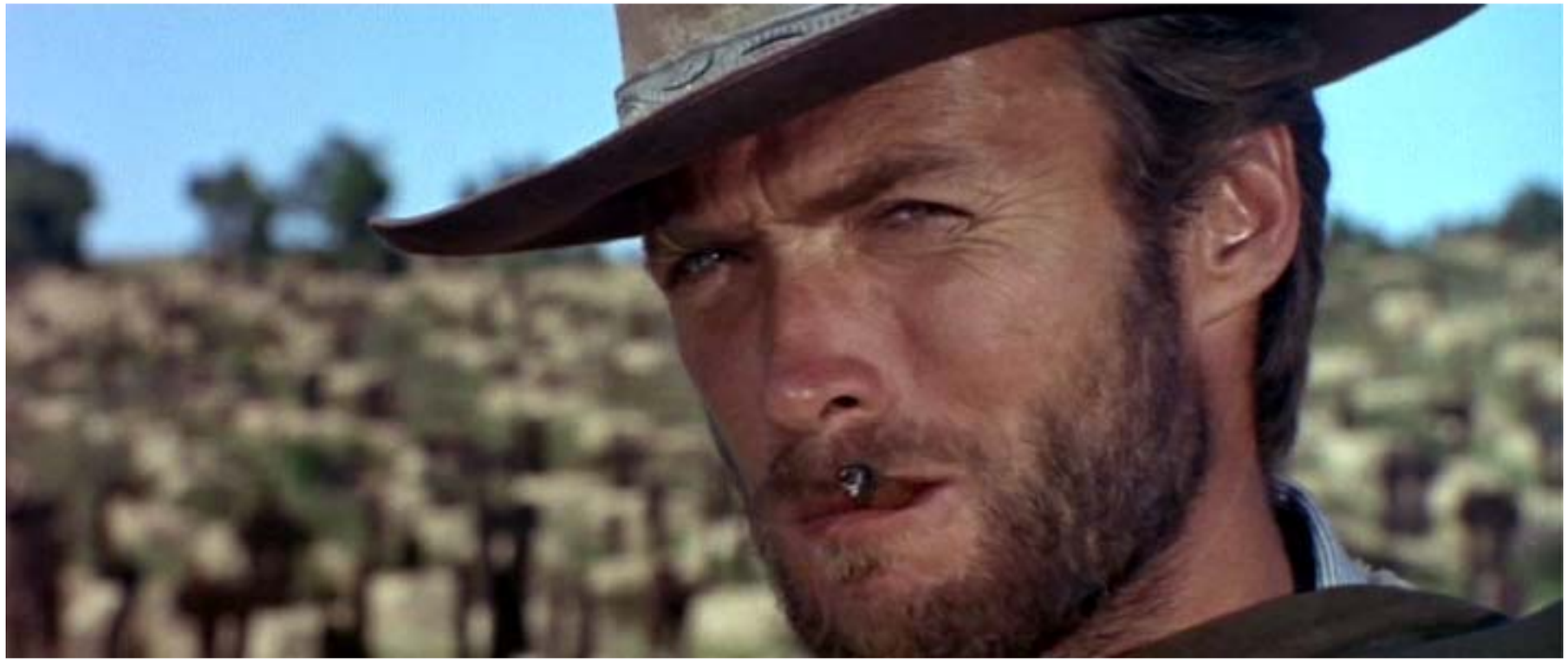
# Data Protection and Privacy since September…

*“Il Buono, il Brutto, il Cattivo”*
*“The Good, the Bad and the Ugly”*



# Court rulings

# Judgment in Case C-507/17
# Google LLC v Commission nationale de l'informatique et des libertés (CNIL)

- 24 September 2019, Full text, Press Release

- By an adjudication of 10March2016, the President of the Commission nationale de l'informatique et des libertés (French Data Protection Authority, France) (‘the CNIL’) imposed a penalty of €100000 on Google Inc. because of that company’s refusal, when granting a de-referencing request, to apply it to all its search engine’s domain name extensions…

- The operator of a search engine is not required to carry out a de-referencing on all versions of its search engine.

- It is, however, required to carry out that de-referencing on the versions corresponding to all the Member States and to put in place measures discouraging internet users from gaining access, from one of the Member States, to the links in question which appear on versions of that search engine outside the EU

# Judgment in Case C-673/17
# Bundesverband der Verbraucherzentralen und Verbraucherverbände– Verbraucherzentrale Bundesverband eV v Planet49GmbH on Cookies

- 1 October 2019, Full text, Press Release

- The German Federation of Consumer Organisations has challenged before the German courts the use by the German company, Planet49, of a pre-ticked checkbox in connection with online promotional games, by which internet users wishing to participate consent to the storage of cookies. The cookies in question aim to collect information for the purposes of advertising Planet49's partners' products.…

- Furthermore, according to the Court, the information that the service provider must give to a user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies.

- Storing cookies requires internet users' active consent.

- A pre-ticked checkbox is therefore insufficient.

# Judgment in Case C-18/18
# Eva Glawischnig-Piesczek v Facebook Ireland Limited

- 3 October 2019, Full text, Press Release

- Mme Eva Glawischnig-Piesczek, who was a member of the Nationalrat (National Council, Austria), chair of the parliamentary party ‘die Grünen’ (The Greens) and federal spokesperson for that party, sued Facebook Ireland in the Austrian courts. She is seeking an order that Facebook Ireland remove a comment published by a user on that social network harmful to her reputation, and allegations which were identical and/or of an equivalent content…

- EU law does not preclude a host provider such as Facebook from being ordered to remove identical and, in certain circumstances, equivalent comments previously declared to be illegalIn addition.

- EU law does not preclude such an injunction from producing effects worldwide, within the framework of the relevant international law which it is for Member States to take into account

# EDPB & EDPS

- EDPB:
    - Opinion 15/2019 on the draft decision of the competent supervisory authority of the United Kingdom regarding the Binding Corporate Rules of Equinix Inc. (08 October 2019)
    - EDPB Stakeholder Event on Data Subject Rights (04 November 2019 November)
    - Fifteenth Plenary Session of the EDPB - 12 & 13 November 2019
    - Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation
    - Guidelines 3/2019 on processing of personal data through video devices (consultation closed)
- EDPS:
    - Opinion on EU-Japan Passenger Name Record Data Agreement (25 October 2019)

# FBI misused surveillance data, spied on its own, FISA ruling finds

- https://arstechnica.com/tech-policy/2019/10/unsealed-fisa-ruling-slaps-fbi-for-misuse-of-surveillance-data/

- In an October 2018 ruling unsealed and posted on October 8, 2019 by the Office of the Director of Intelligence, the United States Foreign Intelligence Surveillance Court (FISC) found that the employees of the Federal Bureau of Investigation had inappropriately used data collected under Section 702 of the Foreign Intelligence Surveillance Act (FISA). The FBI was found to have misused surveillance data to look into American residents, including other FBI employees and their family members, making large-scale queries that did not distinguish between US persons and foreign intelligence targets.

# FISA ruling (part II)

- https://thehill.com/policy/national-security/464880-court-rules-fbi-surveillance-violated-americans-rights

“The ruling identified tens of thousands of improper FBI searches of intelligence databases in 2017 and 2018, according to the ruling, which found these searches may have been used to vet personnel and cooperating sources.

It also found that the FBI was not properly identifying and documenting which searches were connected to people in the U.S.

The ruling found improper use of the database by individuals, including at least one FBI contractor who searched an intelligence database for information on himself, relatives and other personnel.”

# LinkedIn-hiQ Opinion

- Full text
- https://www.eff.org/deeplinks/2019/09/victory-ruling-hiq-v-linkedin-protects-scraping-public-data
- “Ruling in hiQ v. Linkedin Protects Scraping of Public Data”
- “In a long-awaited decision in hiQ Labs, Inc. v. LinkedIn Corp., the Ninth Circuit Court of Appeals ruled that automated scraping of publicly accessible data likely does not violate the Computer Fraud and Abuse Act (CFAA).”
- “This is an important clarification of the CFAA’s scope, which should provide some relief to the wide variety of researchers, journalists, and companies who have had reason to fear cease and desist letters threatening liability simply for accessing publicly available information in a way that publishers object to. It’s a major win for research and innovation, which will hopefully pave the way for courts and Congress to further curb abuse of the CFAA.”

# ICDPC

- https://edps.europa.eu/data-protection/our-work/publications/international-conferences/resolutions-and-declaration-2018_en
- Declaration on Ethics and Data Protection in Artificial Intelligence
- Resolution on e-learning platforms
- ICDPPC Future of the Conference Working Group
- Resolution on a roadmap on the Future of the International Conference
- Resolution on Collaboration between Data Protection Authorities and Consumer Protection Authorities for Better Protection of Citizens and Consumers in the Digital Economy
- Resolution on the Conference Census

# E-privacy

- https://iapp.org/news/a/finland-eyes-eprivacy-agreement-before-years-end/

- "The Presidency of the EU Council is expected to propose yet another iteration of the ePrivacy text for the next meeting of the Working Party on Telecommunications and Information Society Nov. 7."

- "Ever since the European Commission first presented its plans to overhaul the ePrivacy law in January 2017, the file has been mired in lobbying and conflicting positions of EU member states. In fact, until Finland took over the presidency in July, it appeared to be completely stalled."

# German Data Protection Authorities Adopt New GDPR Fine Model

- https://www.linkedin.com/pulse/german-data-protection-authorities-adopt-new-gdpr-fine-tim-wybitul

- “The Conference of the German Data Protection Authorities (DSK) — the joint body of the German data protection authorities — has agreed on a radical new model for calculating EU General Data Protection Regulation (GDPR) fines. If adopted, the new fine model will likely lead to fines that frequently approach the maximum limits under Article 83 of the GDPR.”

# Data Breaches

# Inadvertently been used for advertising purposes

- https://help.twitter.com/en/information-and-ads

- “We recently discovered that when you provided an email address or phone number for safety or security purposes (for example, two-factor authentication) this data may have inadvertently been used for advertising purposes…”

# DoorDash

- “DoorDash, a takeout delivery company, confirmed a data breach on Thursday almost five months after it occurred on May 4, and a year after some users started complaining that their accounts had been inexplicably compromised. The company said that the incident exposed data from 4.9 million users, merchants, and delivery workers. Users who made accounts after April 5, 2018 were not affected by the breach. DoorDash said that the incident occurred through a third-party service. The breach compromised names, email addresses, order histories, phone numbers, delivery addresses, and hashed and salted passwords. Hackers also grabbed the last four digits of some user credit cards, but not the complete numbers or card verification values (CVV). Hackers also accessed the last four digits of some merchants' and delivery workers' bank account numbers. The cherry on top is that the hackers also stole the driver's license numbers of about 100,000 delivery workers.” 27/07/2019

- https://www.wired.com/story/doordash-breach-notpetya-fedex-security-roundup/

# Yahoo photos and videos

- Engineer admits hacking Yahoo accounts searching for images

- “A former Yahoo software engineer has pleaded guilty to hacking into the accounts of some 6,000 Yahoo users in search of sexual photos and videos.”

- https://apnews.com/873ff30a74a04b4ea7c89cb7bb7fa6e1

- 30 September 2019

# UniCredit

- https://www.zdnet.com/article/unicredit-reveals-data-breach-exposing-3-million-customer-records/

- UniCredit reveals data breach exposing 3 million customer records

- The Italian bank says that a single file is to blame.

- In total, roughly three million records were exposed, revealing the names, telephone numbers, email addresses, and cities where clients were registered.

# 7-Eleven fuel app

- https://www.theguardian.com/technology/2019/oct/25/7-eleven-fuel-app-data-breach-exposes-users-personal-details

- 7-Eleven fuel app data breach exposes users' personal details

- The popular petrol-buying app run by 7-Eleven has suffered a data breach that allowed customers to view the names, email addresses, mobile numbers and dates of birth of other users.

- The customer, who asked not to be named, said he discovered the fault on Thursday when he opened the app and found someone else’s information, including the amount of money in their account, their name, email address, phone number, and date of birth. He logged back out and in several times, and other people’s information appeared in the account when he logged back in.

# Adobe Creative Cloud

- https://www.zdnet.com/article/adobe-left-7-5-million-creative-cloud-user-records-exposed-online/

- Adobe left 7.5 million Creative Cloud user records exposed online

- The basic customer details of nearly 7.5 million Adobe Creative Cloud users were exposed on the internet inside an Elasticsearch database that was left connected online without a password.

- Exposed user details included email addresses, Adobe member IDs (usernames), country of origin, and what Adobe products they were using. Other information also included account creation date, the last date of their login, whether the account belonged to an Adobe employee, and subscription and payment status.

# Card scammer scammed

- “BriansClub,” one of the largest underground stores for buying stolen credit card data, has itself been hacked. The data stolen from BriansClub encompasses more than 26 million credit and debit card records taken from hacked online and brick-and-mortar retailers over the past four years, including almost eight million records uploaded to the shop in 2019 alone.

- The leaked data shows that in 2015, BriansClub added just 1.7 million card records for sale. But business would pick up in each of the years that followed: In 2016, BriansClub uploaded 2.89 million stolen cards; 2017 saw some 4.9 million cards added; 2018 brought in 9.2 million more.

- Between January and August 2019 (when this database snapshot was apparently taken), BriansClub added roughly 7.6 million cards.

-

# NordVPN

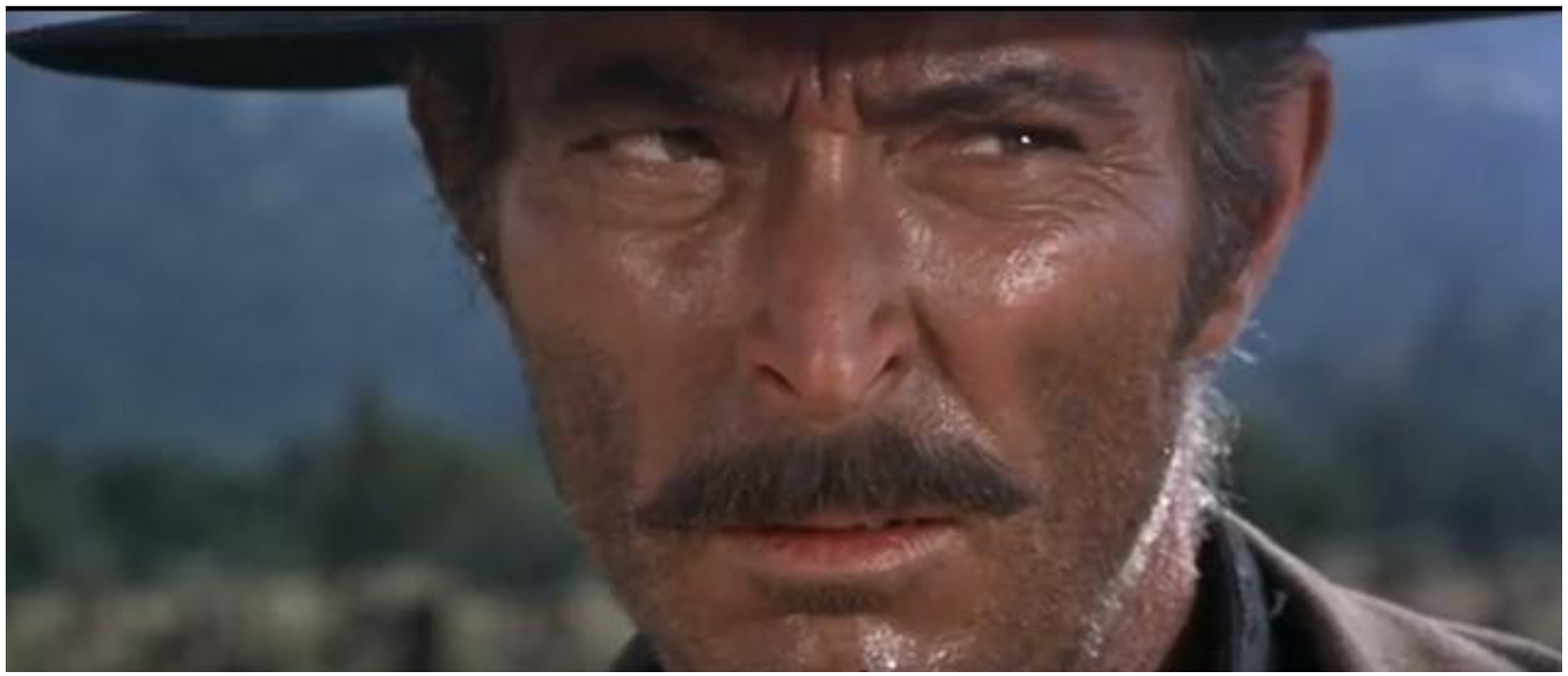
- https://www.cnet.com/news/popular-vpn-service-nordvpn-confirms-datacenter-breach/

- Popular VPN service NordVPN confirms data center breach
- Hackers in 2018 accessed a lone server in Finland.

- Techs at the company found an account of the data breach a few months ago, which led to a security audit. The VPN provider said it canceled its contract with the data center and verified that none of its servers could be accessed in a similar fashion.

# Used “To” instead of “BCC”

- https://www.bbc.com/news/uk-england-berkshire-50209064
- Email addresses exposed in West Berkshire Council data breach
- A council has shared more than 1,000 people's email addresses in a data breach.
- The council said it has reported the incident to data protection watchdog the Information Commissioner's Office (ICO).
- "On 25 October, the council was made aware of an incident by which a large number of service users were copied into an email containing a survey about leisure centres. … This led to each recipient being able to see one another's email addresses."
- The council later sent a second email to its service users saying: "We're really sorry that your email address was shared in this way."
- It said a member of staff had inserted addresses into the wrong field when composing the email.



# On Surveillance, and some Blog posts and general Clickbait**

**It means what you think it means: bait for clicks. It's a link which entices you to click on it.

# US-UK CLOUD act agreement

- EDPB-EDPS Joint Response on the US Cloud Act to the request from European Parliament's Committee on Civil Liberties, Justice and Home Affairs

"We are of the view that currently, unless a US CLOUD Act warrant is recognised or made enforceable on the basis of an international agreement, the lawfulness of such transfers of personal data cannot be ascertained, without prejudice to exceptional circumstances where processing is necessary in order to protect the vital interests of the data subject."

- Epic commented:

"The agreement permits cross-border access to personal data without judicial approval, allows for law enforcement investigations under lower standards than in the U.S., and lacks notice to data subjects who are subject to surveillance. In testimony before the European Parliament, EPIC International Counsel Eleni Kyriakides argued that cross-border access to personal data should ensure robust human rights protections, such as notice, judicial authorization, and transparency."

- https://cyberlaw.stanford.edu/blog/2019/10/big-interception-flaw-us-uk-cloud-act-agreement by Albert Gidari:

"But there is a big flaw in the agreement that hasn't been discussed -- it allows either the US or UK to require a covered provider to wiretap a user located not in the US or UK, but in any third country, without the approval of that sovereign nation and perhaps even without its knowledge. Yes, read that again."

- And also a paper by Theodore Christakis: 21 Thoughts and Questions about the UK/US CLOUD Act Agreement (and an Explanation of How it Works – with Charts).

# AI Facial recognition

- https://www.ft.com/content/90ce2dce-c413-11e9-a8e9-296ca66511c9 22 August 2019
    - “EU plans sweeping regulation of facial recognition”
    - “Brussels is exploring ways to impose strict limits on the use of facial recognition technology in an attempt to stamp out creeping public surveillance of European citizens.”
    - “On Wednesday, Sweden’s national data protection authority imposed the first fine under GDPR for misuse of facial recognition on a school that trialled the technology to monitor the daily attendance of students. The school was fined SKr200,000 (€18,670) for breaching students’ privacy rights using camera surveillance.”
- https://news.bloomberglaw.com/privacy-and-data-security/police-use-of-facial-recognition-tech-approved-in-sweden 25 October 2019
    - “Identifying criminal suspects through facial recognition tools is more effective than identifications made by officers, ‘and is thus a means of allowing them to carry out their duties more effectively,’ the DPA said in its decision”
- https://www.bloomberg.com/news/articles/2019-10-03/french-liberte-tested-by-nationwide-facial-recognition-id-plan
    - “France Set to Roll Out Nationwide Facial Recognition ID Program”

# Rethinking Encryption

- https://www.lawfareblog.com/rethinking-encryption
- By Jim Baker, former general counsel of the Federal Bureau of Investigation
- Bruce Schneier's comment:

*" Basically, he argues that the security value of strong encryption greatly outweighs the security value of encryption that can be bypassed. He endorses a 'defense dominant' strategy for Internet security.*

*Keep in mind that Baker led the FBI's legal case against Apple regarding the San Bernardino shooter's encrypted iPhone. In writing this piece, Baker joins the growing list of former law enforcement and national security senior officials who have come out in favor of strong encryption over backdoors: Michael Hayden, Michael Chertoff, Richard Clarke, Ash Carter, William Lynn, and Mike McConnell.*

*Edward Snowden also agrees. "*

- Bruce Schneier is an internationally renowned security technologist.

# Whats App hacking

- https://www.reuters.com/article/us-facebook-cyber-whatsapp-nsogroup/exclusive-whatsapp-hacked-to-spy-on-top-government-officials-at-us-allies-sources-idUSKBN1XA27H 31 October 2019

- “Government officials around the globe targeted for hacking through WhatsApp”

- “Senior government officials in multiple U.S.-allied countries were targeted earlier this year with hacking software that used Facebook Inc’s (FB.O) WhatsApp to take over users’ phones, according to people familiar with the messaging company’s investigation.”

- “While it is not clear who used the software to hack officials’ phones, NSO has said it sells its spyware exclusively to government customers.“

# DoH - DNS over HTTPS

- https://arstechnica.com/tech-policy/2019/09/isps-worry-a-new-chrome-feature-will-stop-them-from-spying-on-you/

- “Why big ISPs aren’t happy about Google’s plans for encrypted DNS”

- “When you visit a new website, your computer probably submits a request to the domain name system (DNS) to translate the domain name (like arstechnica.com) to an IP address. Currently, most DNS queries are unencrypted, which raises privacy and security concerns. Google and Mozilla are trying to address these concerns by adding support in their browsers for sending DNS queries over the encrypted HTTPS protocol.”

- “DNS over HTTPS means ISPs can’t spy on their users”

# Location Tracking

- https://www.wired.co.uk/article/amazon-sidewalk-apple-u1-networks
    - 28 September 2019
    - “Amazon and Apple are quietly building networks that know the location of everything”
        - “Amazon's new Sidewalk protocol and Apple's experiments with ultra-wideband signal a new battleground that gets Amazon out of the house and Apple inside it”
- “Wi-Fi Hotspot Tracking” by Bruce Schneier 10 October 2019:
    - "Wi-Fi hotspots can track your location, even if you don't connect to them. This is because your phone or computer broadcasts a unique MAC address.”
    - “The defence is to turn Wi-Fi off on your phone when you're not using it.”

# Tracking by Smart TVs

- https://twitter.com/random_walker/status/1177570679232876544

- “When we watch TV, our TVs watch us back and track our habits. This practice has exploded recently since it hasn’t faced much public scrutiny. But in the last few days, not one but *three* papers have dropped that uncover the extent of tracking on TVs.”

- “The first paper looked at Roku and Amazon Fire TV. These platforms let you subscribe to “channels”, which are basically apps. As you can guess, they are loaded with trackers. Doubleclick alone is on 97.5% of Roku channels.”

- “There are some channels with over 50 trackers. Also, the majority of trackers were able to grab a unique ID such as MAC address. A few channels leaked email addresses to trackers and many leaked video titles—often unencrypted, so your viewing history is exposed on the network. “

- “Some of their findings are what you’d intuitively expect: devices made by Chinese companies tend to talk to Chinese servers. Others findings are more surprising: Nearly all TVs they tested contacted Netflix, even though they never configured any TV with a Netflix account (?!?!) “

- Three academic papers

# Cloud cams

- https://www.bloomberg.com/news/articles/2019-10-10/is-amazon-watching-you-cloud-cam-footage-reviewed-by-humans

- Amazon Workers May Be Watching Your Cloud Cam Home Footage

- Teams in India and Romania use video snippets sent by customers for troubleshooting purposes and to train artificial intelligence algorithms.

- Nowhere in the Cloud Cam user terms and conditions does Amazon explicitly tell customers that human beings are training the algorithms behind their motion detection software.

- And despite Amazon’s insistence that all the clips are provided voluntarily, according to two of the people, the teams have picked up activity homeowners are unlikely to want shared, including rare instances of people having sex.

# How to Set Your Google Data to Self-Destruct

- https://www.nytimes.com/2019/10/02/technology/personaltech/google-data-self-destruct-privacy.html?

- “Google has now given us an option to set search and location data to automatically disappear after a certain time. We should all use it.”

# Gamers propose punishing Blizzard for its anti-Hong Kong partisanship by flooding it with GDPR requests

- Being a global multinational sure is hard! Yesterday, World of Warcraft maker Blizzard faced global criticism after it disqualified a high-stakes tournament winner over his statement of solidarity with the Hong Kong protests -- Blizzard depends on mainland China for a massive share of its revenue and it can't afford to offend the Chinese state.

- Today, outraged games on Reddit's /r/hearthstone forum are scheming a plan to flood Blizzard with punishing, expensive personal information requests under the EU's expansive General Data Privacy Regulation -- Blizzard depends on the EU for another massive share of its revenue and it can't afford the enormous fines it would face if it failed to comply with these requests, which take a lot of money and resource to fulfill.

- https://boingboing.net/2019/10/08/ddos-gdpr.html

# Screening all photos for the presence of children and bare skin

- https://www.swissinfo.ch/eng/pornography-screening_whatsapp-facebook-photos/45263836 29 September 2019

- “Harmless vacation photo or criminal content? Swiss federal police need to make this decision thousands of times per year as US platforms send them images posted online and shared via private message.”

- “According to the SonntagsZeitungexternal link Sunday newspaper, the Swiss federal police (FedPol)external link received 9,000 pictures last year. Of these, about 10% were of a criminal nature. The rest were ordinary photos, such as families relaxing at the beach. Critics complain that the automated system lacks transparency and accountability, and is tantamount to mass surveillance.”

# E-Sports tickets

- https://www.ccn.com/fifa-20-data-breach-ea-privacy/

- Latest FIFA 20 Data Breach Shows EA Doesn’t Care About Your Privacy

- Yesterday, EA opened up registrations for its latest eSports venture, FIFA 20 Global Series, this year’s iteration of a season-long series of competitive events leading to the FIFA eWorld Cup.

- Shortly afterward, players began reporting that they could access the details of other players who had already signed-up upon clicking the verification link sent to them after registering. The data included email addresses, gamer tags, country of residence, and date of birth.

- Users took to Twitter to voice their concern;

- EA took down the registration page for the FIFA 20 Global Series soon after.

- However, the damage was already done. Twitter users reported desperately failing to regain ownership of their accounts via EA’s two-factor-authorization system, and receiving unsolicited verification codes.