Software Liability, Hackbacks, and Deepfakes

Emerging topics in cyber risk that need to be quantified

Éireann Leverett

@concinnityrisks

Erin Burns

@camerapop

An acceptable introduction

Software Liability

Tort liability when IoT devices get hacked is possible, and even being discussed in the EC and USA.

How would it change things?

Active Defense Legislation

The US and France are making moves to legislate for companies to be allowed to hackback under certain circumstances.

How would this change the balance of things?

Deepfakes

It is possible to make images of people saying and doing anything. The speed at which they are shared is faster than the time it takes to identify them as fakes.

How will this impact us?

Software Liability

Software Liability

Example Laws

The Ethiopian Federal Government Procurement and Property Administration Proclamation No.649/2009: Definition given for “goods” includes ***marketable software***

Product Liability Directive 85/374/EEC

Relevant Cases

FDA Class 1 Recall of Medtronic pacemakers

Kingsway Hall Hotel Ltd. v. Red Sky IT (Hounslow) Ltd. (2010)

FTC D-Link Case

Change

If this becomes common place…could we see secure coding be a requirement from insurers of software companies to their insureds?

How do we quantify?

Challenges to liability cost quantification:

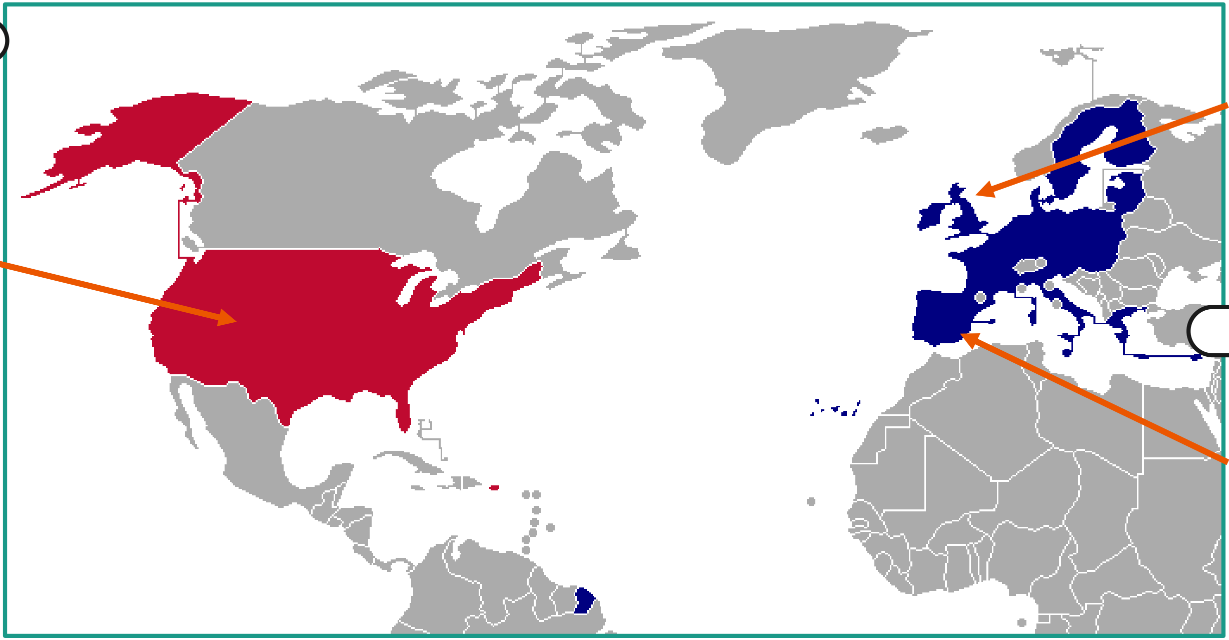
- Jurisdiction Shopping
- Estimating Software User #s
  - (E.G. Class Action Suits)
- Platform/Service/Device categorisation
- Frequency of
  - Malpractice
  - Negligence
- Amount of Software Available
  - CPE Dictionary up to date?
  - Number of configurations
- Software dependency
  - Upstream/downstream affected too

HackBack

Hackback: Legal landscape

USA
Active Cyber Defense Certainty Act (H. R. 4036 & 3270)

Computer Fraud and Abuse Act 1996



UK
1997 Police Act

Computer Misuse Act 1990, § 1-3

France
Addressed in Annex 7 of Revue stratégique de cyberdéfense

Deepfakes

Deepdive into Deepfakes

Have a policy in place to combat mis/dis info

Someone makes a video of your CEO laughing as they are informed the company's oil tanker has hit a beach. What do you do?

Have a strategy for response in press/media/social media.

When developing the strategy focus on rapid countering online more than legal.

Source: @bill_posters_uk

How would we quantify these risks in the future?

Thank you!

@concinnityrisks

@camerapop

Liability Resources

Standardisation and certification of safety, security and privacy in the 'Internet of Things'
https://journalofethics.ama-assn.org/article/are-current-tort-liability-doctrines-adequate-addressing-injury-caused-ai/2019-02
New revised baseline text of draft Recommendation X.secup-iot (Secure software update for IoT devices)
https://bit.ly/2Sq0KiM
Liability for Autonomous and Artificially Intelligent Robots
https://bit.ly/2JY2En1
Report From The Commission To The European Parliament, The Council And The European Economic And Social Committee On The Application Of The Council Directive On The Approximation Of The Laws, Regulations, And Administrative Provisions Of The Member States Concerning Liability For Defective Products (85/374/Eec)
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:246:FIN
Proclamation No. 649/2009. Ethiopian Federal Government Procurement and Property Administration Proclamation - 9 September 2009
https://bit.ly/2XVhwMI

HackBack Resources

Orlando Doctrine articles
https://flipboard.com/@bsdunlap/orlando-doctrine-vq6o2umry
Active Cyber Defense Certainty Act
https://www.congress.gov/bill/116th-congress/house-bill/3270/text
Active Cyber Defense Certainty Act explainer
https://tomgraves.house.gov/uploadedfiles/acdc_expaliner.pdf
Hack-back legislation: What your security team needs to know
https://techbeacon.com/security/hack-back-legislation-what-your-security-team-needs-know
Doing unto others…the law and efficacy of hacking back
https://www.bcl.com/doing-unto-othersthe-law-and-efficacy-of-hacking-back/
A Right to Cybercounter Strikes: The Risks of Legalizing Hack Backs
https://ieeexplore.ieee.org/abstract/document/7030161/
Highlights of the French cybersecurity strategy https://blog.lukaszolejnik.com/highlights-of-french-cybersecurity-strategy/
France Says 'No' To Company Hack-Backs Following Online Attacks -- But Wants To Keep The Option Open For Itself
https://bit.ly/2Y16D7m

Deepfake Resources

Deepfakes paper: Few-Shot Adversarial Learning of Realistic Neural Talking Head Models
https://arxiv.org/abs/1905.08233
Mark Zuckerberg Deepfake:
https://www.instagram.com/bill_posters_uk/?utm_source=ig_embed
Legality - **We Don’t Need New Laws for Faked Videos, We Already Have Them**
https://www.eff.org/deeplinks/2018/02/we-dont-need-new-laws-faked-videos-we-already-have-them
NYTimes: Here Come the Fake Videos, Too
https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html
Examples and tutorials on creating deepfakes see Derpfakes Youtube channel:
https://www.youtube.com/channel/UCUix6Sk2MZkVOr5PWQrtH1g
Inside the Pentagon's race against deepfake videos
https://edition.cnn.com/2019/06/11/tech/zuckerberg-deepfake/index.html