnson</td>
<td>YES</td>
<td>No</td>
</tr>
<tr>
<td>Exotic Imports</td>
<td>YES</td>
<td>No</td>
</tr>
<tr>
<td>Einstein Motors</td>
<td>YES</td>
<td>No</td>
</tr>
<tr>
<td>Bravo Bits</td>
<td>Probably yes</td>
<td>Probably no</td>
</tr>
<tr>
<td>Firefly</td>
<td>Maybe?</td>
<td>Maybe??</td>
</tr>
<tr>
<td>Dastardly</td>
<td>Who cares? He has no money! If any other person found liable, they could be jointly &amp; severally liable for up to 100% of Victim’s damages.</td>
<td></td>
</tr>
</tbody>
</table>
### Legal analysis: the law today

<table>
<thead>
<tr>
<th>If Victim brings a lawsuit in Ireland against...</th>
<th>Negligence (common law)</th>
<th>Strict Liability Defective Product (EU 85/374)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Duty of care to victim (foreseeable, proximity)</td>
<td>Supply of product</td>
</tr>
<tr>
<td></td>
<td>Acted unreasonably (negligently)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Liable</td>
<td></td>
</tr>
<tr>
<td>Johnson</td>
<td>YES</td>
<td>n/a</td>
</tr>
<tr>
<td>Exotic Imports</td>
<td>YES</td>
<td>n/a</td>
</tr>
<tr>
<td>Einstein Motors</td>
<td>YES</td>
<td>n/a</td>
</tr>
<tr>
<td>Bravo Bits</td>
<td>Probably yes</td>
<td>Probably no</td>
</tr>
<tr>
<td>Firefly</td>
<td>Maybe?</td>
<td>Maybe??</td>
</tr>
</tbody>
</table>

Law of strict liability for defective products makes manufacturers and component suppliers financially responsible for dangerous products they supply that hurt people – they are efficient cost spreaders.
## Legal analysis: after transposition of PLD in 2024-26?

If Victim brings a lawsuit in Ireland against...

<table>
<thead>
<tr>
<th>If Victim brings a lawsuit in Ireland against...</th>
<th>Negligence (common law)</th>
<th>Strict Liability Defective Product (EU PLD?)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Duty of care to victim (foreseeable, proximity)</td>
<td>Acted unreasonably (negligently)</td>
</tr>
<tr>
<td>Johnson</td>
<td>YES</td>
<td>No</td>
</tr>
<tr>
<td>Exotic Imports</td>
<td>YES</td>
<td>No</td>
</tr>
<tr>
<td>Einstein Motors</td>
<td>YES</td>
<td>No</td>
</tr>
<tr>
<td>Bravo Bits</td>
<td>Probably yes</td>
<td>Probably no</td>
</tr>
<tr>
<td>Firefly</td>
<td>Maybe?</td>
<td>Maybe??</td>
</tr>
<tr>
<td>Dastardly</td>
<td>Who cares? He has no money! If any other person found liable, they could be jointly &amp; severally liable for up to 100% of Victim’s damages.</td>
<td></td>
</tr>
</tbody>
</table>