

PRIVATE LAW LIABILITY IN THE IOT

MIREILLE HILDEBRANDT

March 30, 2020

FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic

As large numbers of people turn to video-teleconferencing (VTC) platforms to stay connected in the wake of the COVID-19 crisis, reports of VTC hijacking (also called "Zoom-bombing") are emerging nationwide. The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language.

ZOOM CLASSROOM HIJACKING

IS ZOOM LIABLE?

PCMag editors select and review products [independently](#). We may earn affiliate commissions from buying links, which help support our testing. [Learn more](#).

[Home](#) > [How-To](#) > [Communications](#) > [Video Conferencing Software](#)

How to Prevent Zoom-Bombing

Zoom is the video calling app of choice during the COVID-19 pandemic. Unfortunately, some features make your meetings susceptible to hijacking. Learn how to stop bad actors and keep your calls secure.



By [Jill Duffy](#) Updated April 16, 2020




ZOOM BOMBING SETTINGS

IS THE CONFERENCE ORGANIZER
WHO FAILS TO USE THE SETTINGS
LIABLE?

MOTHERBOARD
TECH BY VICE

Hackers Are Selling a Critical Zoom Zero-Day Exploit for \$500,000

People who trade in zero-day exploits say there are two Zoom zero-days, one for Windows and one for MacOS, on the market.

 By [Lorenzo Franceschi-Bicchieri](#)

April 15, 2020, 3:54pm  Share  Tweet  Snap

15 APRIL 2020

THE REALM OF CRIMINAL LAW
COULD THIS BE USED AS EVIDENCE WHEN
PROVING DAMAGE UNDER TORT LAW?

Zoom's Privacy Problems Snowball as Two Zero Days Uncovered

The Industry's Only SaaS-Delivered Enterprise DLP

Our unique approach to DLP allows for quick deployment and on-demand scalability, while providing full data visibility and no-compromise protection.

No-Compromise Data Protection is:

Amid increased scrutiny from researchers and privacy activists, two new zero days in the teleconferencing app surfaced on Wednesday.

29 SEPTEMBER 2020

For those who thought the problems are over

The Fresh Smell of ransomed coffee

by Martin Hron September 25, 2020 28 min read



We turned a coffee maker into a dangerous machine asking for ransom by modifying the maker's firmware. While we could, could someone else do it too? As you might expect, the answer is: Yes. Follow us on a journey where we show you that firmware is the new software.

Firmware is the new software

IoT
'firmware is
the new software'

The New York Times

Cyber Attack Suspected in German Woman's Death

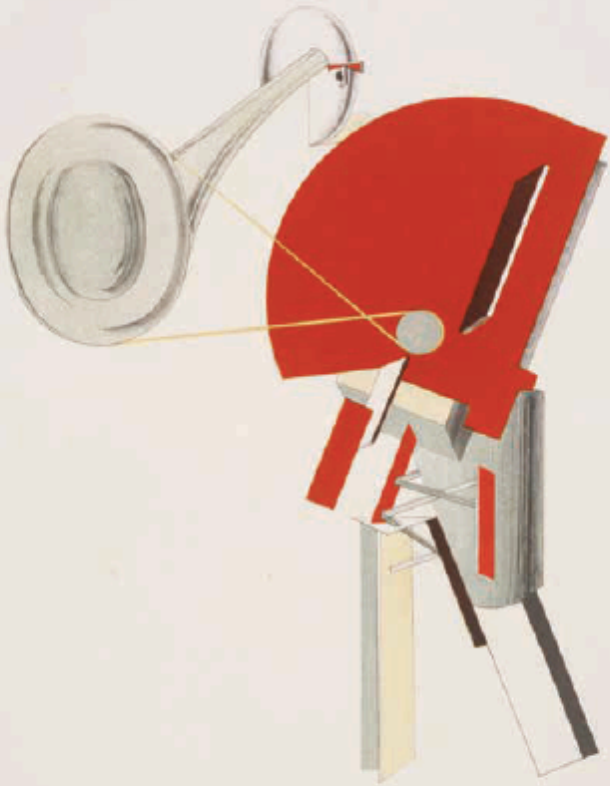
Prosecutors believe the woman died from delayed treatment after hackers attacked a hospital's computers. It could be the first fatality from a ransomware attack.



IoT

- Healthcare
- Connected cars
- Smart energy grid
- Smart cities

OXFORD

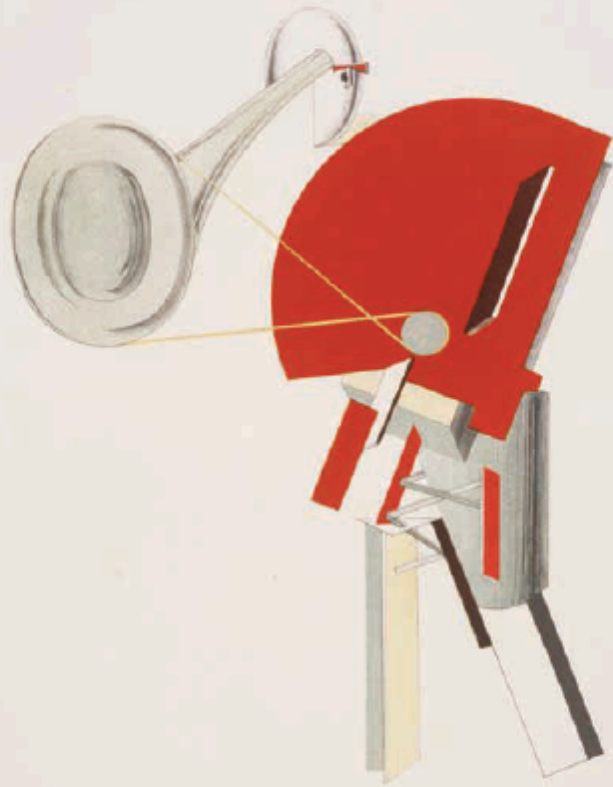


LAW FOR
COMPUTER
SCIENTISTS
and OTHER FOLK

MIREILLE
HILDEBRANDT

TAKING LAW SERIOUSLY

THE book



LAW FOR
COMPUTER
SCIENTISTS
and OTHER FOLK

MIREILLE
HILDEBRANDT

Chapter 8 Private law liability for faulty ICT

234 Private Law Liability for Faulty ICT

I expect that private law liability, together with data protection law, competition law, and consumer protection, will take the lead in reconfiguring the legal landscape of the onlife world. This should contribute to more adaptive legal protection and a better distribution of checks and balances between technology developers, manufacturers, retail, service providers, and end-users.



AGENDA

- AI harms at two levels
- Tort liability
 - *In the EU: national law*
 - *Product liability (EC White Paper AI 2020)*
 - *GDPR (private law liability art. 79-82)*



AI harms at two levels

1. Identifiable damage or harm of individuals

- *breach of contract (e.g. in case of non-conformity)*
- *tort (third party liability for damage caused)*
- *injunctions (court order to stop unlawful behaviour)*

2. Implications at level of society

- *administrative law (GDPR)*
- *consumer law (unfair contract terms)*
- *safety law (Machinery Directive, General Product Safety Directive)*



AI harms at two levels

Role of private law liability:

- 1. Compensation for harm suffered (individual)**
- 2. Deterrence and prevention (economic incentive)**

Tort liability

- **EU tort law (national law)**
- **Default: each bears their own damage, except if:**
 - *damage (to be proven by the victim)*
 - *wrongful act (fault or negligence)*
 - *attribution (to the tortfeasor)*
 - *causality (btw damage and act)*
- *Fault liability*
- *Strict liability*
- **Note that for an injunction no need to prove damage**
 - **Art. 3:296 BW**
 - **Art. 79 GDPR**



Tort liability

■ Product liability

- *EU legislation, incorporated in national law*
 - mitigated strict liability
 - reversal of burden of proof
 - if damage, defect and causality is proven (by injured party)
 - manufacturer must pay compensation
 - unless they prove otherwise



Tort liability

■ Product liability

- *Product liability does not apply to consumer transactions with suppliers outside the EU (e.g. Alibaba)*
- *See the BEUC report that was written about this in 2017 https://www.beuc.eu/publications/beuc-x-2017-122_the_challenge_of_protecting_eu_consumers_in_global_online_markets.pdf*



Tort liability

- **Product liability**
 - *At this moment it is not clear to what extent software falls within the scope of the term 'product' in the directive*
 - *At this moment liability for a 'defect' in the directive probably does not apply to software or firmware updates, because the defect must be known or knowable at the moment the product is put on the internal market of the EU*
 - *The EU is working on adaptations of a.o. the Product Liability Directive to clarify and update legal protection*

Tort liability

- **What if you cannot prove damage?**
 - *E.g. the case of the Samsung* *it was more interesting to file an injunction, asking the court to order Samsung to provide updates in specific cases where they don't*
 - *If the court had agreed that Samsung has a duty of care to provide updates during a longer period than they do or under other conditions than they do, it could have ordered Samsung to provide those updates*
 - *The applicant need not prove damage in this case, though they will have to convince the court that such a duty of care exists (e.g. based on art. 6:162 that speaks of 'hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt')*
 - *The court found that the Consumer Protection organisation did not provide sufficient evidence that SAMSUNG violated its duty of care*

Tort liability

- **What if you cannot prove damage?**
 - E.g. in case of a data breach, where it may be difficult to put a number on the damage for individuals
 - Art. 79 GDPR requires that Member States provide access to court in case of a violation of the GDPR, e.g. in case of unlawful processing, to make sure such processing is terminated
 - Art. 80 GDPR requires that Member States allow a dedicated NGO to file an injunction in its own name or in the name of data subjects who mandate their claim
 - Art. 82 is about suing for damages, in that case art. 80 leave to the Member States whether they want to allow for collective action
 - So in case of an injunction, art. 80 directly provides a right to collective action, though this is not the case if one wishes to sue for damages
 - E.g. the recent tort action against Oracle and Salesforce may break down if damage is not proven

Tort liability

- To obtain protection against security mishaps in the IoT:
 - **an injunction** is far more effective, because what you want is that the company changes their policy and/or backend system, and they will have to demonstrate to the court that they are complying with the order on pain of penalty payments
 - **suing for damages** is much less effective, because it is difficult for the potential victim to find out whether proper action is taken to prevent future damages (besides difficulty with proving damage)
 - in both cases the applicant must prove that the tortfeasor violates their **duty of care** in relation to the applicant(s) (and in case of a collective action, the interests they support and/or the victims they represent)



EUROPEAN
COMMISSION

Brussels, 19.2.2020
COM(2020) 64 final

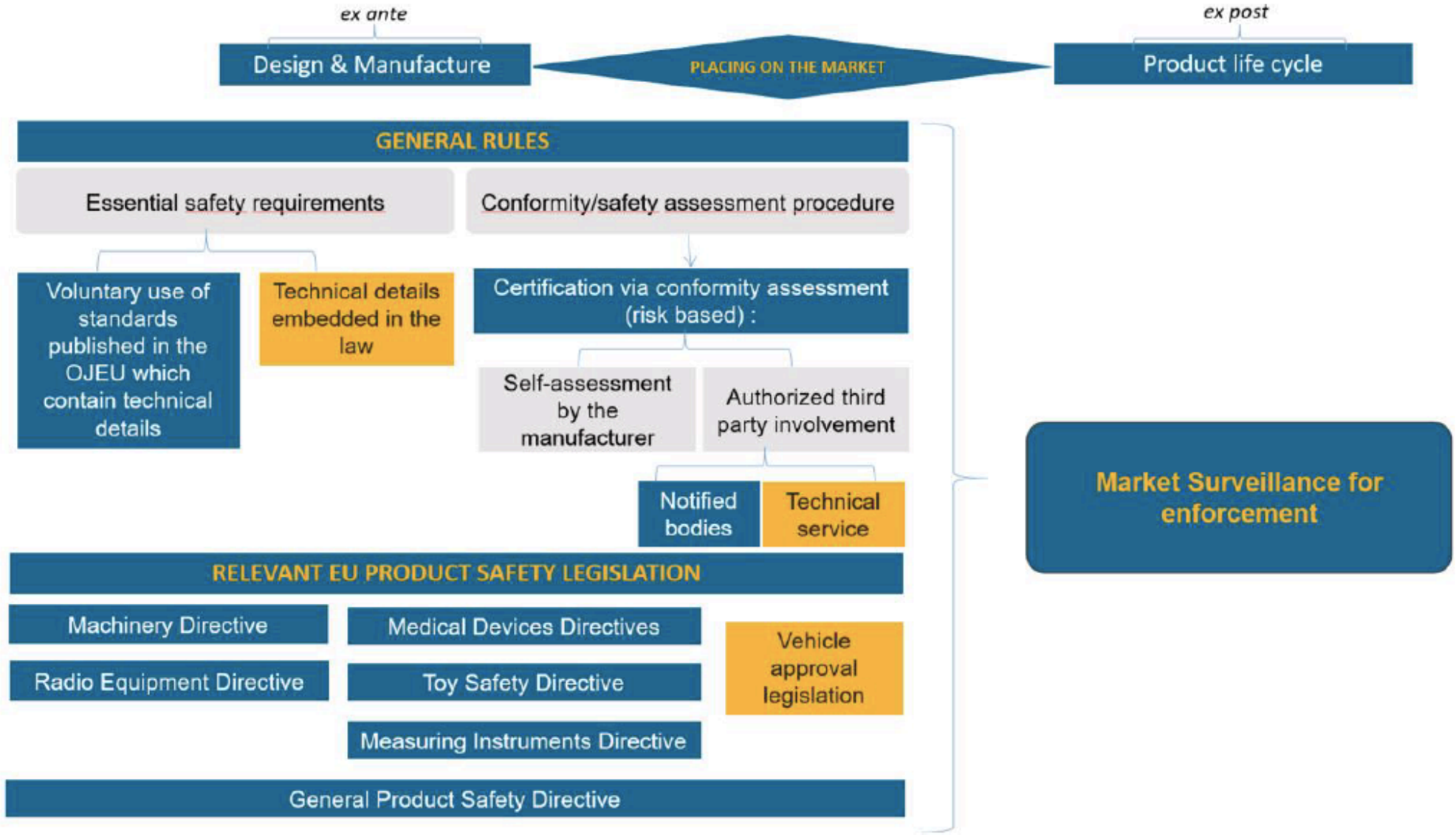
**REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE
COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE**

**Report on the safety and liability implications of Artificial Intelligence, the Internet of
Things and robotics**

- SAFETY & SECURITY

[HTTPS://EC.EUROPA.EU/INFO/SITES/I
NFO/FILES/REPORT-SAFETY-LIABILITY-
ARTIFICIAL-INTELLIGENCE-
FEB2020 EN 1.PDF](https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_en_1.pdf)

The underlying logic of the current Union product safety legislation²⁵





EUROPEAN
COMMISSION

Brussels, 19.2.2020
COM(2020) 64 final

**REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE
COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE**

**Report on the safety and liability implications of Artificial Intelligence, the Internet of
Things and robotics**

SAFETY & SECURITY

NEW ISSUES RAISED BY:

- CONNECTIVITY
- AUTONOMY
- MENTAL HEALTH RISKS
- DATA DEPENDENCY
- OPACITY
- COMPLEXITY PRODUCTS SYSTEMS
- SOFTWARE COMPONENTS
- COMPLEXITY VALUE CHAINS

Upcoming EU liability law

European Commission White Paper proposes to:

1. update definition of product
2. reduce burden of proof wrt 'defect'
3. reduce or remove 'later defect' and 'development risk' defences tortfeasor
4. extend liability beyond 'putting into circulation'
5. consider strict liability for damage caused by autonomous AI applications



YOU'RE TRYING TO PREDICT THE BEHAVIOR
OF <COMPLICATED SYSTEM>? JUST MODEL
IT AS A <SIMPLE OBJECT>, AND THEN ADD
SOME SECONDARY TERMS TO ACCOUNT FOR
<COMPLICATIONS I JUST THOUGHT OF>.

EASY, RIGHT?

SO, WHY DOES <YOUR FIELD> NEED
A WHOLE JOURNAL, ANYWAY?



LIBERAL-ARTS MAJORS MAY BE ANNOYING SOMETIMES,
BUT THERE'S *NOTHING* MORE OBNOXIOUS THAN
A PHYSICIST FIRST ENCOUNTERING A NEW SUBJECT.

- INTERSECT

- Law: enables, prohibits, restricts
 - *Reasonable*
 - *Pertinent*