Killing Mi Software with EUR-Laws*

IETF118 Prague, Late Night "Bad Attitude Pechakucha", November 8, 2023

Robert Carolina,† General Counsel

Internet Systems Consortium

(*) NOTHING IS FINISHED YET. The Gang in Brussels are arguing about these now.
(†) These comments are personal and should not be attributed to anyone I know, to anyone who knows me, or to anyone else for that matter.
If you keep reading these notes, you risk injuring your eyesight. All terms and conditions stated herein are governed by and shall be construed in accordance with the laws of England (not including its body of private international law).

Over the course of 30 Years...

The Cyber Security Body Of Knowledge
www.cybok.org

CyBOK

Law and Regulation Knowledge Area
Version 1.0.2

Robert Carolina | Royal Holloway, University of London

And now for something completely different

Genuine picture. Obviously from "King of the Hill," and something that took way too long to make using the rudimentary tools under my control. Mike Judge is a genius.

Problems	Solution

• Functionality has drifted
  • from “tangible products” (e.g., cars)
  • to “digital products”
  (e.g., software that actuates car controls)
• Most human beings ($especially < +2\ \sigma$)
  • buy functionality, not security
  • cannot distinguish good & bad software
• Too many software vendors have too little incentive to invest in making software more secure (or to pass the laugh test)
 	
George “Lemon Tree” Akerlof predicted this type of outcome in 1970*
	The EU declares
	
	software is a “product” for purposes of:
	
	• **<u>product conformity regulation</u>**, and
	• **<u>product liability law</u>**

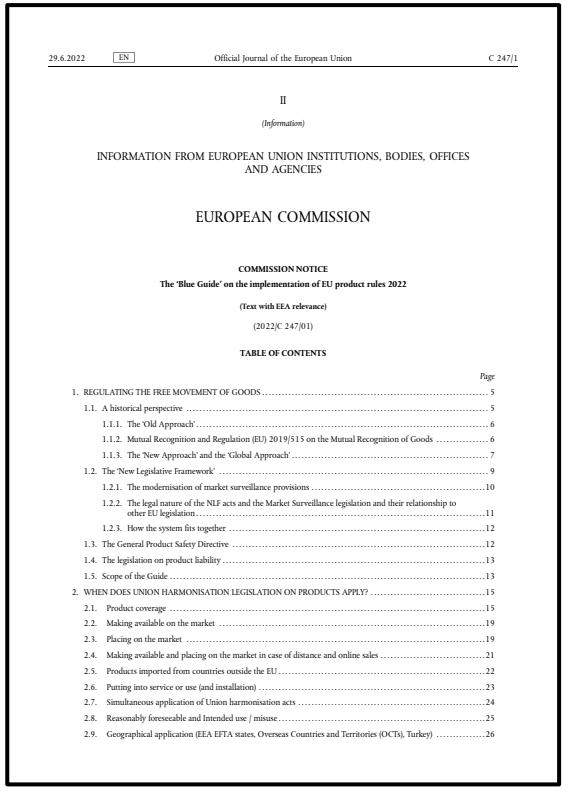
* Akerlof, George A. (1970). "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism". Quarterly Journal of Economics. The MIT Press. 84 (3): 488–500. doi:10.2307/1879431. If you have not heard of this before, I am shocked. It’s a helpful way to describe a type of market failure that is common in the field of cybersecurity and information technology more generally. You should read more. Just not these notes.

New law	What it does
Cybersecurity Resilience Act (CRA)	• Software subject to conformity assessment (CE Marking) • Procedural, informational, and reporting obligations
Product Liability Directive (PLD)	• Make software manufacturers* liable for defective software • Does not apply to source code† as such
For both…	• Obligations attach to those who place product “on the market” • Includes giving software away for free, if something else is in play – like accepting some money to help someone use the software you gave away for free • Framework “inspired” by The Blue Guide

(*) If you shove software out into the world with your name or logo on it, you are probably a manufacturer. (†) There is no definition for “source code” because Of Course Not. The people who wrote this do not have a clear idea of how the distinction between source and executable gets blurred. But I am getting a little bit ahead of myself here. Stay tuned.

All Hail, the Blue Guide!

Published: 2014
No of pages: 134
COUNTIF("software") = 1
COUNTIF("open source") = 0



29.6.2022 EN Official Journal of the European Union C 247/1

II

(Information)

INFORMATION FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES

EUROPEAN COMMISSION

COMMISSION NOTICE
The 'Blue Guide' on the implementation of EU product rules 2022

(Text with EEA relevance)

(2022/C 247/01)

TABLE OF CONTENTS

Page

Published: 2022
No of pages: 152
COUNTIF("software") = 13
COUNTIF("open source") = 0

- Does it exempt charities?
- Is there a careful & thoughtful discussion on re-classifying software as a product?

Software: Are we talking about the same thing?

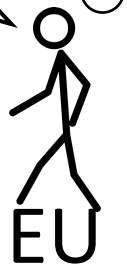
We do not need a definition of software. It's obvious.*†

Small companies will have no problem with this regulation. They manage simple products.*

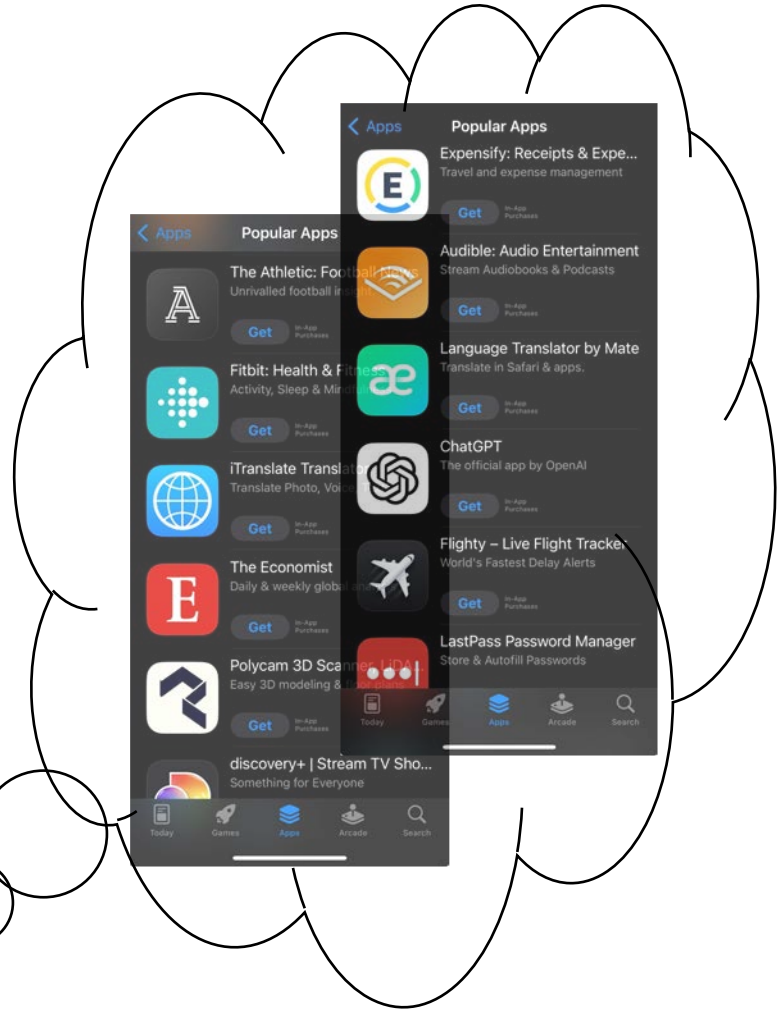
We can't possibly regulate by reference to software types and use cases. That would make my job much harder.*

Whiskey Tango Foxtrot?

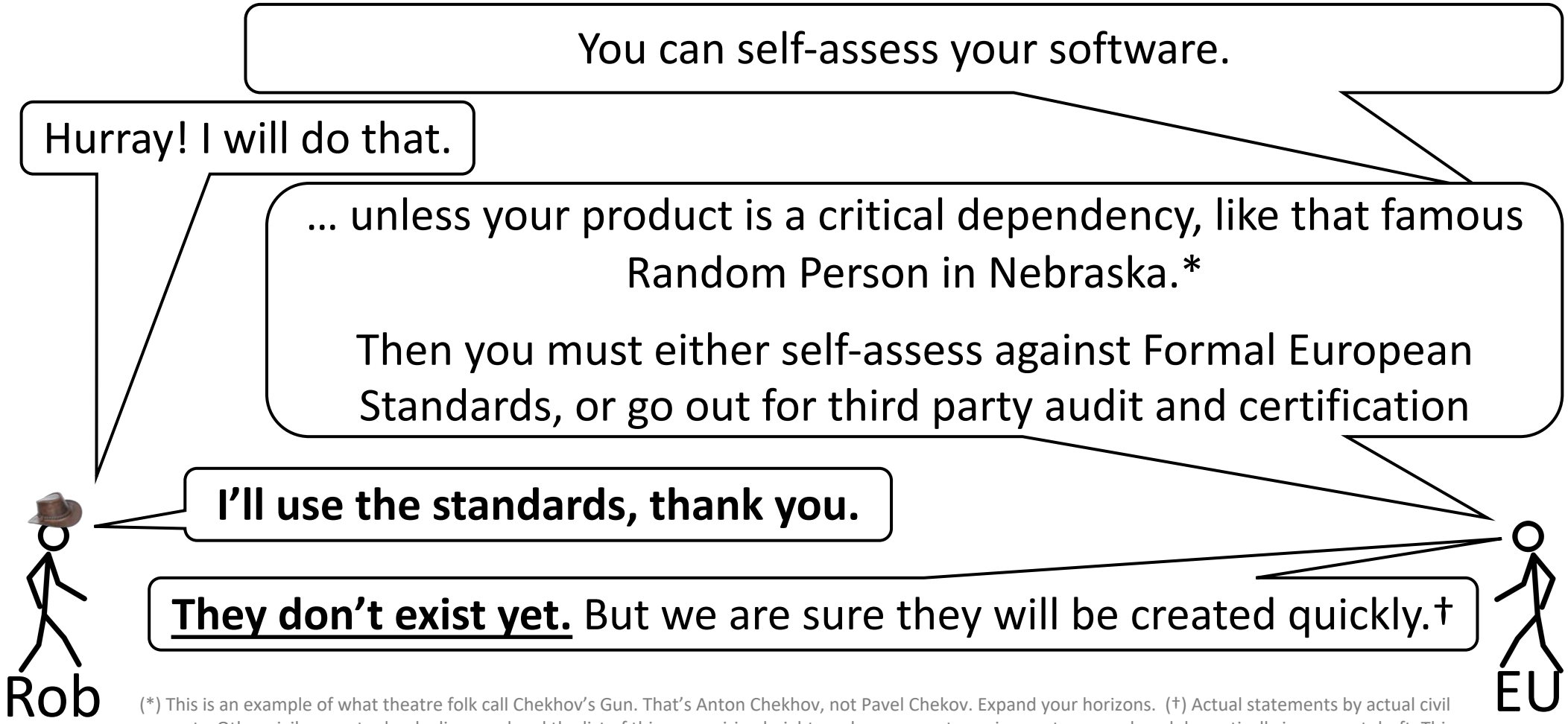
Rob



EU

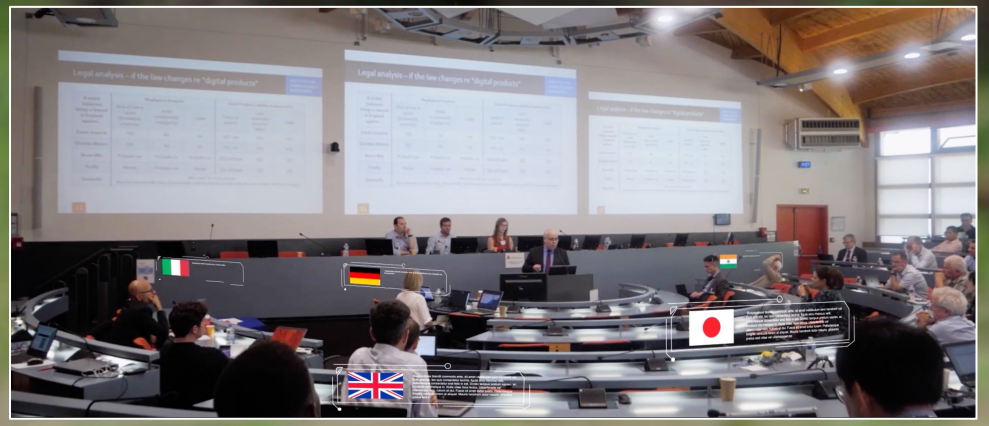


CE Conformity assessment



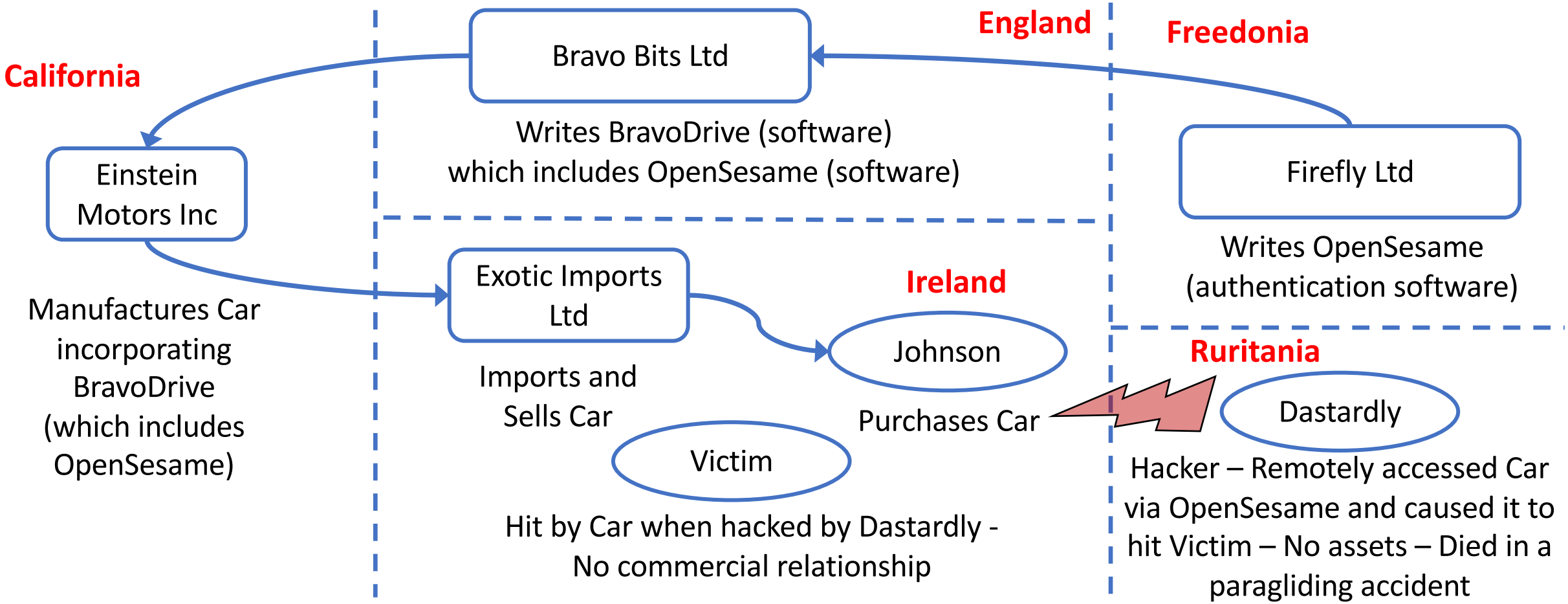
(*) This is an example of what theatre folk call Chekhov's Gun. That's Anton Chekhov, not Pavel Chekov. Expand your horizons. (†) Actual statements by actual civil servants. Other civil servants clearly disagreed and the list of things requiring heightened assessment requirements was reduced dramatically in a recent draft.

Arriving soon: security assessment standards for DNS software



The snail picture was catalogued as CC material without any further information. Obviously the ETSI logo is property of ETSI. The inset photos are from an ETSI promotional video. In an interesting coincidence they were filming the promotional video the same week that I was delivering an address at ETSI Security Week in 2019. So yes, that's me at the podium talking to delegates for an hour about strict product liability for digital products. Would you like to see some of the slides I used? I hope so because they are coming up next. Funny how the world works, isn't it. You have definitely reached the point of diminishing returns on this note.

New Product Liability Directive (PLD) example: Hypothetical supply chain



I do not have any rights clearance information here because I drew this diagram myself. These footnotes could become the source of audience anxiety syndrome. An early performance by the Blue Man Group pointed out that we all suffer from information overload and a fear of missing out. This is a note you could easily have ignored without missing anything of significance. Let that be a lesson to you.

Hypothetical lawsuit: the law today

If Victim brings a lawsuit in Ireland against…	Negligence (common law)			Strict Liability Defective Product (EU 85/374)		
	Duty of care to victim (foreseeable, proximity)	Acted unreasonably (negligently)	Liable	Supply of product	Lacks reasonably expected safety	Liable
Johnson	YES	No	n/a	Not a supplier	n/a	n/a
Exotic Imports	YES	No	n/a	YES - car	YES	YES
Einstein Motors	YES	No	n/a	YES - car	YES	YES
Bravo Bits	Probably yes	Probably no	Probably no	No - software	n/a	n/a
Firefly	Maybe?	Maybe??	Maybe???	No - software	n/a	n/a

Law of strict liability for defective products makes manufactures and component suppliers financially responsible for dangerous products they supply that hurt people – they are efficient cost spreaders.

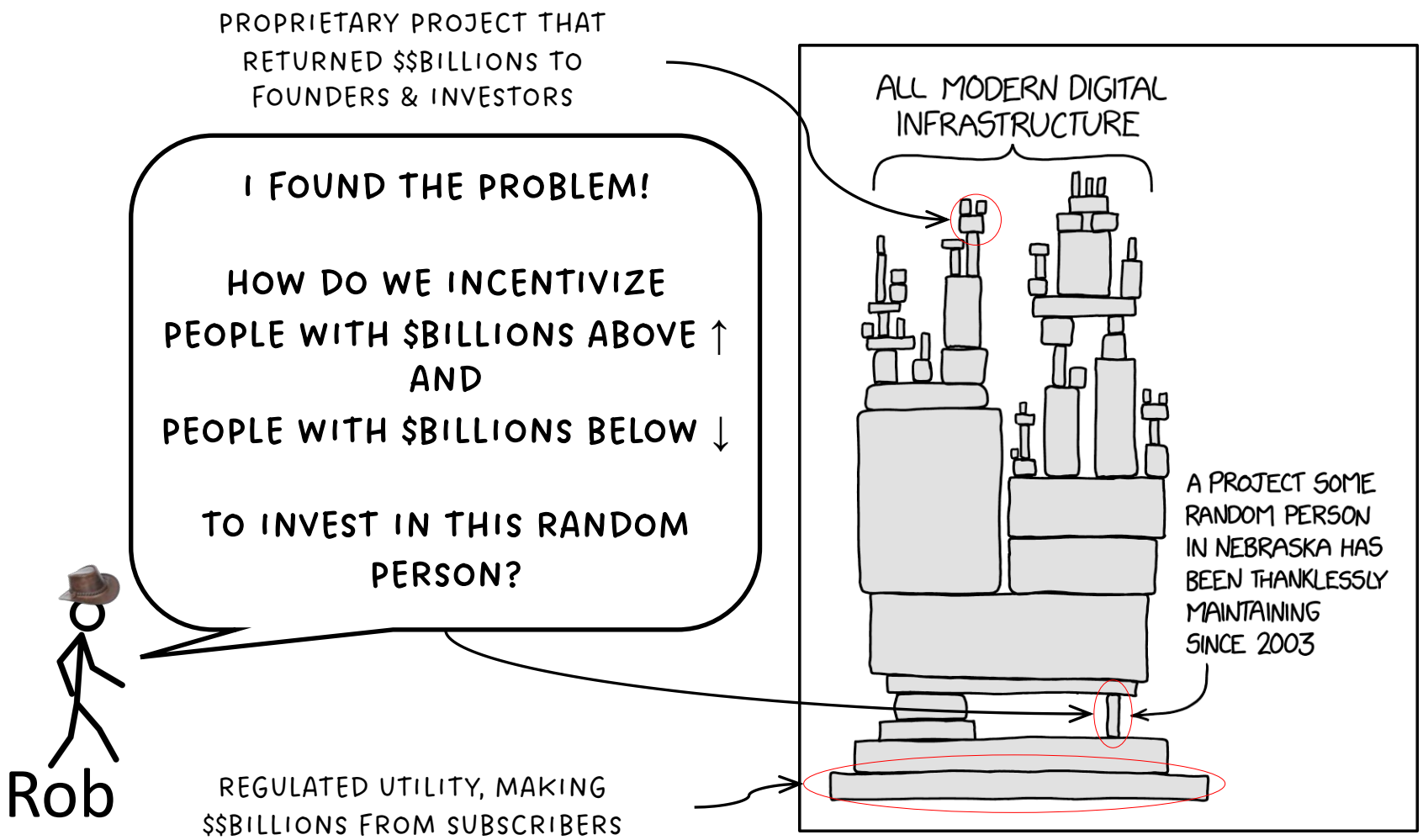
Believe it or not, I used a previous version of this slide to present these same ideas to a meeting of security experts at ETSI Security Week back in 2019. There's even a brief video of me delivering that talk in an ETSI promotional video they were making that week. I've placed a picture of that into this presentation, if you know where to look. But the reality is that you were probably off spending your time here reading the contents of the grid above.

Hypothetical lawsuit: after transposition of new PLD in 2025-26?

If Victim brings a lawsuit in Ireland against…	Negligence (common law)			Strict Liability Defective Product (EU PLD?)		
	Duty of care to victim (foreseeable, proximity)	Acted unreasonably (negligently)	Liable	Supply of product	Lacks reasonably expected safety	Liable
Johnson	YES	No	n/a	Not a supplier	n/a	n/a
Exotic Imports	YES	No	n/a	YES - car	YES	YES
Einstein Motors	YES	No	n/a	YES - car	YES	YES
Bravo Bits	Probably yes	Probably no	Probably no	**YES-software**	**YES**	**YES**
Firefly	Maybe?	Maybe??	Maybe???	**YES-software**	**YES**	**YES**

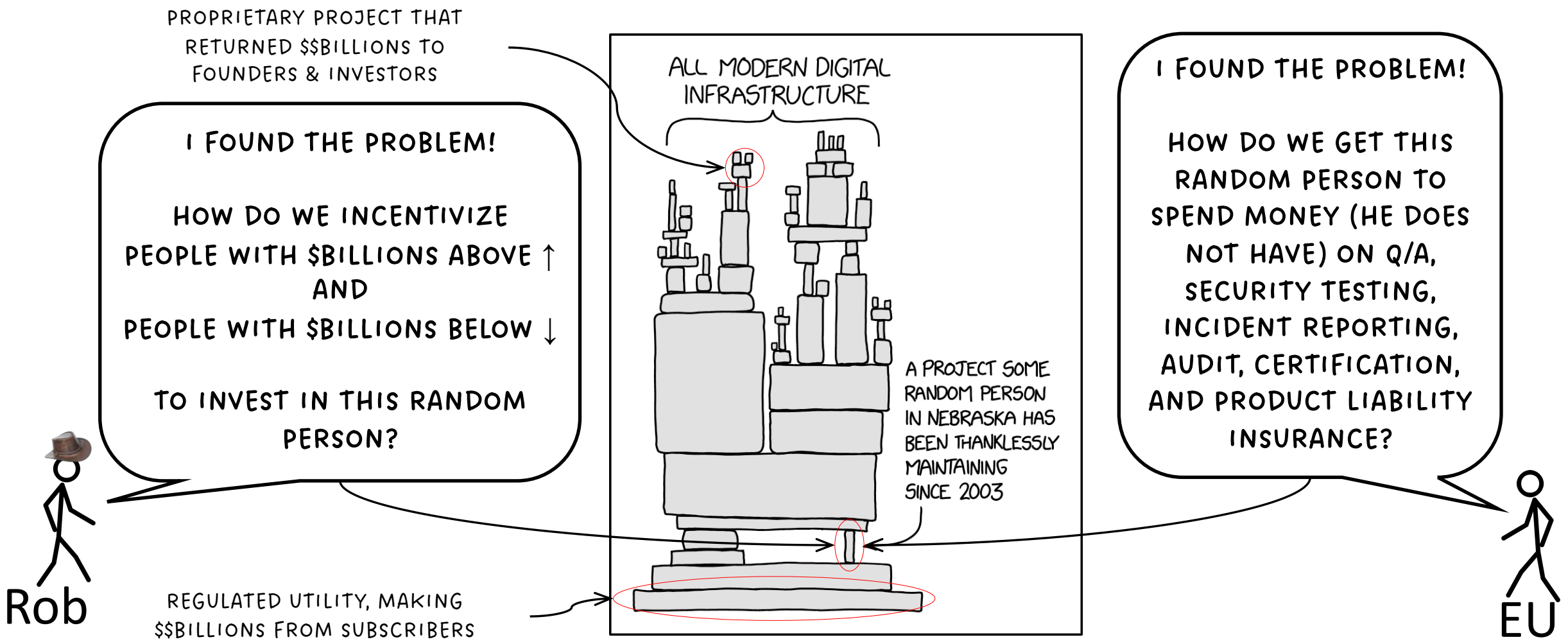
New law would **expand strict liability** and make "manufacturers" and/or "importers" of **software** financially responsible for dangerous software they supply that hurts people.

Describing the open source problem



This space intentionally blank. Foreshadowing

A minor difference in approach



The Open Source Community

Why there will be no general exemption from these laws for opensource software

- “What makes you so special?”
  - “If your software screws up, do we not bleed?”
  - “None of you can explain why you believe you are in the same boat.”
- “Besides, no matter what else happens we need to regulate People in Hats and people who are sort of like People in Hats
  - and people who might be on their way to wearing Hats
  - or distributing stuff that uses stuff made by people who wear Hats.”

- BUT, we might exempt a few of the Truly Worthy… if you can convince us that you truly are. Worthy, that is.

The Open Source Community 2.0

Still picture from "Spartacus," directed by S. Kubrick (1960). I'm going to suggest that any combination of "fair use" and/or "fair dealing" and/or "parody" are sufficient reasons to use this image. When I started lecturing, I used only words so I never thought I would need to do rights-clearance for my presentations. But hey, the Pechakucha Police want images more than words, so I need to find memes that work. Here's something I didn't know. Apparently, Spartacus was a meme used by the Communist Party to celebrate the rise of the proletariat. If you are the first person to shout out to me "Rob, You Are Spartacus" during this presentation I will award you ten Euros for your fast reading provided that you also comply with the additional terms & conditions stated herein. Back to the communist thing. I'm sure you appreciate that I am NOT trying to celebrate the Bad Old Days of Communism. I just wanted to re-create a famous moment from a big budget Hollywood film and then turn it upside down. But seriously, reading these notes while trying to listen to a lecture will confuse you if you are not careful. As a condition of the award stated, you must actually shout the negative of the statement previously quoted. Reading these notes may help you significantly.

NEXT:

- Biden Administration Cybersecurity Policy
- Software vendors need to be made liable for bad software

  (But HOW?)

- Team USA is taking a more cautious approach
- Asking for considered opinion from academia on HOW to allocate liability for bad software.
- Probably no new law before 2025
- Will it matter after Europe finishes it rush to… whatever?