Privacy Technologies, Law and Policy

1 June 2021

Dr Michael Veale

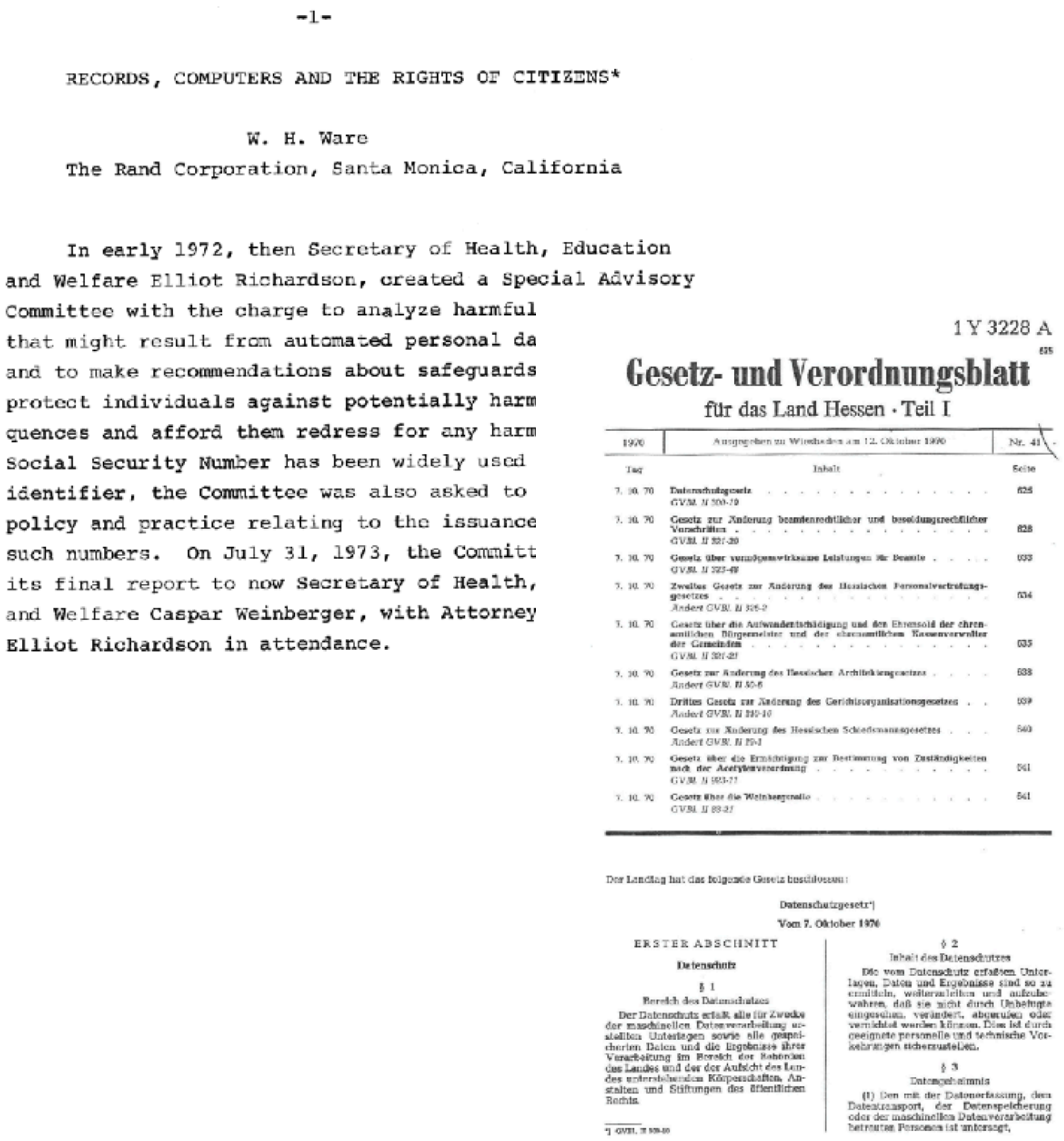
Lecturer in Digital Rights and Regulation

Faculty of Laws, University College London

A Short History of Data Protection Law

History of Data Protection

- **1970s**
  - Secretary's Advisory Committee on Automated Personal Data Systems at the US Department of Health, Education and Welfare (1972)
  - Data protection law in Hesse (1970); Sweden (1973); Rhineland-Palatinate (1974); Germany (1977); France (1978)
  - Many of these laws were concerned with government-run databanks.



-1-

RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS*

W. H. Ware
The Rand Corporation, Santa Monica, California

In early 1972, then Secretary of Health, Education and Welfare Elliot Richardson, created a Special Advisory Committee with the charge to analyze harmful that might result from automated personal da and to make recommendations about safeguards protect individuals against potentially harm quences and afford them redress for any harm Social Security Number has been widely used identifier, the Committee was also asked to policy and practice relating to the issuance such numbers. On July 31, 1973, the Committ its final report to now Secretary of Health, and Welfare Caspar Weinberger, with Attorney Elliot Richardson in attendance.

1 Y 3228 A

625

Gesetz- und Verordnungsblatt

für das Land Hessen · Teil I

1970	Ausgegeben zu Wiesbaden am 12. Oktober 1970	Nr. 41

Tag	Inhalt	Seite
7. 10. 70	Datenschutzgesetz GVBl. II 300-10	625
7. 10. 70	Gesetz zur Änderung beamtenrechtlicher und besoldungsrechtlicher Vorschriften GVBl. II 321-20	628
7. 10. 70	Gesetz über vermögenswirksame Leistungen für Beamte GVBl. II 323-49	633
7. 10. 70	Zweites Gesetz zur Änderung des Hessischen Personalvertretungsgesetzes Ändert GVBl. II 326-2	634
7. 10. 70	Gesetz über die Aufwandsentschädigung und den Ehrensold der ehrenamtlichen Bürgermeister und der ehrenamtlichen Kassenverwalter der Gemeinden GVBl. II 331-21	635
7. 10. 70	Gesetz zur Änderung des Hessischen Architektengesetzes Ändert GVBl. II 50-6	638
7. 10. 70	Drittes Gesetz zur Änderung des Gerichtsorganisationsgesetzes Ändert GVBl. II 210-10	639
7. 10. 70	Gesetz zur Änderung des Hessischen Schiedsmannsgesetzes Ändert GVBl. II 19-1	640
7. 10. 70	Gesetz über die Ermächtigung zur Bestimmung von Zuständigkeiten nach der Acetylenverordnung GVBl. II 503-77	641
7. 10. 70	Gesetz über die Weinbergrolle GVBl. II 83-23	641

Der Landtag hat das folgende Gesetz beschlossen:

Datenschutzgesetz*)

Vom 7. Oktober 1970

ERSTER ABSCHNITT

Datenschutz

§ 1

Bereich des Datenschutzes

Der Datenschutz erfaßt alle für Zwecke der maschinellen Datenverarbeitung erstellten Unterlagen sowie alle gespeicherten Daten und die Ergebnisse ihrer Verarbeitung im Bereich der Behörden des Landes und der der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts.

§ 2

Inhalt des Datenschutzes

Die vom Datenschutz erfaßten Unterlagen, Daten und Ergebnisse sind so zu ermitteln, weiterzuleiten und aufzubewahren, daß sie nicht durch Unbefugte eingesehen, verändert, abgerufen oder vernichtet werden können. Dies ist durch geeignete personelle und technische Vorkehrungen sicherzustellen.

§ 3

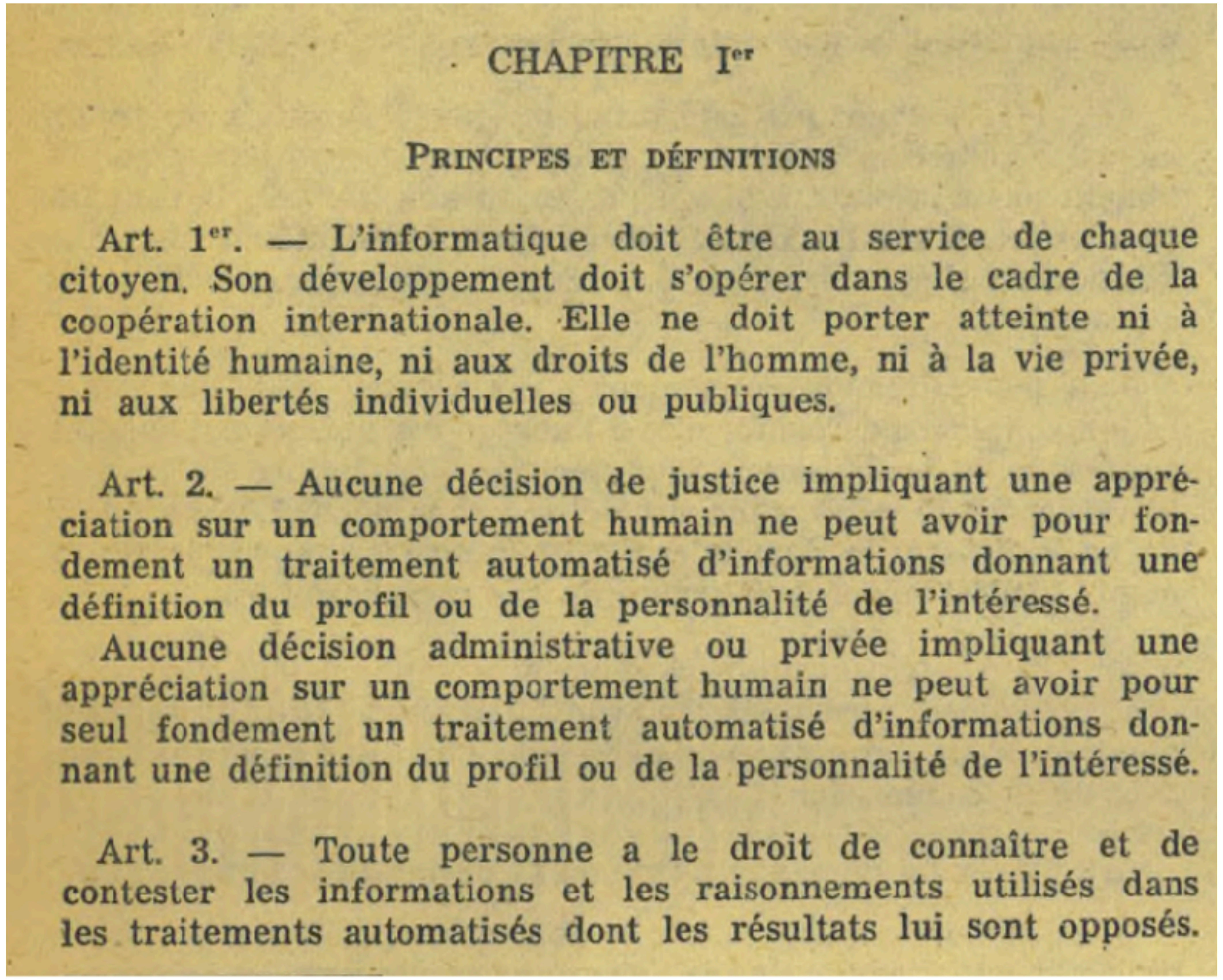
Datengeheimnis

(1) Den mit der Datenerfassung, dem Datentransport, der Datenspeicherung oder der maschinellen Datenverarbeitung betrauten Personen ist untersagt,

*) GVBl. II 300-10

Data rights

- The French law in particular went beyond some independent regulator supervising data processing to include **data rights**.



CHAPITRE Ier

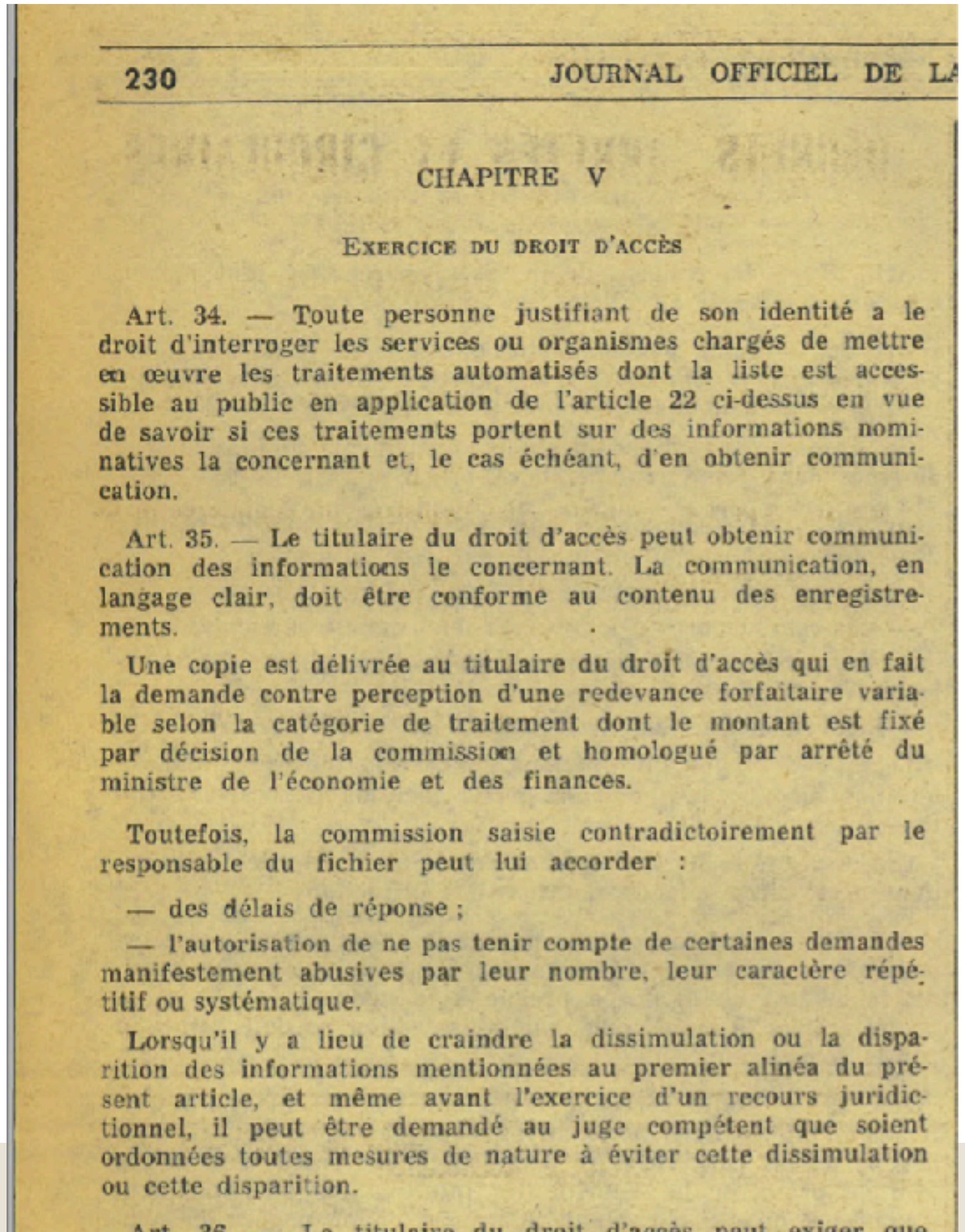
PRINCIPES ET DÉFINITIONS

Art. 1er. — L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Art. 2. — Aucune décision de justice impliquant une appréciation sur un comportement humain ne peut avoir pour fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé.

Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé.

Art. 3. — Toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements automatisés dont les résultats lui sont opposés.



230 JOURNAL OFFICIEL DE LA

CHAPITRE V

EXERCICE DU DROIT D'ACCÈS

Art. 34. — Toute personne justifiant de son identité a le droit d'interroger les services ou organismes chargés de mettre en œuvre les traitements automatisés dont la liste est accessible au public en application de l'article 22 ci-dessus en vue de savoir si ces traitements portent sur des informations nominatives la concernant et, le cas échéant, d'en obtenir communication.

Art. 35. — Le titulaire du droit d'accès peut obtenir communication des informations le concernant. La communication, en langage clair, doit être conforme au contenu des enregistrements.

Une copie est délivrée au titulaire du droit d'accès qui en fait la demande contre perception d'une redevance forfaitaire variable selon la catégorie de traitement dont le montant est fixé par décision de la commission et homologué par arrêté du ministre de l'économie et des finances.

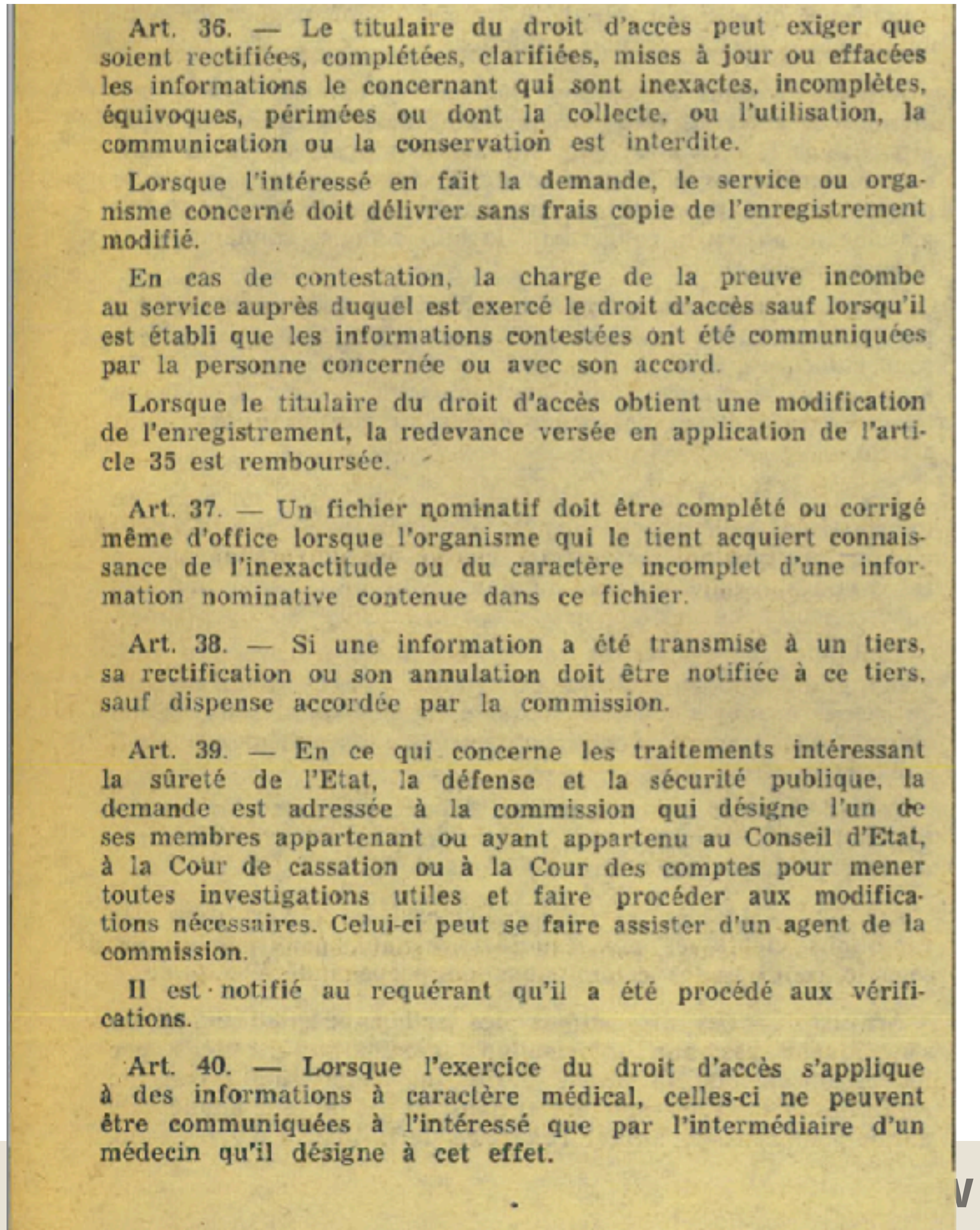
Toutefois, la commission saisie contradictoirement par le responsable du fichier peut lui accorder :

— des délais de réponse ;

— l'autorisation de ne pas tenir compte de certaines demandes manifestement abusives par leur nombre, leur caractère répétitif ou systématique.

Lorsqu'il y a lieu de craindre la dissimulation ou la disparition des informations mentionnées au premier alinéa du présent article, et même avant l'exercice d'un recours juridictionnel, il peut être demandé au juge compétent que soient ordonnées toutes mesures de nature à éviter cette dissimulation ou cette disparition.

Art. 36. — Le titulaire du droit d'accès peut exiger que



Art. 36. — Le titulaire du droit d'accès peut exiger que soient rectifiées, complétées, clarifiées, mises à jour ou effacées les informations le concernant qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte, ou l'utilisation, la communication ou la conservation est interdite.

Lorsque l'intéressé en fait la demande, le service ou organisme concerné doit délivrer sans frais copie de l'enregistrement modifié.

En cas de contestation, la charge de la preuve incombe au service auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les informations contestées ont été communiquées par la personne concernée ou avec son accord.

Lorsque le titulaire du droit d'accès obtient une modification de l'enregistrement, la redevance versée en application de l'article 35 est remboursée.

Art. 37. — Un fichier nominatif doit être complété ou corrigé même d'office lorsque l'organisme qui le tient acquiert connaissance de l'inexactitude ou du caractère incomplet d'une information nominative contenue dans ce fichier.

Art. 38. — Si une information a été transmise à un tiers, sa rectification ou son annulation doit être notifiée à ce tiers, sauf dispense accordée par la commission.

Art. 39. — En ce qui concerne les traitements intéressant la sûreté de l'Etat, la défense et la sécurité publique, la demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour mener toutes investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission.

Il est notifié au requérant qu'il a été procédé aux vérifications.

Art. 40. — Lorsque l'exercice du droit d'accès s'applique à des informations à caractère médical, celles-ci ne peuvent être communiquées à l'intéressé que par l'intermédiaire d'un médecin qu'il désigne à cet effet.

International Instruments

- **OECD**: Guidelines on international policy on the protection of privacy and transborder flows of personal data (1980)
- **Council of Europe**: Convention 108 (1981)
- **European Union**: Data Protection Directive 1995; Article 7 and 8 of the Charter of Fundamental Rights (2000/2009); General Data Protection Regulation 2016
- Now: Over 150 countries with some form of privacy law

How to read (European) privacy law

- **Text of the GDPR** http://data.europa.eu/eli/reg/2016/679/oj
  - Recitals and Articles
  - Also other laws (Law Enforcement Directive; ePrivacy Directive; national implementations)
- **Case law**
  - European Court of Justice
  - National courts
  - European Court of Human Rights (and European Convention on Human Rights)
- **Guidance**
  - European Data Protection Board (EDPB)
  - National Regulators

Structure of Data Protection Law and Enforcement

Sources of Law

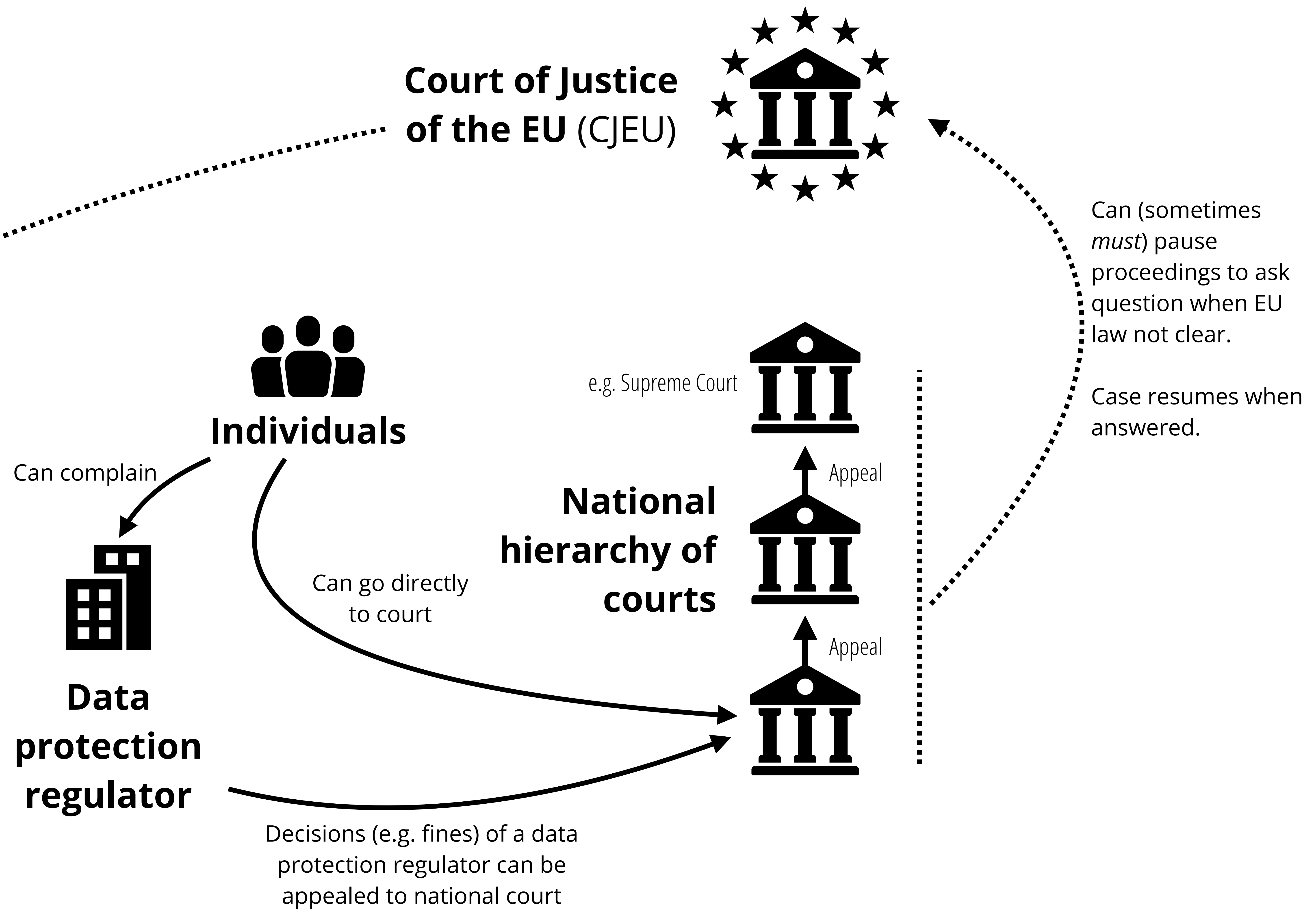
GDPR
EU Regulation, applies without being put in national law.

Judgements of the CJEU
(And judgements of national higher courts bind lower ones in common law systems)

National data protection law
Contextualises the GDPR

Sources of "Soft" Law

Guidance from regulators
National or collaborative across EU, e.g. EDPB



Court of Justice of the EU (CJEU)

Can (sometimes *must*) pause proceedings to ask question when EU law not clear.

Case resumes when answered.

Individuals

Can complain

Can go directly to court

Data protection regulator

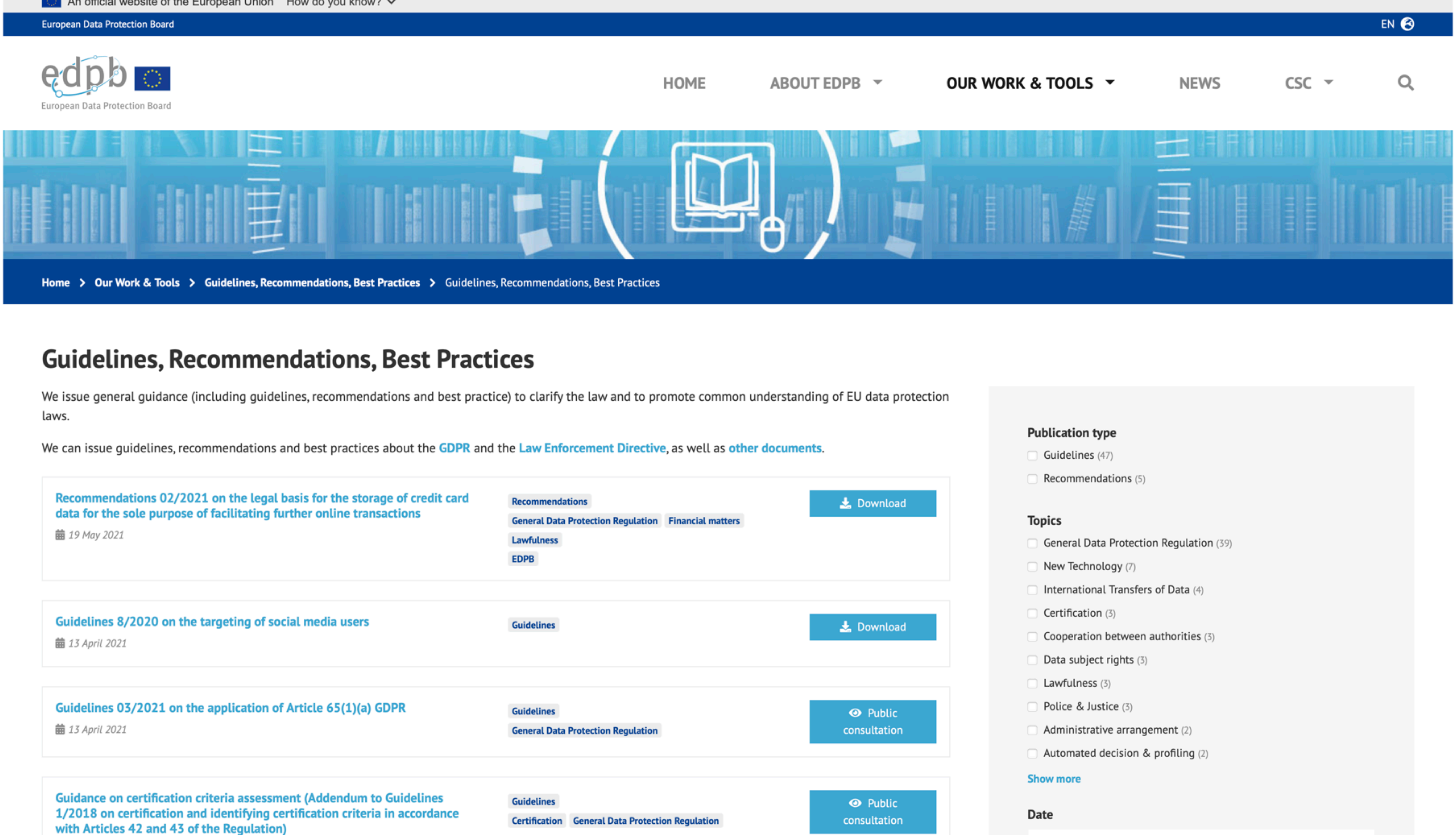
National hierarchy of courts

e.g. Supreme Court

Appeal

Appeal

Decisions (e.g. fines) of a data protection regulator can be appealed to national court



An official website of the European Union How do you know?
European Data Protection Board
EN
edpb
European Data Protection Board
HOME
ABOUT EDPB
OUR WORK & TOOLS
NEWS
CSC
Home > Our Work & Tools > Guidelines, Recommendations, Best Practices > Guidelines, Recommendations, Best Practices

Guidelines, Recommendations, Best Practices

We issue general guidance (including guidelines, recommendations and best practice) to clarify the law and to promote common understanding of EU data protection laws.

We can issue guidelines, recommendations and best practices about the GDPR and the Law Enforcement Directive, as well as other documents.

Recommendations 02/2021 on the legal basis for the storage of credit card data for the sole purpose of facilitating further online transactions 19 May 2021	Recommendations General Data Protection Regulation Financial matters Lawfulness EDPB	Download
Guidelines 8/2020 on the targeting of social media users 13 April 2021	Guidelines	Download
Guidelines 03/2021 on the application of Article 65(1)(a) GDPR 13 April 2021	Guidelines General Data Protection Regulation	Public consultation
Guidance on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation)	Guidelines Certification General Data Protection Regulation	Public consultation

Publication type

- □ Guidelines (47)
- □ Recommendations (5)

Topics

- □ General Data Protection Regulation (39)
- □ New Technology (7)
- □ International Transfers of Data (4)
- □ Certification (3)
- □ Cooperation between authorities (3)
- □ Data subject rights (3)
- □ Lawfulness (3)
- □ Police & Justice (3)
- □ Administrative arrangement (2)
- □ Automated decision & profiling (2)

Show more

Date

Data Protection ≠ Privacy

Charter of Fundamental Rights of the European Union

Article 7

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Definitions, Principles and Rights in Data Protection Law

Data controllers, data subjects, data processors

- Data controllers determine the purposes and means of the processing of personal data. Defined by what they do, not by a contractual decision.
- Data subjects are identified or identifiable natural persons to whom any information relate.
- Data processors: do what they are told by controllers.

Personal data and data processing

- Personal data: any information relating to an identified or identifiable natural person.
- Processing is broad!
  - [A]ny operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (art 4(2))

Scope of the law

- **Territorial scope: wide**
  - Any organisation in the world processing personal data of European residents.
  - Any organisation in Europe processing personal data of any natural person.
- **Material scope: personal data**
  - Not synonymous with the American term Personally Identifying Information (PII).
  - Also data that indirectly can identify you with other data that is reasonably available to other people or organisations in the world.
  - Smart meter data; hashed MAC addresses; location traces; browser fingerprints.
  - Exemption for “household” purposes (but narrow, see CJEU in *Lindqvist*)

Principle-based regulation

- processed lawfully, fairly and in a transparent manner in relation to the data subject (‘**lawfulness, fairness and transparency**’);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes […] (‘**purpose limitation**’);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘**data minimisation**’);
- accurate and, where necessary, kept up to date […] (‘**accuracy**’);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed […] (‘**storage limitation**’);
- processed in a manner that ensures appropriate security […] (‘**integrity and confidentiality**’).
- The controller shall be responsible for, and be able to demonstrate compliance […] (‘**accountability**’)

GDPR art 5.

Legal bases for processing personal data

- **Consent** for a specific purpose
  - Must be as easy to withdraw as to give, disaggregated and not “bundled” up. See art 7 for conditions.
- Processing is necessary for:
  - the **performance of a contract**
  - **legitimate interests of the controller/another**, balanced against those of the data subject
  - **vital interests** (largely about life in peril)
  - **legal obligation** (specific industries e.g. finance)
  - **task in the public interest**/official authority (e.g. tax fraud detection)

GDPR art 6.

Data protection rights

- Right to be informed
- Right of access
- Right to data portability
- Right to rectify data
- Right of erasure
- Right to object to processing
- Right to restrict processing
- Right not to be subject to automated decision-making
- Rights to lodge a complaint; to a judicial remedy against a DPA or controller/processor

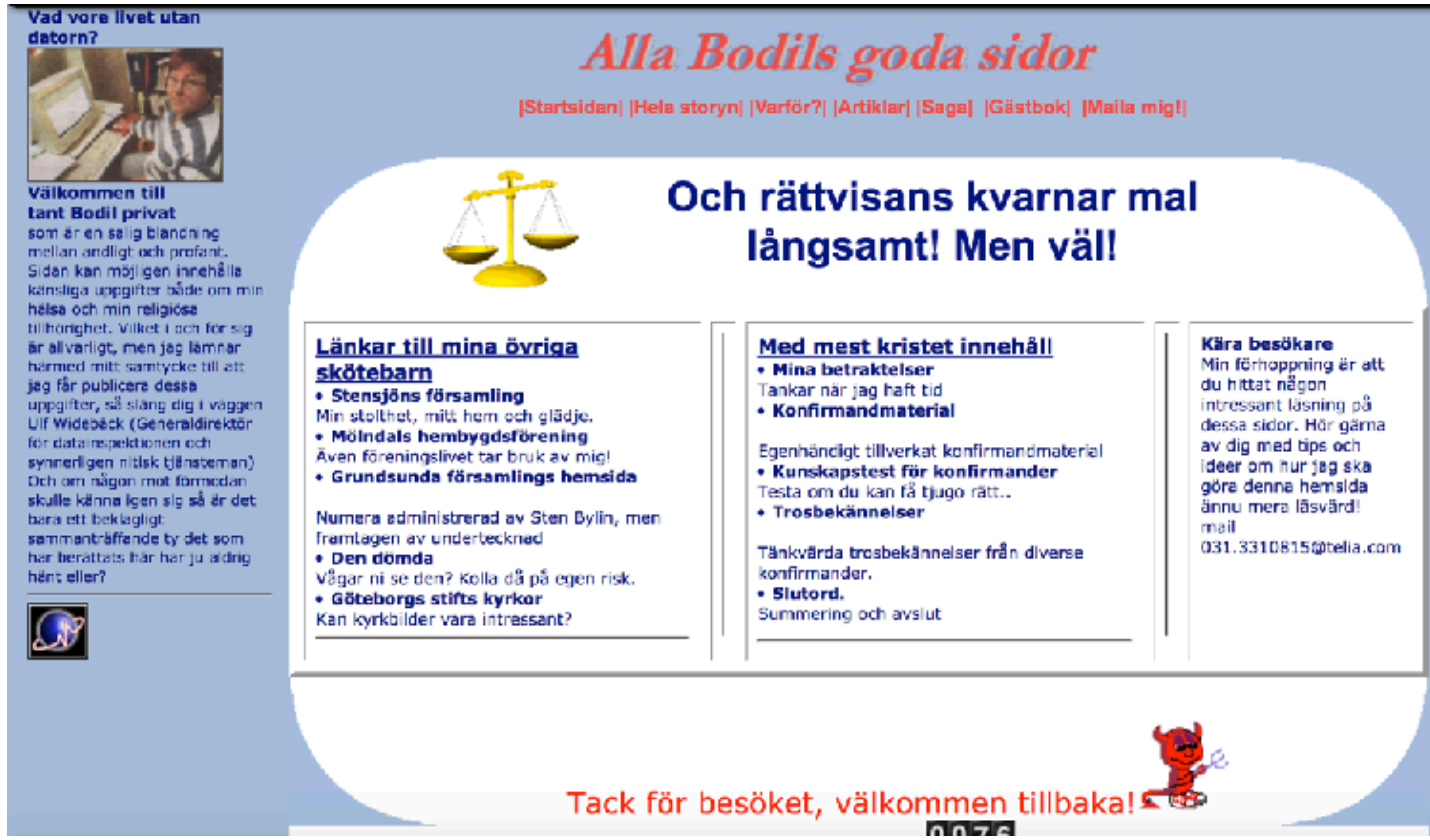
Zoom in: Cases around personal data

personal data is any information relating to an identified or identifiable natural person.

Broad definition of personal data I

Case C-101/01 *Lindqvist* EU:C:2003:596

- **Bodil Lindqvist** worked in a church in the south of Sweden. She was learning HTML and set up a personal webpage.
- She wrote a humorous page listing bios of her 18 colleagues (without asking them), including that one had a small foot injury. When she learned some colleagues did not appreciate them, she removed them.
- The Swedish public prosecutor brought criminal proceedings for not informing the Swedish DPA and processing sensitive data (medical injury). The proceedings were stayed in a CJEU referral.



Vad vore livet utan datorn?

Välkommen till tant Bodil privat
som är en salig blandning mellan andligt och profant. Sidan kan möjligen innehålla känsliga uppgifter både om min hälsa och min religiösa tillhörighet. Vilket i och för sig är allvarligt, men jag lämnar härmed mitt samtycke till att jag får publicera dessa uppgifter, så släng dig i väggen Ulf Widebäck (Generaldirektör för datainspektionen och synnerligen nitisk tjänsteman) Och om någon mot förmodan skulle känna igen sig så är det bara ett beklagligt sammanträffande ty det som har berättats här har ju aldrig hänt eller?

Alla Bodils goda sidor

|Startsidan| |Hela storyn| |Varför?| |Artiklar| |Saga| |Gästbok| |Maila mig!|

Och rättvisans kvarnar mal långsamt! Men väl!

Länkar till mina övriga skötebarn
- **Stensjöns församling**
Min stolthet, mitt hem och glädje.
- **Mölndals hembygdsförening**
Även föreningslivet tar bruk av mig!
- **Grundsunda församlings hemsida**

Numera administrerad av Sten Bylin, men framlagen av undertecknad
- **Den dömda**
Vågar ni se den? Kolla då på egen risk.
- **Göteborgs stifts kyrkor**
Kan kyrkbilder vara intressant?

Med mest kristet innehåll
- **Mina betraktelser**
Tankar när jag haft tid
- **Konfirmandmaterial**

Egenhändigt tillverkat konfirmandmaterial
- **Kunskapstest för konfirmander**
Testa om du kan få tjugo rätt..
- **Trosbekännelser**

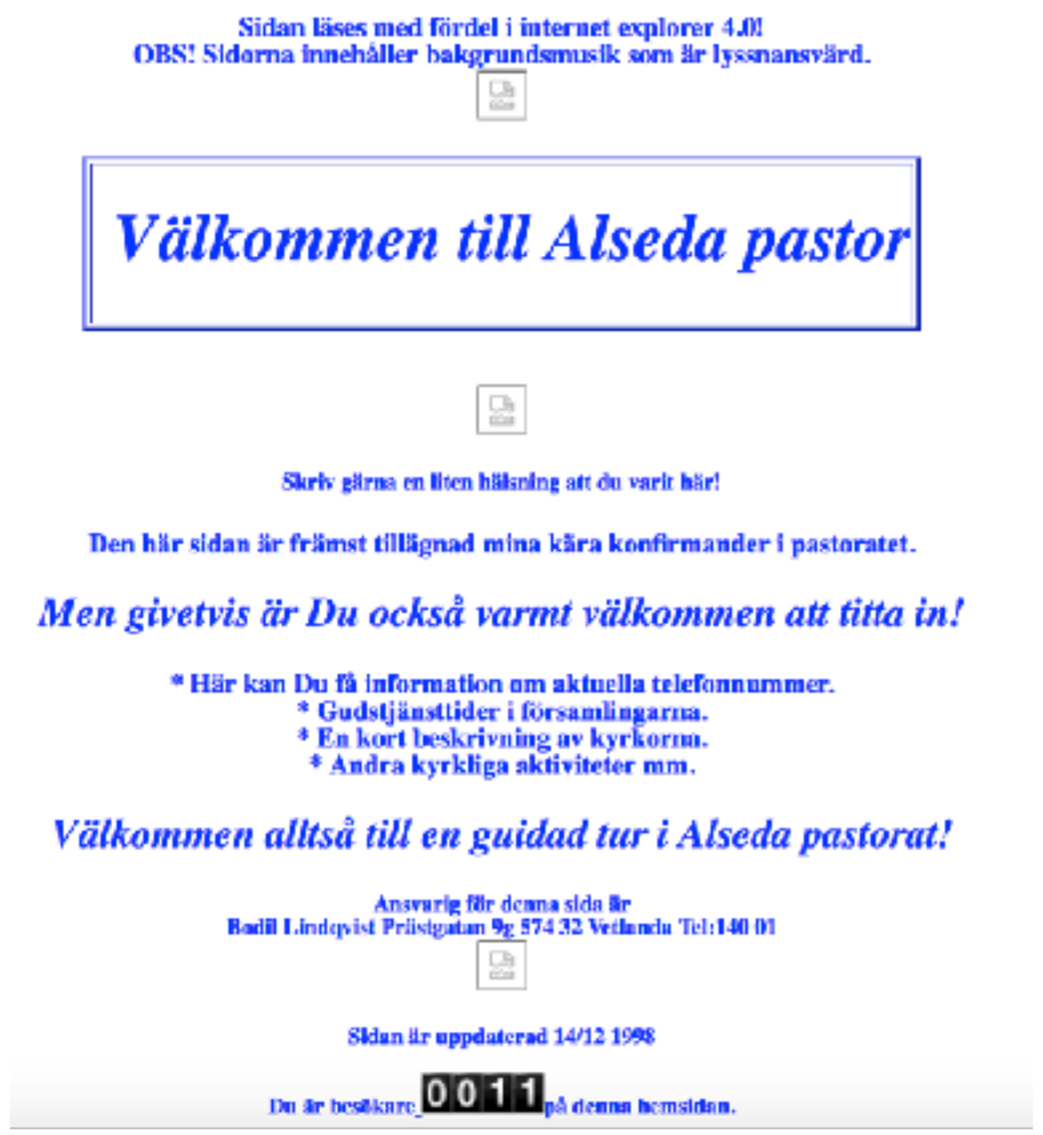
Tänkvärda trosbekännelser från diverse konfirmander.
- **Slutord.**
Summering och avslut

Kära besökare
Min förhoppning är att du hittat någon intressant läsning på dessa sidor. Hör gärna av dig med tips och ideer om hur jag ska göra denna hemsida ännu mera läsvärd!
mail
031.3310815@telia.com

Tack för besöket, välkommen tillbaka!

0076

Bodil Lindqvist



Sidan läses med fördel i internet explorer 4.0!
OBS! Sidorna innehåller bakgrundsmusik som är lyssnansvärd.

Välkommen till Alseda pastor

Skriv gärna en liten hälsning att du varit här!

Den här sidan är främst tillägnad mina kära konfirmander i pastoratet.

Men givetvis är Du också varmt välkommen att titta in!

* Här kan Du få information om aktuella telefonnummer.
* Gudstjänsttider i församlingarna.
* En kort beskrivning av kyrkorna.
* Andra kyrkliga aktiviteter mm.

Välkommen alltså till en guidad tur i Alseda pastorat!

Ansvarig för denna sida är
Bodil Lindqvist Prästgatan 9g 574 32 Vetlanda Tel:140 01

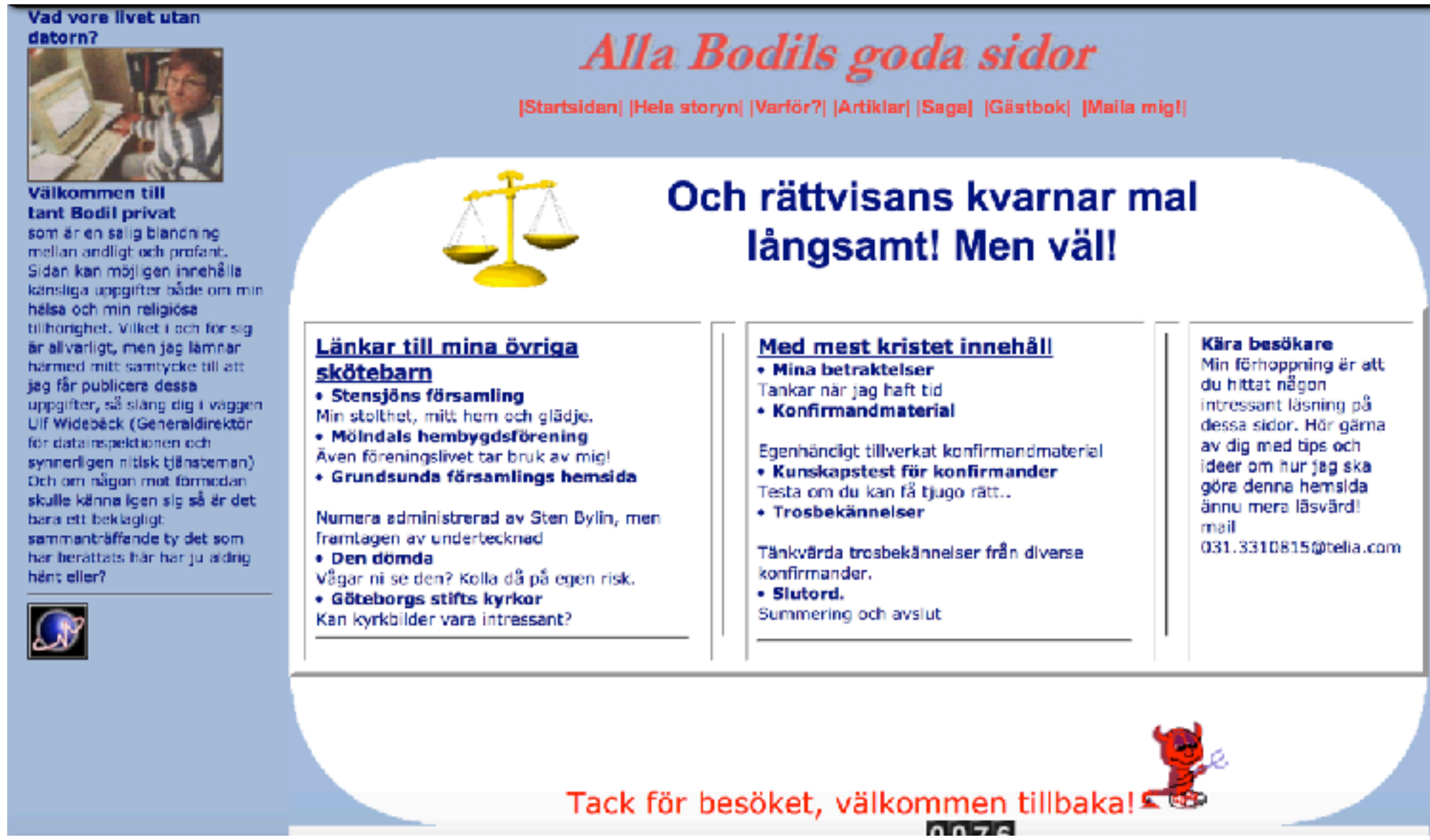
Sidan är uppdaterad 14/12 1998

Du är besökare 0011 på denna hemsidan.

Broad definition of personal data I

Case C-101/01 *Lindqvist* EU:C:2003:596

- **CJEU:**
  - the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means
  - Such processing of personal data is not covered by any of the exceptions in Article 3(2) of Directive 95/46. *(i.e. it is not "carried out by a natural person in the course of a purely personal or household activity")*



Vad vore livet utan datorn?

Välkommen till tant Bodil privat
som är en salig blandning mellan andligt och profant. Sidan kan möjligen innehålla känsliga uppgifter både om min hälsa och min religiösa tillhörighet. Vilket i och för sig är allvarligt, men jag lämnar härmed mitt samtycke till att jag får publicera dessa uppgifter, så släng dig i väggen Ulf Widebäck (Generaldirektör för datainspektionen och synnerligen nitisk tjänsteman) Och om någon mot förmodan skulle känna igen sig så är det bara ett beklagligt sammanträffande ty det som har berättats här har ju aldrig hänt eller?

Alla Bodils goda sidor

|Startsidan| |Hela storyn| |Varför?| |Artiklar| |Saga| |Gästbok| |Maila mig!|

Och rättvisans kvarnar mal långsamt! Men väl!

Länkar till mina övriga skötebarn
- **Stensjöns församling**
Min stolthet, mitt hem och glädje.
- **Mölndals hembygdsförening**
Även föreningslivet tar bruk av mig!
- **Grundsunda församlings hemsida**

Numera administrerad av Sten Bylin, men framlagen av undertecknad
- **Den dömda**
Vågar ni se den? Kolla då på egen risk.
- **Göteborgs stifts kyrkor**
Kan kyrkbilder vara intressant?

Med mest kristet innehåll
- **Mina betraktelser**
Tankar när jag haft tid
- **Konfirmandmaterial**

Egenhändigt tillverkat konfirmandmaterial
- **Kunskapstest för konfirmander**
Testa om du kan få tjugo rätt..
- **Trosbekännelser**

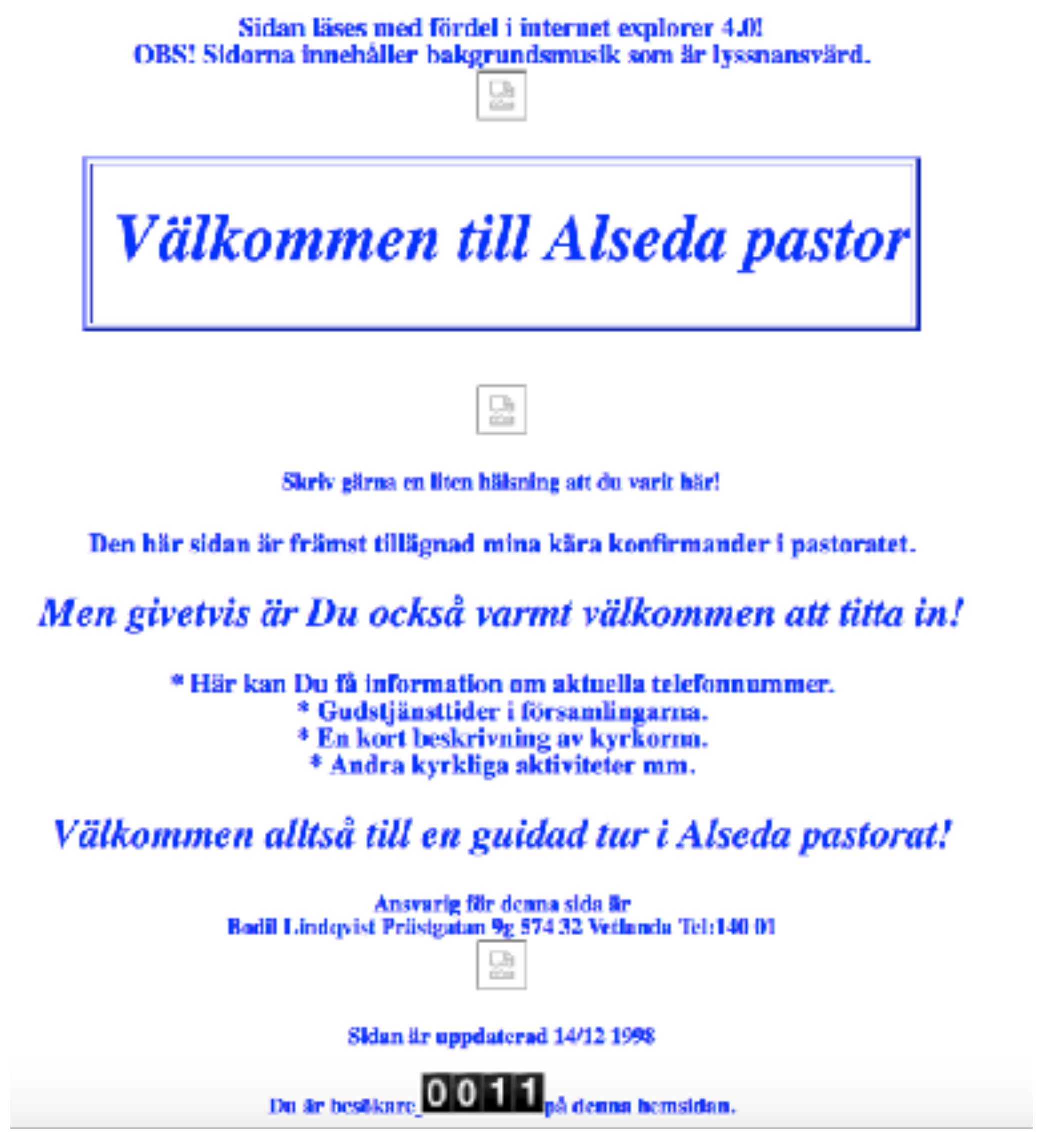
Tänkvärda trosbekännelser från diverse konfirmander.
- **Slutord.**
Summering och avslut

Kära besökare
Min förhoppning är att du hittat någon intressant läsning på dessa sidor. Hör gärna av dig med tips och ideer om hur jag ska göra denna hemsida ännu mera läsvärd!
mail
031.3310815@telia.com

Tack för besöket, välkommen tillbaka!

0076

Bodil Lindqvist



Sidan läses med fördel i internet explorer 4.0!
OBS! Sidorna innehåller bakgrundsmusik som är lyssnansvärd.

Välkommen till Alseda pastor

Skriv gärna en liten hälsning att du varit här!

Den här sidan är främst tillägnad mina kära konfirmander i pastoratet.

Men givetvis är Du också varmt välkommen att titta in!

* Här kan Du få information om aktuella telefonnummer.
* Gudstjänsttider i församlingarna.
* En kort beskrivning av kyrkorna.
* Andra kyrkliga aktiviteter mm.

Välkommen alltså till en guidad tur i Alseda pastorat!

Ansvarig för denna sida är
Bodil Lindqvist Prästgatan 9g 574 32 Vetlanda Tel:140 01

Sidan är uppdaterad 14/12 1998

Du är besökare 0011 på denna hemsidan.

Broad definition of personal data II

Case C-582/14 *Breyer* ECLI:EU:C:2016:779

- Activist Patrick Breyer visited German federal sites who stored his (dynamic) IP address for the purposes of stopping DDoS attacks. He objected to the retention of this data.
- Static IP addresses identify a computer; are clearly PD (already determined in *Scarlet Extended*.) **Identified** natural persons.
- Dynamic IP addresses however change regularly, and need information to link to a subscriber (e.g. held by an ISP). **Identifiable?**
- The Court found that it may not be "reasonably likely" if connecting these data were prohibited by law. In this case, it was not, and as such, Breyer's PD was being processed.

Broad definition of personal data III

Case C–434/16 *Nowak* ECLI:EU:C:2017:994

- Peter Nowak wished to use the right of access to have a copy of his annotated exam script.
- Recall that personal data is any information relating to an identified or identifiable natural person.
- Court held that the written content and comments were personal data under this provision.
- “Relates to” considered by the Court “by reason of its content, purpose or effect”. Opinions can be personal data
  - although they may relate to more than one person which can cause trouble

Identifiability to individuation

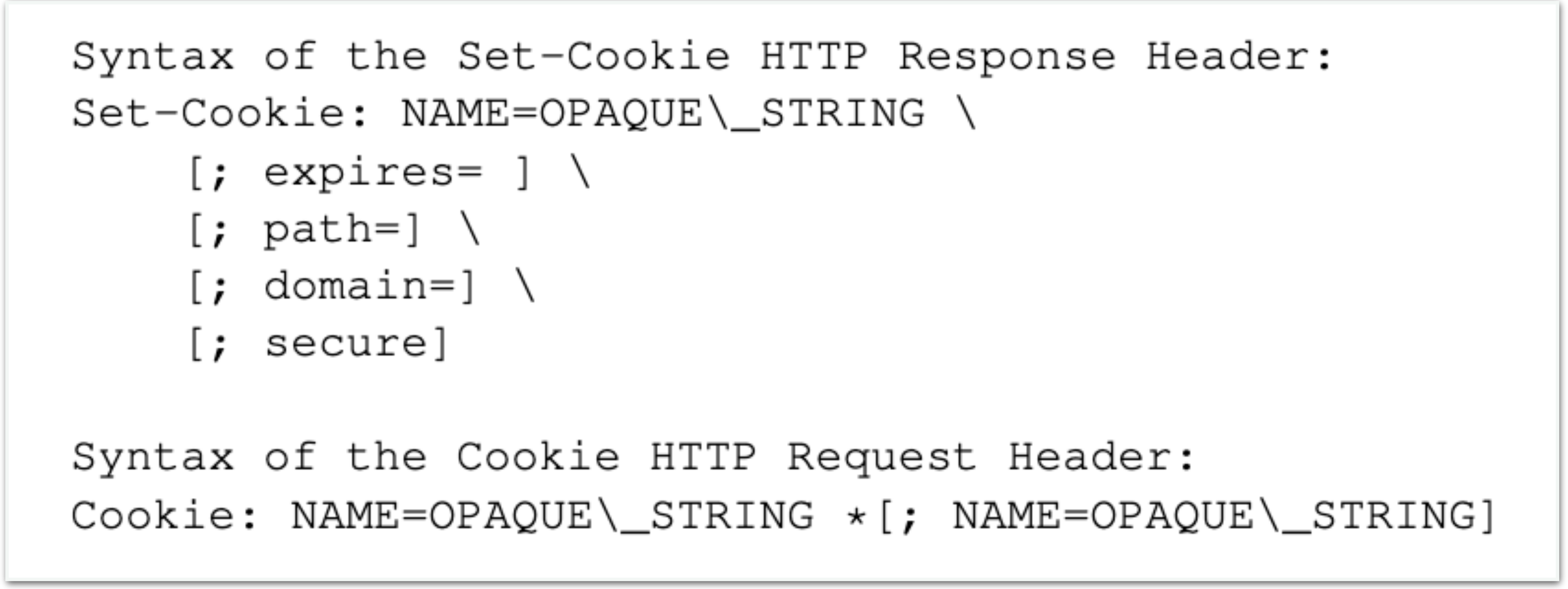
Bridges and *Vidal-Hall*

- Sometimes, establishing identifiability in a specific case might be hard. Two UK cases illustrate this:
    - Cookie data in *Vidal-Hall v Google Inc* [2015] EWCA Civ 311.
    - Facial recognition data in *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police and Secretary of State for the Home Department* [2019] EWHC 2341 (Admin) (and the successful subsequent appeal).
- Courts in the UK sympathetic towards looking whether the *purpose* of a system (or business model) is to *individuate* people.
- Consequences for PETs?

Online Tracking and the Law

A short history of Web tracking

- In the early 90s, the Web was ‘stateless’ — it had no *memory of its visitors*.
- **Cookies** were invented to solve this problem: they are simply **text placed on your browser by a web server that a server can look at later**.



```
Syntax of the Set-Cookie HTTP Response Header:
Set-Cookie: NAME=OPAQUE\_STRING \
    [; expires= ] \
    [; path=] \
    [; domain=] \
    [; secure]

Syntax of the Cookie HTTP Request Header:
Cookie: NAME=OPAQUE\_STRING *[; NAME=OPAQUE\_STRING]
```

First proposal for state management on the web (Apr. 18, 1995)

Webpage complexity grows

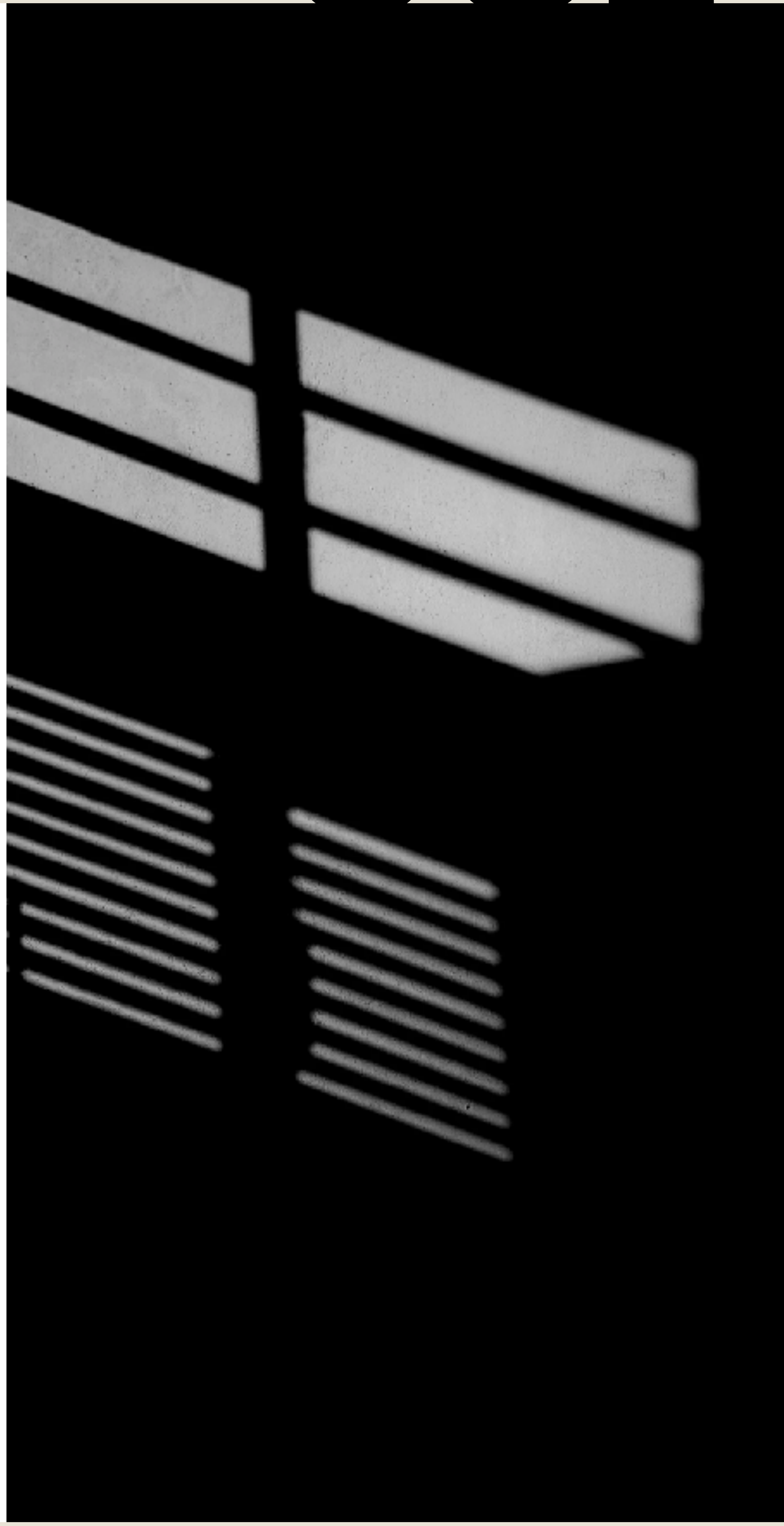
- In the early days of the Web, all content on a webpage came from the same **server**.
- An early, popular browser, **Netscape Navigator**, introduced the function of rendering two webpages in a single browsing window in 1996 (frames).
- This created a problem: could the second website access the cookies the first had laid?

The same origin policy

- The solution — the Same Origin Policy.
- Cookies only accessible by servers that share features (particularly the domain) of the one that laid them.
- A user visiting ucl.ac.uk should expect only ucl.ac.uk cookies to be read — not kcl.ac.uk cookies.

Crafty workarounds

- Didn't fix the problem for long:
  - Websites started calling many distinct servers. Used to be 1, now 100s — because a website would instruct your computer to query many domains.
  - These many domains collaborate to share information about users' Web usage and more — called Cookie Syncing.
- Google calls home with unique identifiers for at least 28% of all web page loads, while Facebook does the same for approximately 15%. The proportion is significantly higher in certain sectors, such as news, compared to others, such as banking.*
- Collaboration between trackers means that even under conservative estimates, 53 firms observe more than 91% of users' browsing behaviour.**



*Arjaldo Karaj and others, 'WhoTracks.Me: Shedding Light on the Opaque World of Online Tracking' [2018] arXiv:180408959, 8;

** Muhammad Ahmad Bashir and Christo Wilson, 'Diffusion of User Tracking Data in the Online Advertising Ecosystem' (2018) 2018 Proceedings on Privacy Enhancing Technologies 85.

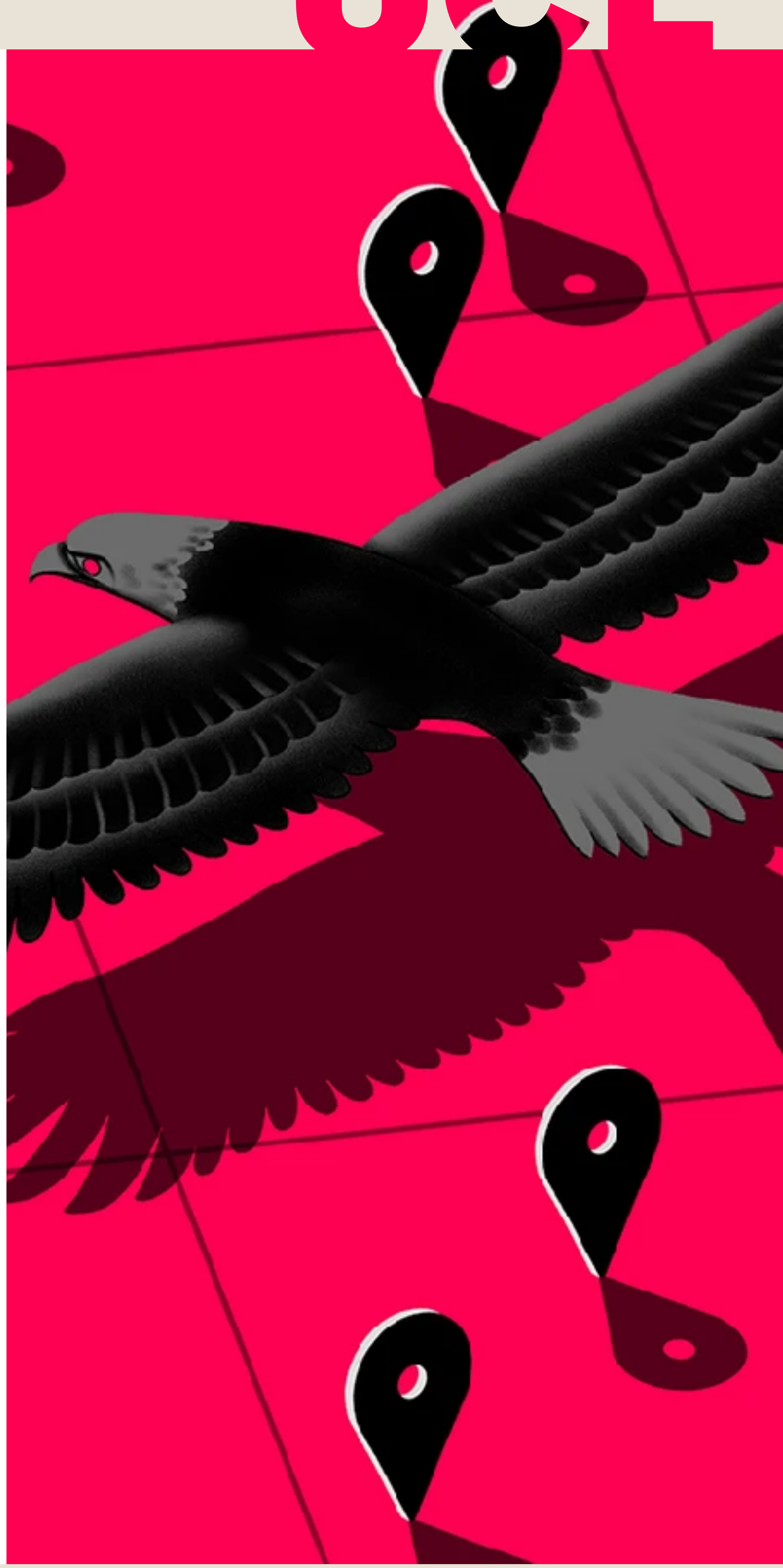
Apps are pretty bad

- Users have more ability to control the Web, through browsers. For apps, they have almost none.
- One recent study identified 2,121 separate advertising tracking services in apps in the Android ecosystem, which can be grouped by ownership into approximately 292 parent organisations.*
- Another study found that 88.4% of apps contained a tracker owned by Alphabet (Google), 42.6% by Facebook, 33.9% by Twitter, 26.3% by Verizon and 22.2% by Microsoft. 30% of News apps, 28% of Family apps, and 25% of Gaming & Entertainment apps contain trackers from more than ten distinct tracker companies.**

*Abbas Razaghpanah and others, 'Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem' (2018) 13–14 <http://eprints.networks.imdea.org/1744/>; **Reuben Binns and others, 'Third Party Tracking in the Mobile Ecosystem', Proceedings of the 10th ACM Conference on Web Science (ACM 2018) 27

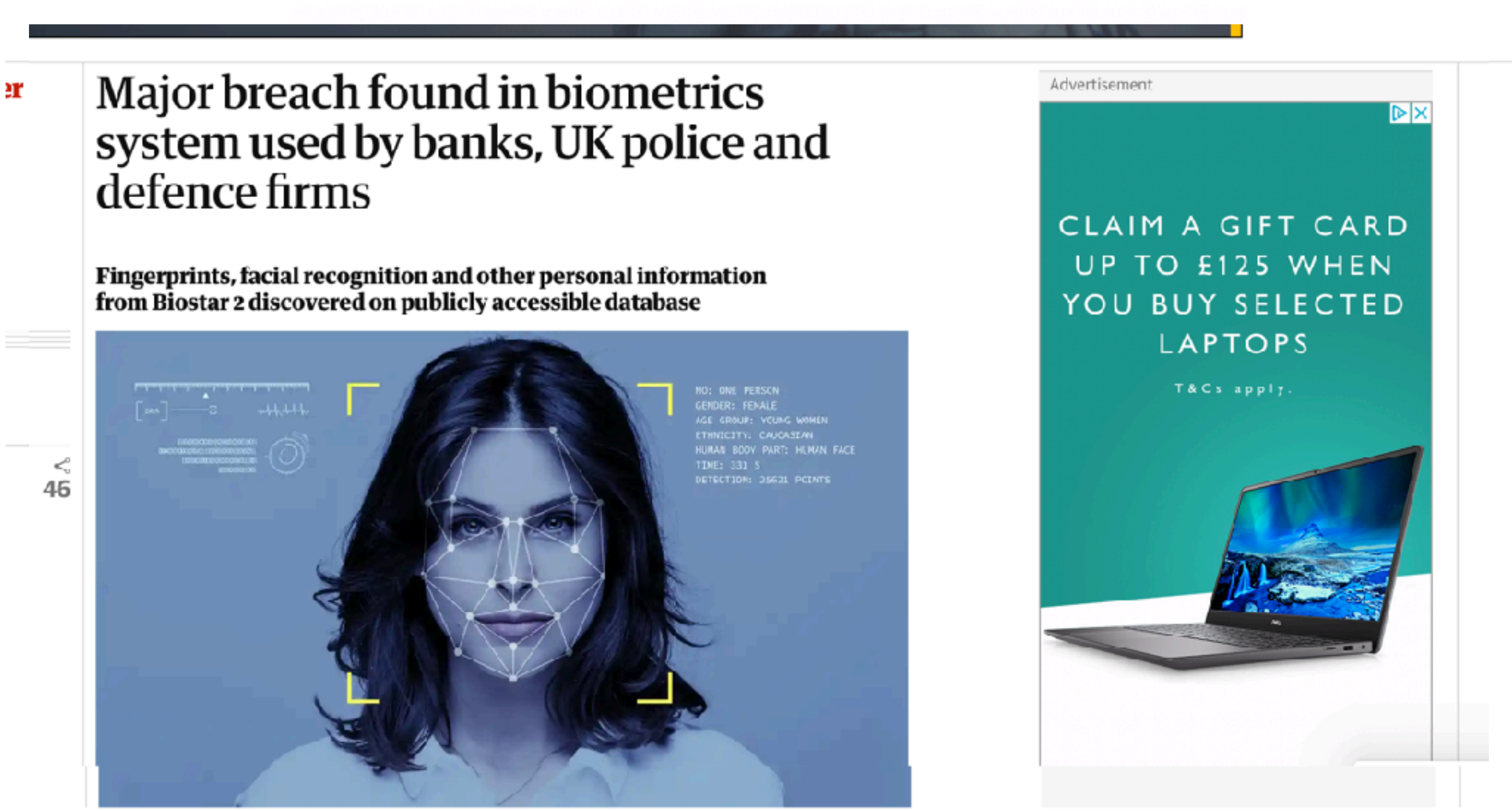
This data isn't just used for advertising

- VICE reported this November that the US military is buying location data harvested from trackers in apps, including a Quar'an and prayer time app downloaded by 98m Muslims around the world; a Craigslist searching app and a spirit level app designed to help with fitting furniture.
- One of the vendors, X-Mode, has also demonstrated how its data can be used to follow where people in COVID-19 hotspots travelled to after potentially exposing one another to the coronavirus.



https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x

But when they are used for ads, it’s pretty bad too.



Major breach found in biometrics system used by banks, UK police and defence firms

Fingerprints, facial recognition and other personal information from Biostar 2 discovered on publicly accessible database

Advertisement

CLAIM A GIFT CARD UP TO £125 WHEN YOU BUY SELECTED LAPTOPS

T&Cs apply.

Real-Time Bidding

From about 2010, automated auctions for your eyeballs.

Data protection-free zone
Visitor
Website
Supply-side platform
Ad exchange
Demand-side platforms
Marketers
Requests page
Serves page
Requests ad
Sends personal data to SSP
Requests ad
100s/1,000s of bid requests
Retail data
Winning bid
Serves ad

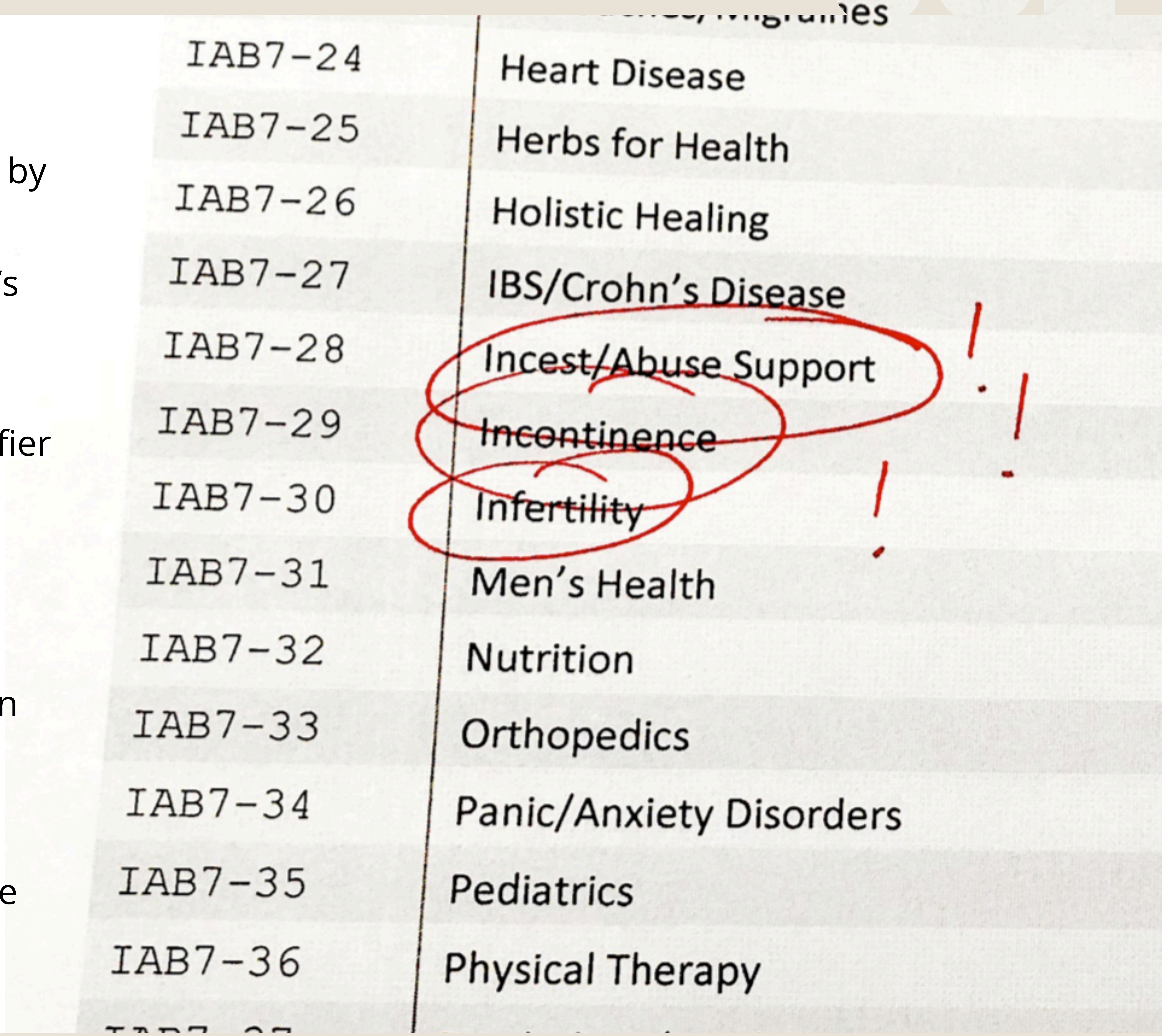
Diagram: The Economist

@mikarv

Data sent to bidders each time this happens

- Site
  - URL of the site being visited
  - Site category or topic
- Device
  - Operating system
  - Browser software and version
  - Device manufacturer, model
  - Mobile provider
  - Screen dimensions

- User
  - Unique identifiers set by vendor and/or buyer.
  - Advertising exchange's cookie ID.
  - A demand-side platform's user identifier
  - Year of Birth
  - Gender
  - Interests
  - Metadata reporting on consent provided
- Geography
  - Longitude and latitude
  - Postal/ZIP code



IAB7-24	Heart Disease
IAB7-25	Herbs for Health
IAB7-26	Holistic Healing
IAB7-27	IBS/Crohn's Disease
IAB7-28	Incest/Abuse Support
IAB7-29	Incontinence
IAB7-30	Infertility
IAB7-31	Men's Health
IAB7-32	Nutrition
IAB7-33	Orthopedics
IAB7-34	Panic/Anxiety Disorders
IAB7-35	Pediatrics
IAB7-36	Physical Therapy

… and retained

- Bid requests go to hundreds or thousands of companies; little oversight.
- **Vectaury** in France — small company ,with only 3.5m€ annual turnover — retained 68m bid request records (and fined by the French data regulator, CNIL) in 2018.
- Their website even claimed that they discarded 70% of all data, and only kept any of it for 12 months meaning that this small company was possibly sent 1/4 billion bid requests in just a single year.

PRIVACY IS HARDCO
VECTAURY'S DI

We strive for the creation of a constr
sustainable ecosystem, serving all
stakeholders

Data at scale for real-time bidding (RTB)

Leading RTB exchanges, daily bid request estimates

Index Exchange	50 billion[ii]
OpenX	60 billion+[i]
Rubicon Project	Unknown. Claims to reach 1 billion people's devices.[iii]
PubMatic	70 billion+[iv]
Oath/AOL	90 billion[v]
AppNexus	131 billion[vi]
Smaato	214 billion[vii]
Google DoubleClick	Unknown. DoubleClick is the dominant exchange.

[i] "Tour IX's Amsterdam and Frankfurt Data Centers", Index Exchange, 2 July 2018 (URL: https://www.indexexchange.com/tour-ix-amsterdam-frankfurt-data-centers/).

[ii] "OpenX Ad Exchange", OpenX (URL: https://www.openx.com/uk_en/products/ad-exchange/).

[iii] "Buyers", Rubicon Project, (URL: https://rubiconproject.com/buyers/).

[iv] "How PubMatic Is Learning Machine Learning", PubMatic, 25 January 2019 (URL: https://pubmatic.com/blog/learning-machine-learning/)

[v] "Maximize yield with Oath's publisher offerings", Oath, 3 April 2018 (URL: https://www.oath.com/insights/maximize-yield-with-oath-s-publisher-offerings/)

[vi] 500 Billion / 29.6 = 18.6 billion impressions per day. Using AppNexus 1:11.5 ratio, this is 214 auctions per day. 500+ impressions figure cited in "Optimize your mobile strategy", Smaato, (URL: https://www.smaato.com/).

[vii] "Transacting at a peak of 11.4 billion daily impressions, our marketplace handles more traffic each day than Visa, Nasdaq, and the NYSE combined" at https://www.appnexus.com/sell. Note that in 2017, AppNexus said in "AppNexus Scales with DriveScale", 2017, (URL: http://go.drivescale.com/rs/451-ESR-800/images/DRV_Case_Study_AppNexus-final.v1.pdf) that 10.7 billion "impressions transacted" came as a result of running 123 billion auctions. The impressions transacted to auctions ratio appears to be roughly 1:11.5. Therefore, the 11.4 daily impressions reported in 2018 equates to 131 billion auctions per day.

Cookie banners and the law

Data protection law

- GDPR — this data is identified or identifiable. By definition, used to remember you and only you.
- e-Privacy — implements confidentiality of communications for electronic world.
  - e-Privacy Directive (soon to be a Regulation, perhaps)
  - UK: PECR (The Privacy and Electronic Communications (EC Directive) Regulations 2003)

e-Privacy Law (PECR regulation 6**)**

6. (1) [..] a person shall not **store or gain access** to **information** stored, in the **terminal equipment** of a subscriber or user unless the requirements of paragraph (2) are met.

(2) The requirements are that the subscriber or user of that terminal equipment

(a) is provided with **clear and comprehensive information** about the purposes of the storage of, or access to, that information; and

(b) has given his or her **consent**.*

[truncated: consent carries over; can be signalled electronically]

(4) Paragraph (1) shall not apply to the technical storage of, or access to, information—

(a) for the **sole purpose of carrying out the transmission** of a communication over an electronic communications network; or

(b) where such storage or access is **strictly necessary for the provision of an information society service requested by the subscriber or user**.

The Privacy and Electronic Communications (EC Directive) Regulations 2003, reg 6. * Note that in Regulation 2 it states that “*“consent” by a user or subscriber corresponds to the data subject’s consent in the GDPR (as defined in section 3(10) of the Data Protection Act 2018)*”.

No cookie banner??

SIGN UP TO NEWSLETTER
SEARCH
NEWS
ACT
CAMPAIGNS
LEARN
IMPACT
ABOUT
DONATE
LONG READ

We asked five menstruation apps for our data and here is what we found...

We asked five menstruation apps to give us access to our data. We got a dizzying dive into the most intimate information about us.

FR

For a world where technology

Sources of law for consent

GDPR (operative provisions)

Article 4

Definitions

11. ‘consent’ of the data subject means any **freely given, specific, informed and unambiguous indication** of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to **demonstrate** that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is **clearly distinguishable from the other matters**, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the **right to withdraw his or her consent at any time**. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. **It shall be as easy to withdraw as to give consent.**

4. **When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.**

Sources of law for consent

GDPR (recitals)

Recital 32

Consent should be given by a **clear affirmative act** establishing a **freely given, specific, informed and unambiguous indication** of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include **ticking a box when visiting an internet website**, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. **Silence, pre-ticked boxes or inactivity should not therefore constitute consent.** Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. **If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.**

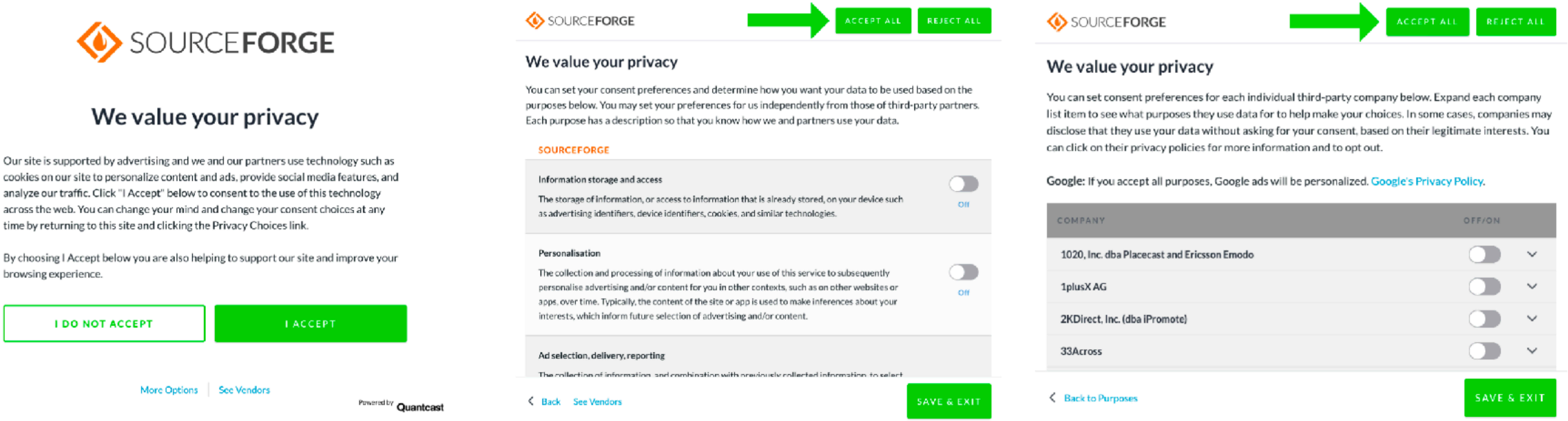
Case C-673/17 *Planet 49* ECLI:EU:C:2019:801.

- The company *Planet49* had a pre-ticked checkbox on a promotional lottery website www.dein-macbook.de.
- The argument that preticked boxes were allowed under the Data Protection Directive was rejected by the CJEU; the clarifications in the GDPR means that this reading applies even more so.
- Consent is “not validly constituted if, in the form of cookies, the storage of information or access to information already stored in a website user’s terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent.” [para 65]

With hundreds of trackers… how?

Consent management platforms emerge

Legal entrepreneurship of an unsavoury kind



We value your privacy

Our site is supported by advertising and we and our partners use technology such as cookies on our site to personalize content and ads, provide social media features, and analyze our traffic. Click "I Accept" below to consent to the use of this technology across the web. You can change your mind and change your consent choices at any time by returning to this site and clicking the Privacy Choices link.

By choosing I Accept below you are also helping to support our site and improve your browsing experience.

We value your privacy

You can set your consent preferences and determine how you want your data to be used based on the purposes below. You may set your preferences for us independently from those of third-party partners. Each purpose has a description so that you know how we and partners use your data.

SOURCEFORGE

Information storage and access

The storage of information, or access to information that is already stored, on your device such as advertising identifiers, device identifiers, cookies, and similar technologies.

Personalisation

The collection and processing of information about your use of this service to subsequently personalise advertising and/or content for you in other contexts, such as on other websites or apps, over time. Typically, the content of the site or app is used to make inferences about your interests, which inform future selection of advertising and/or content.

Ad selection, delivery, reporting

The collection of information, and combination with previously collected information, to select

We value your privacy

You can set consent preferences for each individual third-party company below. Expand each company list item to see what purposes they use data for to help make your choices. In some cases, companies may disclose that they use your data without asking for your consent, based on their legitimate interests. You can click on their privacy policies for more information and to opt out.

Google: If you accept all purposes, Google ads will be personalized. Google's Privacy Policy.

COMPANY	OFF/ON
1020, Inc. dba Placecast and Ericsson Emodo	
1plusX AG	
2KDirect, Inc. (dba iPromote)	
33Across	

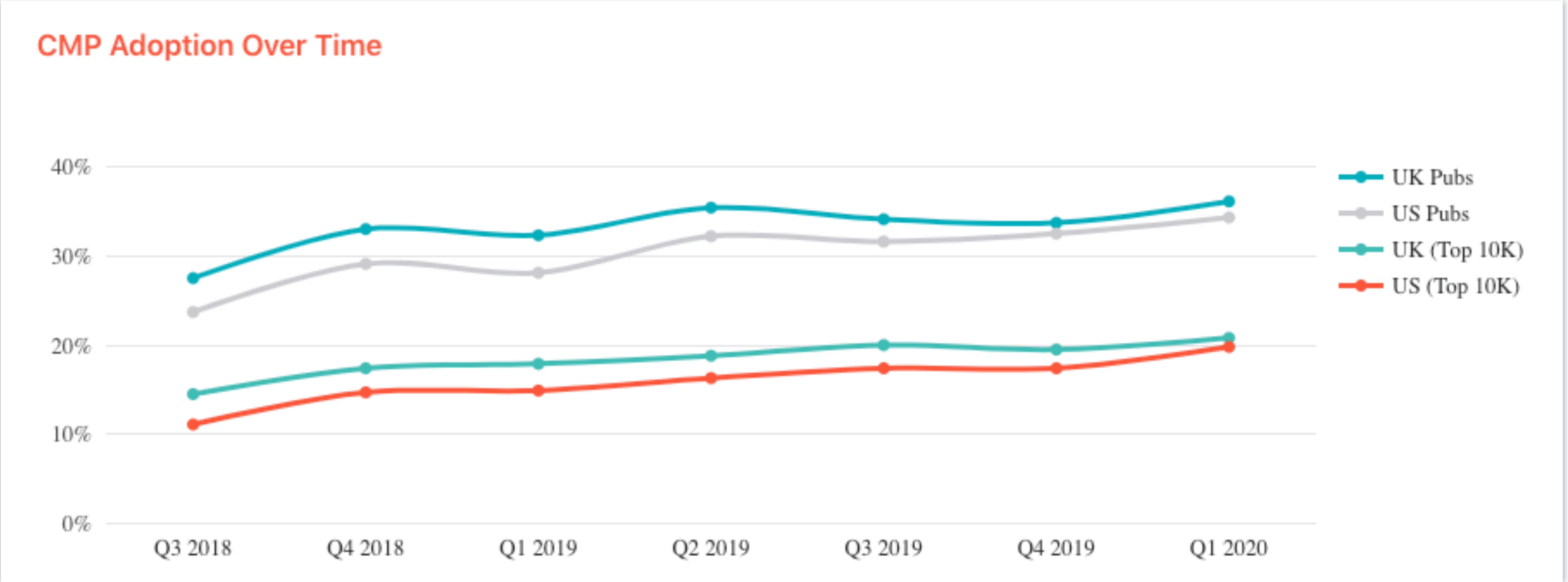
(a) First page

(b) Categories and purposes

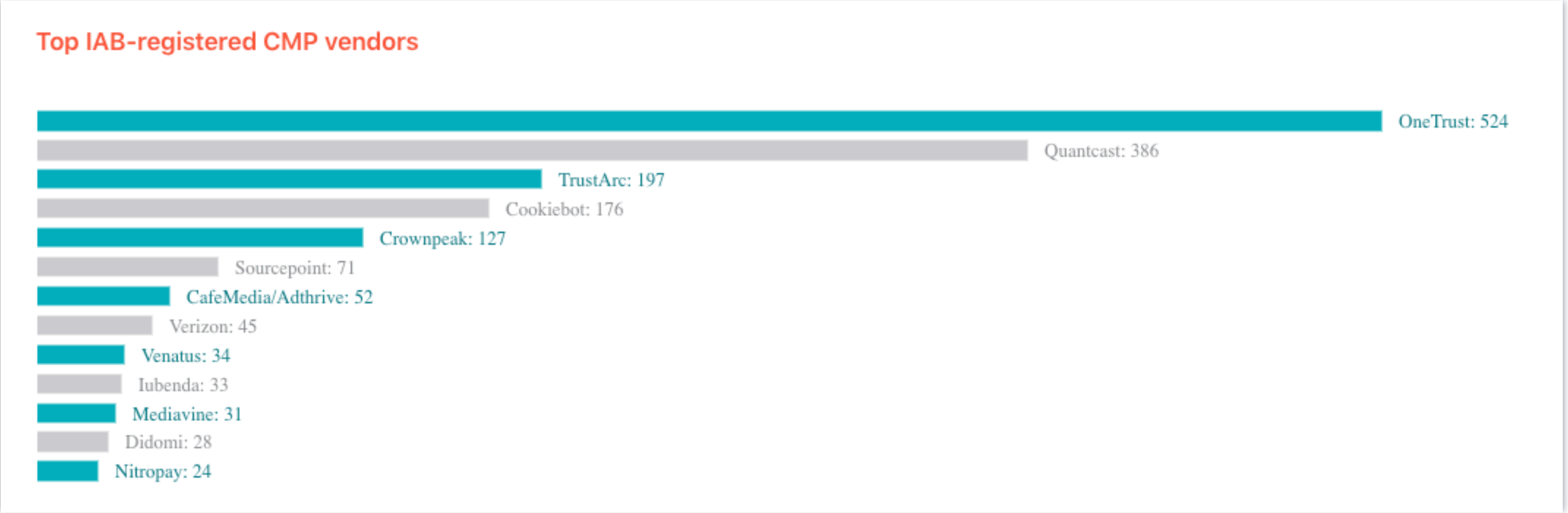
(c) Vendors/third-parties

Figure 1. The three components of the QuantCast CMP on `https://sourceforge.net` as of September 2019.

A concentrated and growing practice



CMP Adoption Over Time

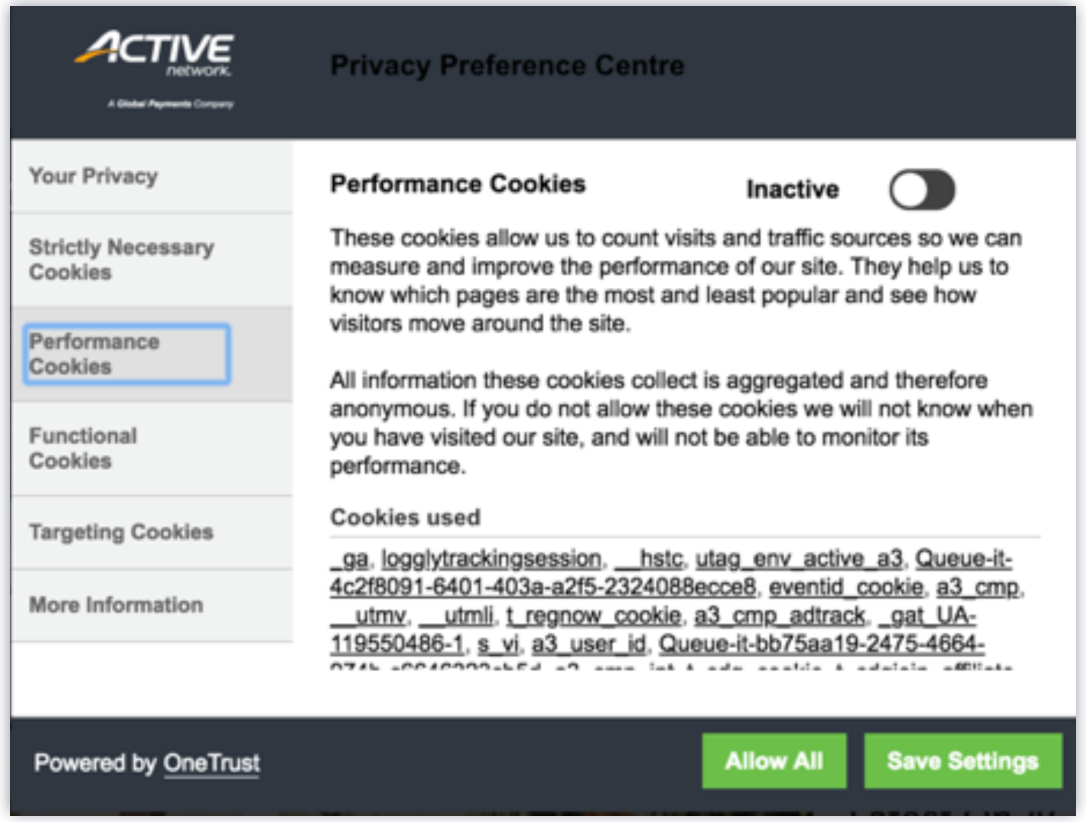


Top IAB-registered CMP vendors

Source: Adzerk.

Many vendors: but are they compliant with the law?

OneTrust



Privacy Preference Centre

Performance Cookies

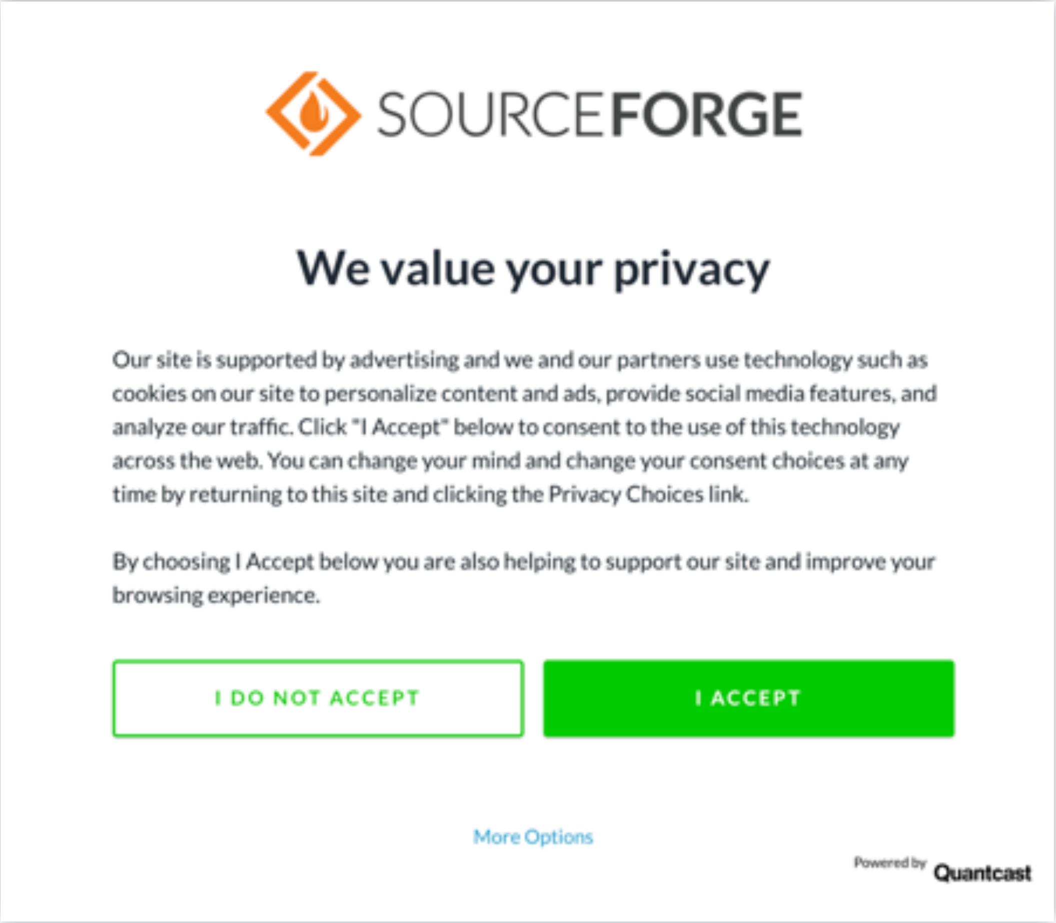
These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us to know which pages are the most and least popular and see how visitors move around the site.

All information these cookies collect is aggregated and therefore anonymous. If you do not allow these cookies we will not know when you have visited our site, and will not be able to monitor its performance.

Cookies used

_ga, logglytrackingsession, __hstc, utag_env_active_a3, Queue-it-4c2f8091-6401-403a-a2f5-2324088ecce8, eventid_cookie, a3_cmp, __utmv, __utmli, t_regnow_cookie, a3_cmp_adtrack, _gat_UA-119550486-1, s_vi, a3_user_id, Queue-it-bb75aa19-2475-4664-

Quantcast

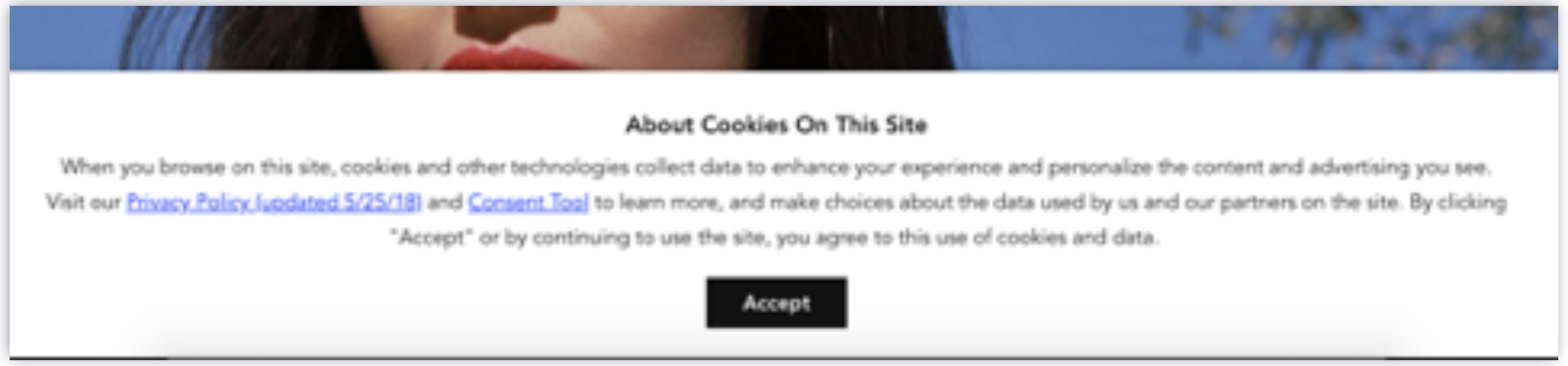


We value your privacy

Our site is supported by advertising and we and our partners use technology such as cookies on our site to personalize content and ads, provide social media features, and analyze our traffic. Click "I Accept" below to consent to the use of this technology across the web. You can change your mind and change your consent choices at any time by returning to this site and clicking the Privacy Choices link.

By choosing I Accept below you are also helping to support our site and improve your browsing experience.

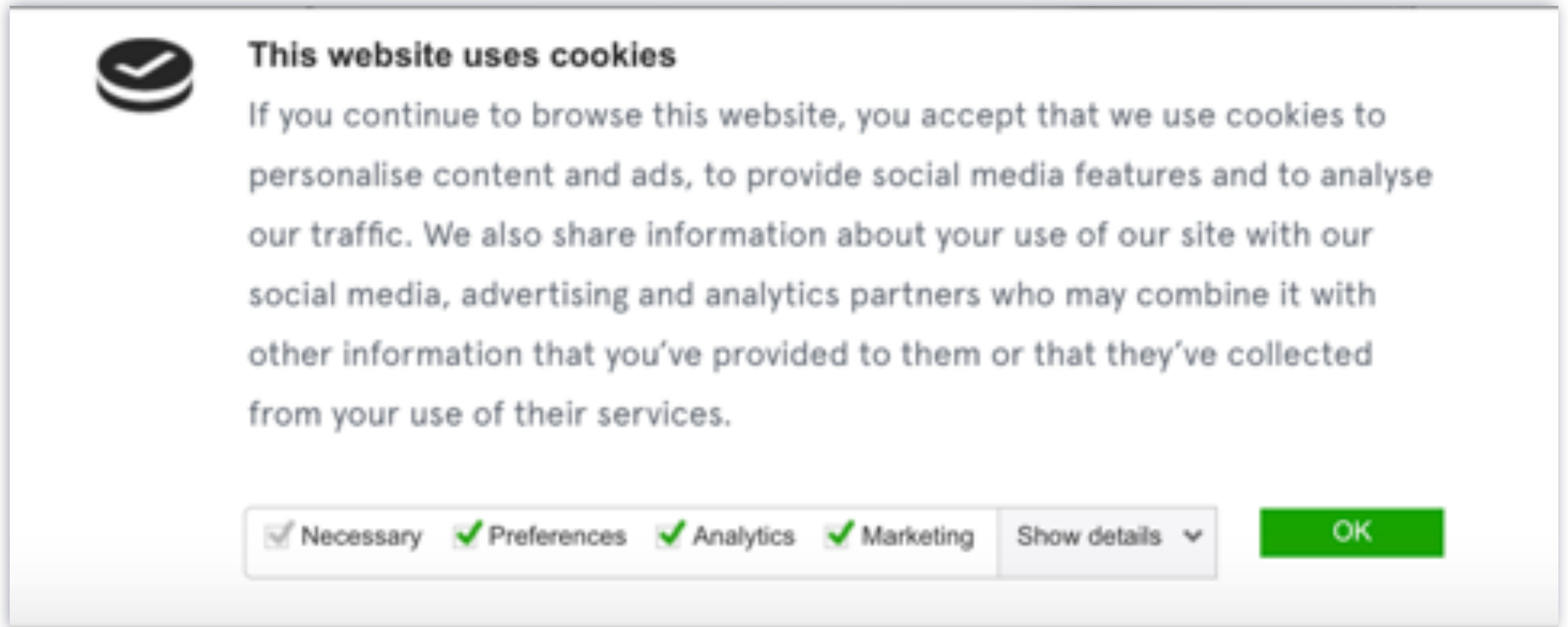
CrownPeak



About Cookies On This Site

When you browse on this site, cookies and other technologies collect data to enhance your experience and personalize the content and advertising you see. Visit our Privacy Policy (updated 5/25/18) and Consent Tool to learn more, and make choices about the data used by us and our partners on the site. By clicking "Accept" or by continuing to use the site, you agree to this use of cookies and data.

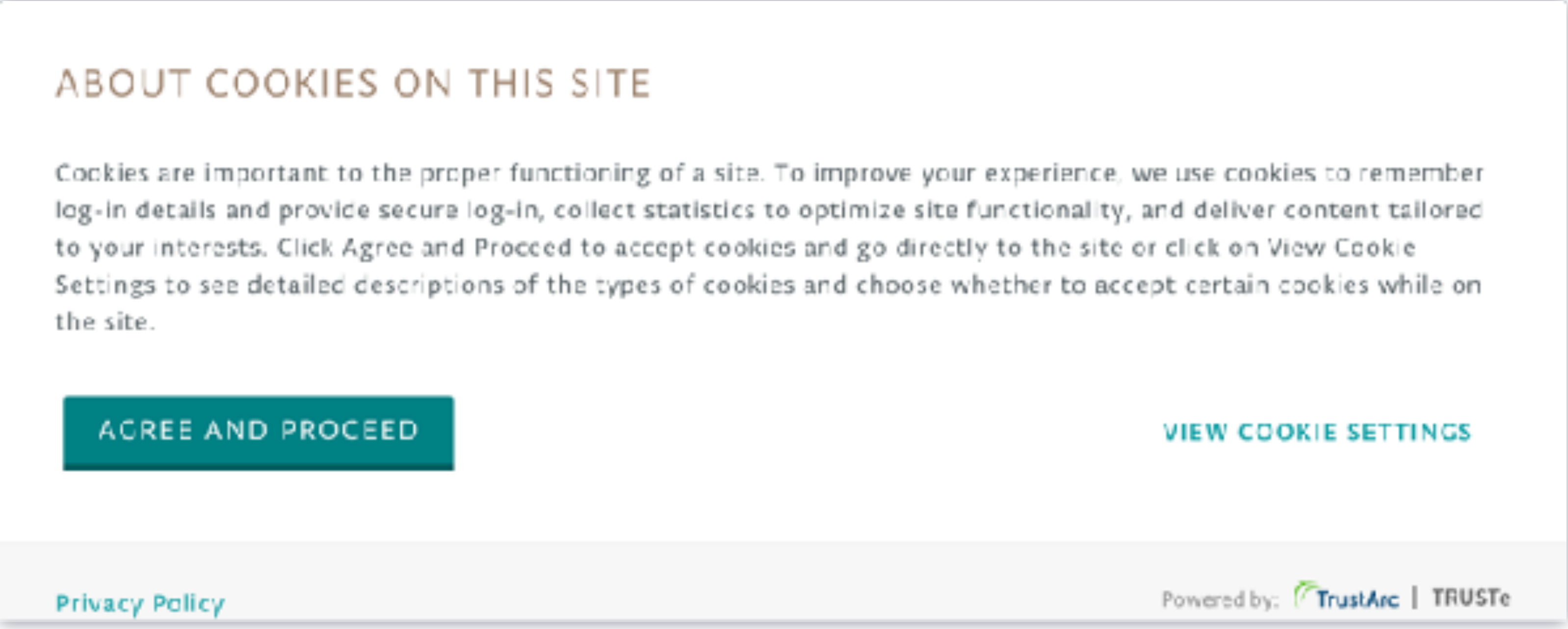
CookieBot



This website uses cookies

If you continue to browse this website, you accept that we use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

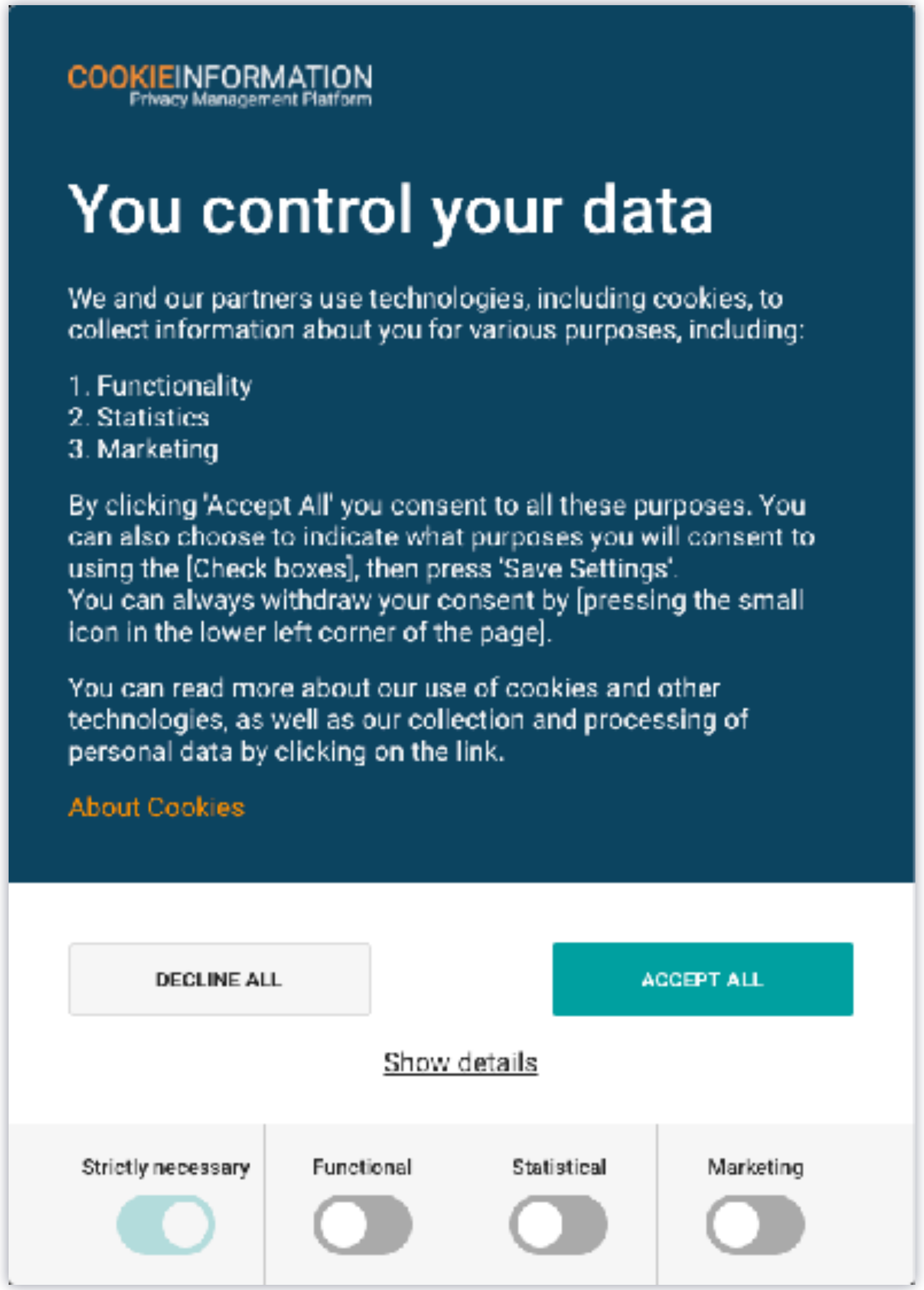
TrustArc



ABOUT COOKIES ON THIS SITE

Cookies are important to the proper functioning of a site. To improve your experience, we use cookies to remember log-in details and provide secure log-in, collect statistics to optimize site functionality, and deliver content tailored to your interests. Click Agree and Proceed to accept cookies and go directly to the site or click on View Cookie Settings to see detailed descriptions of the types of cookies and choose whether to accept certain cookies while on the site.

Cookieinformation



You control your data

We and our partners use technologies, including cookies, to collect information about you for various purposes, including:

1. Functionality
2. Statistics
3. Marketing

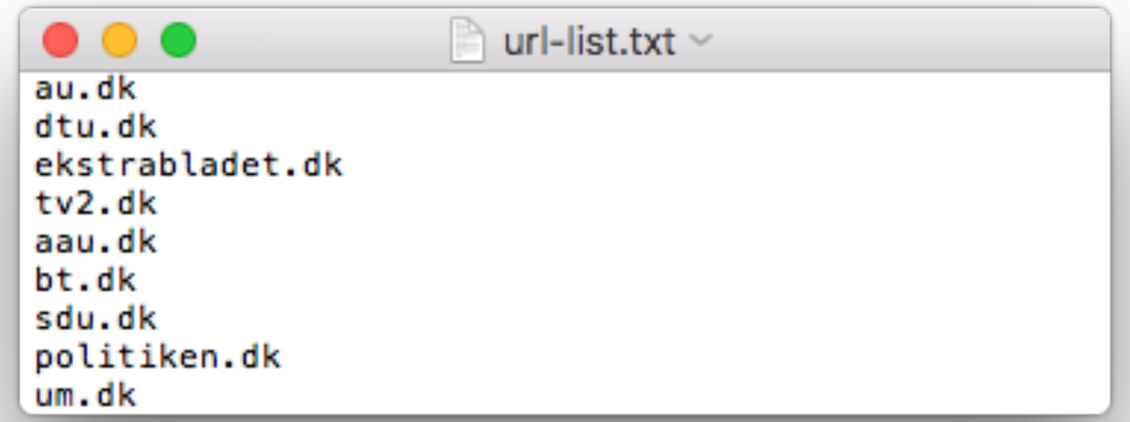
By clicking 'Accept All' you consent to all these purposes. You can also choose to indicate what purposes you will consent to using the [Check boxes], then press 'Save Settings'.
You can always withdraw your consent by [pressing the small icon in the lower left corner of the page].

You can read more about our use of cookies and other technologies, as well as our collection and processing of personal data by clicking on the link.

Empirical, computational legal analysis to find out

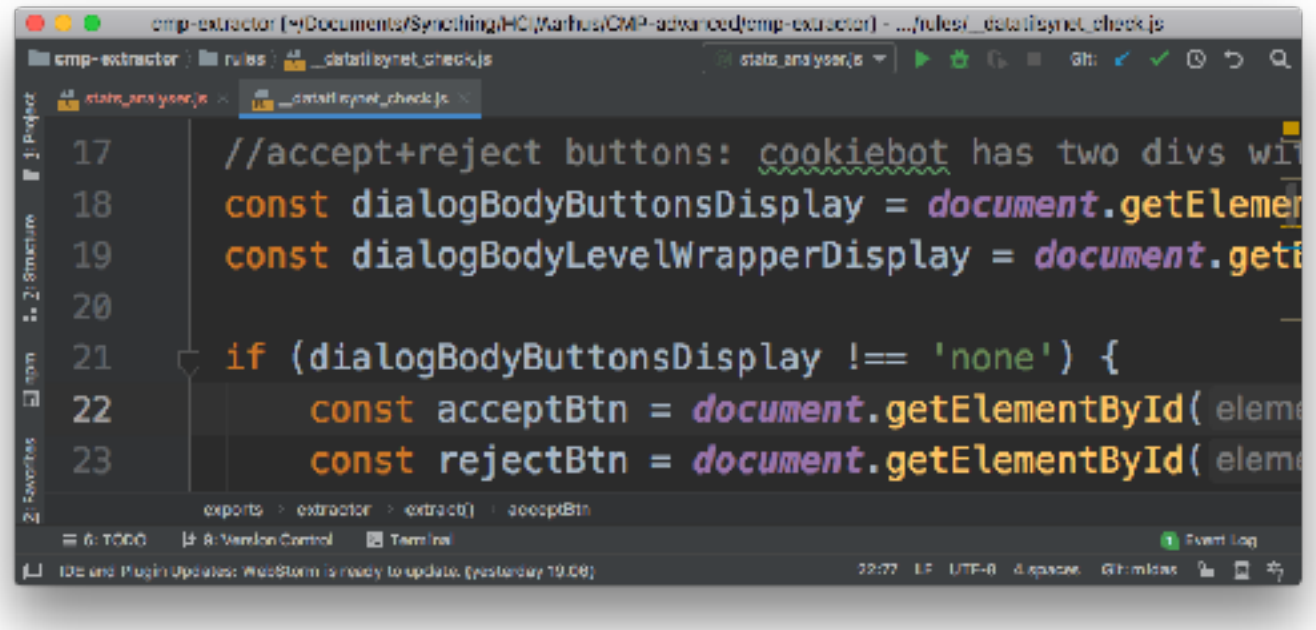
- Together with Aarhus University and MIT, we investigated whether these interfaces were providing valid consent under EU law.
- Built a bespoke *web scraper* and fed it the top 10K UK websites in 2019. We coded it to be able to analyse the top 5 CMPs to see how they were configured.

List of URLs to check



```
au.dk
dtu.dk
ekstrabladet.dk
tv2.dk
aau.dk
bt.dk
sdu.dk
politiken.dk
um.dk
```

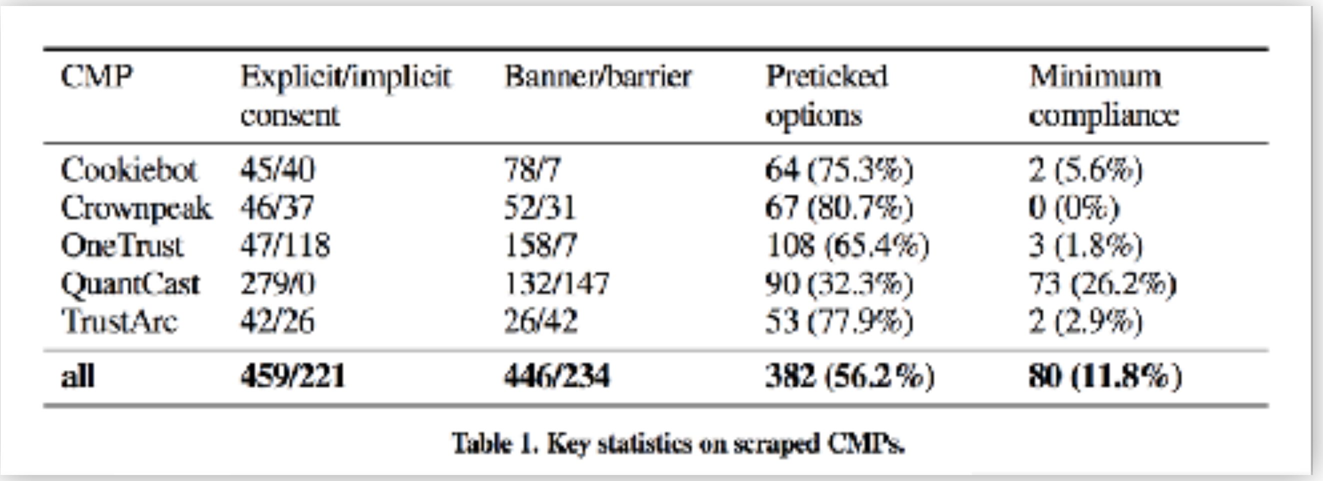
Software analyses pop-ups


cmp-extractor [~/Documents/Syncthing/HCI/Aarhus/CMP-advanced/cmp-extractor] - .../rules/_datatilsynet_check.js
cmp-extractor
rules
_datatilsynet_check.js
stats_analyser.js
exports › extractor › extract() › acceptBtn
6: TODO
9: Version Control
Terminal
Event Log

```
//accept+reject buttons: cookiebot has two divs wi
const dialogBodyButtonsDisplay = document.getElemen
const dialogBodyLevelWrapperDisplay = document.getE

if (dialogBodyButtonsDisplay !== 'none') {
    const acceptBtn = document.getElementById( eleme
    const rejectBtn = document.getElementById( eleme
```

Returns data on compliance



CMP	Explicit/implicit consent	Banner/barrier	Preticked options	Minimum compliance
Cookiebot	45/40	78/7	64 (75.3%)	2 (5.6%)
Crownpeak	46/37	52/31	67 (80.7%)	0 (0%)
OneTrust	47/118	158/7	108 (65.4%)	3 (1.8%)
QuantCast	279/0	132/147	90 (32.3%)	73 (26.2%)
TrustArc	42/26	26/42	53 (77.9%)	2 (2.9%)
all	**459/221**	**446/234**	**382 (56.2%)**	**80 (11.8%)**

Table 1. Key statistics on scraped CMPs.

Midas Nouwens and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence' in (ACM 2020) Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2020).

What were we looking for?

Variable	Values
Notification style	Banner Barrier Other
Bulk description	"...."
Consent action	Visit page Scroll page Navigate page Close pop-up Refresh page Click consent button
Accept all/Reject all Purpose/vendor	Exists? Label Clicks
Purpose/vendor items	Name Description Default status Enabled

Midas Nouwens and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence' in (ACM 2020) Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2020).

And what did we find?

Turned case law into three legal tests

1. No optional boxes preticked
2. Reject all as easy as Accept all
3. Consent is explicit

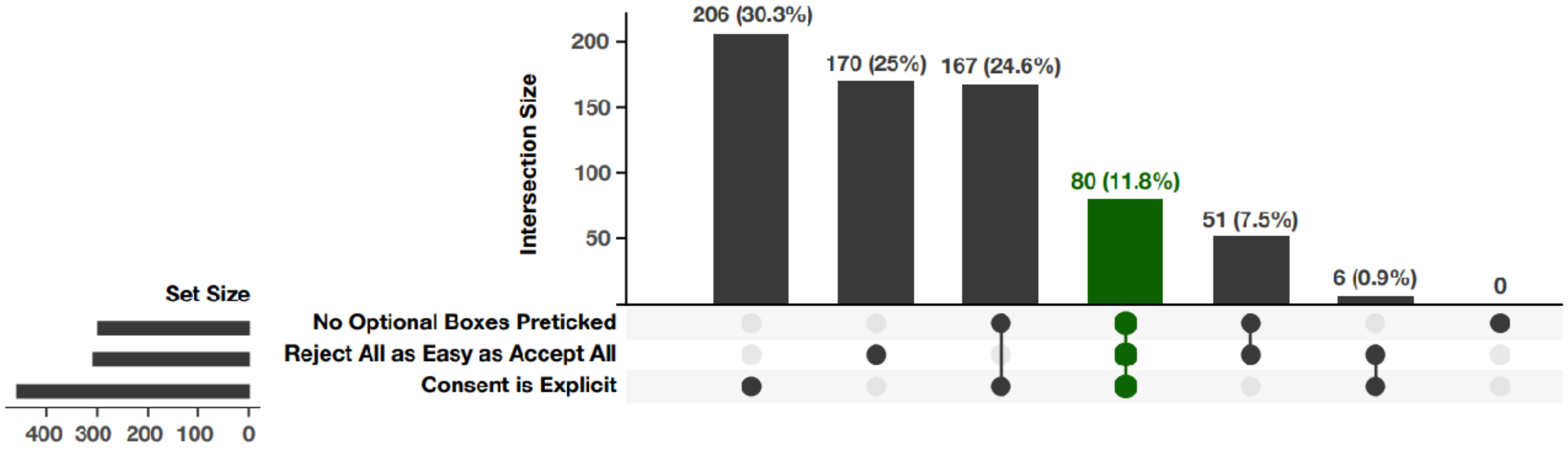
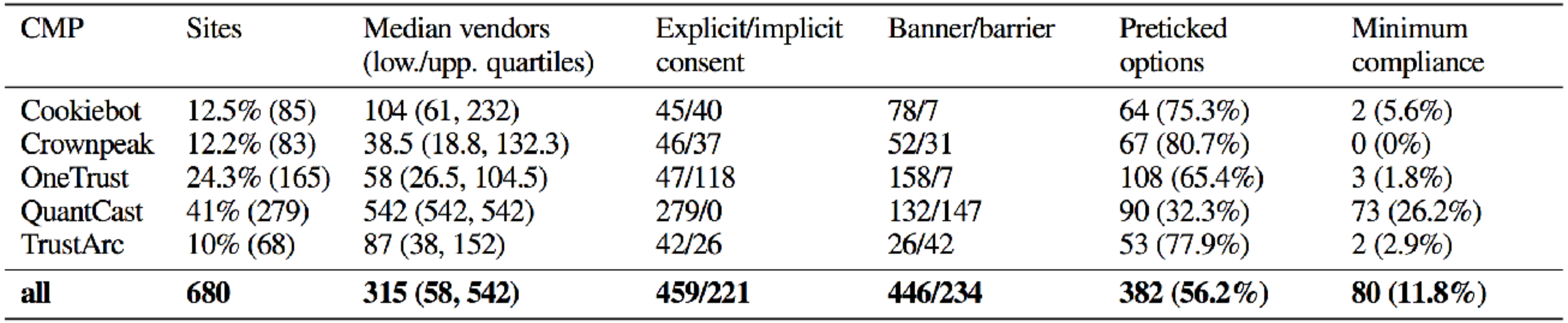


Figure 2. UpSet diagram [16, 36] of sites by adherence to three core conditions of EU law. Sites meeting all three in green.

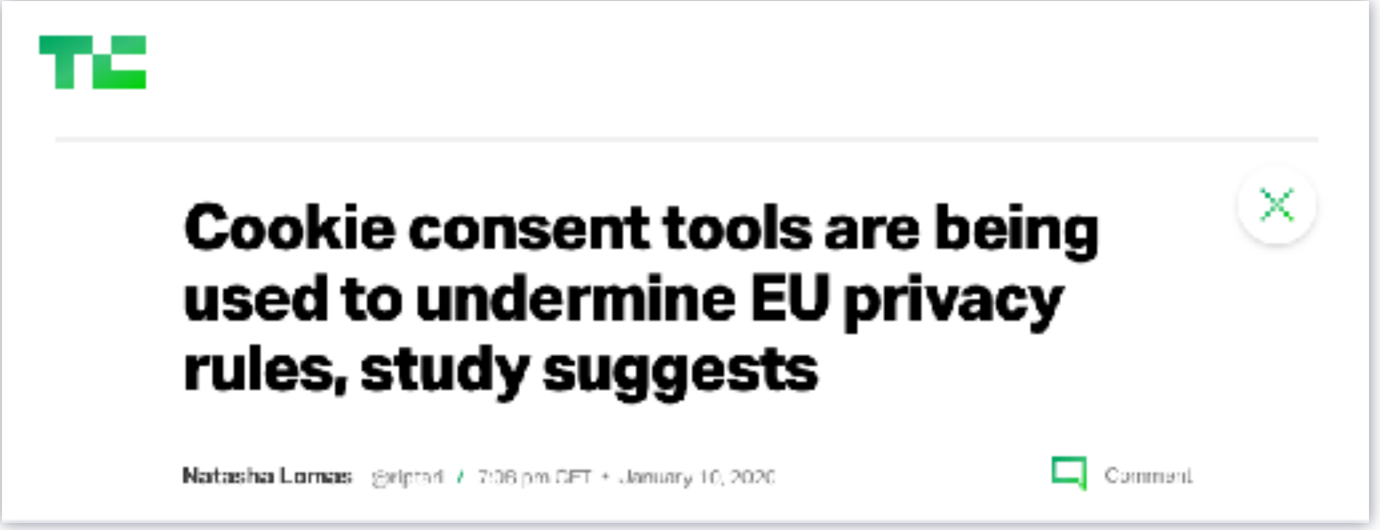


CMP	Sites	Median vendors (low./upp. quartiles)	Explicit/implicit consent	Banner/barrier	Preticked options	Minimum compliance
Cookiebot	12.5% (85)	104 (61, 232)	45/40	78/7	64 (75.3%)	2 (5.6%)
Crownpeak	12.2% (83)	38.5 (18.8, 132.3)	46/37	52/31	67 (80.7%)	0 (0%)
OneTrust	24.3% (165)	58 (26.5, 104.5)	47/118	158/7	108 (65.4%)	3 (1.8%)
QuantCast	41% (279)	542 (542, 542)	279/0	132/147	90 (32.3%)	73 (26.2%)
TrustArc	10% (68)	87 (38, 152)	42/26	26/42	53 (77.9%)	2 (2.9%)
all	**680**	**315 (58, 542)**	**459/221**	**446/234**	**382 (56.2%)**	**80 (11.8%)**

Table 1. Key statistics on scraped CMPs.

Midas Nouwens and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence' in (ACM 2020) Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2020).

Research attracts significant media interest

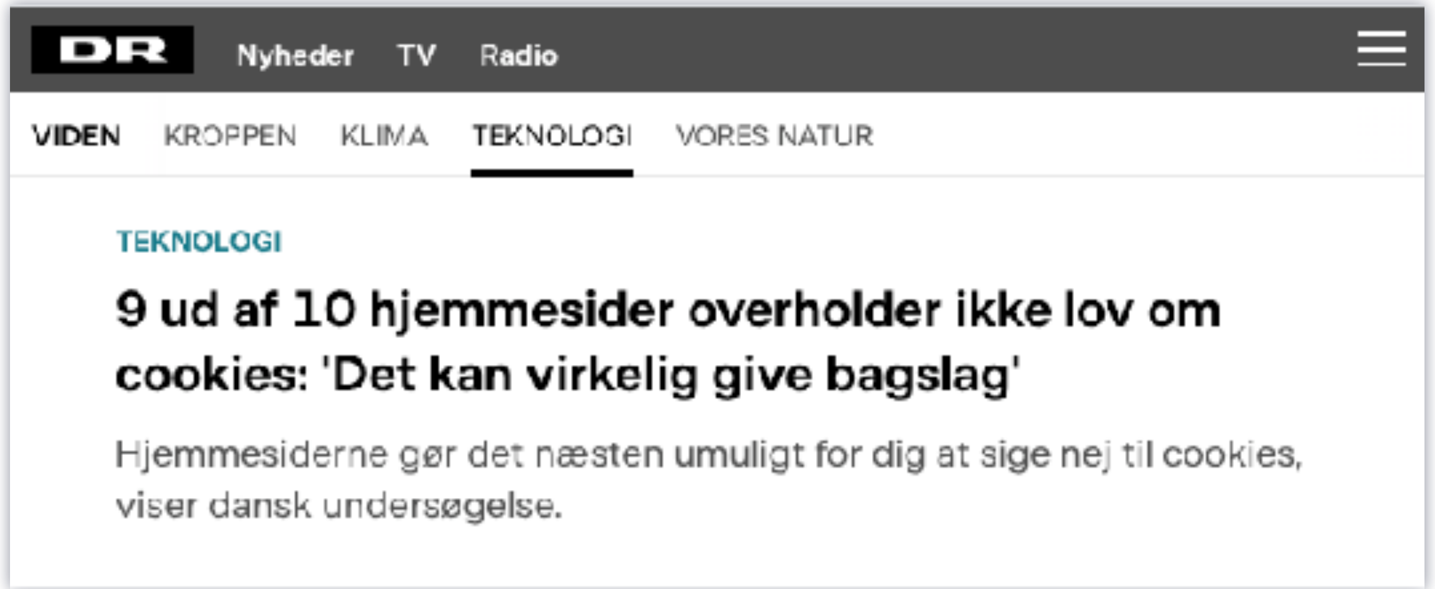


TC

Cookie consent tools are being used to undermine EU privacy rules, study suggests

Natasha Lomas @riptari / 7:08 pm CET • January 10, 2020

Comment



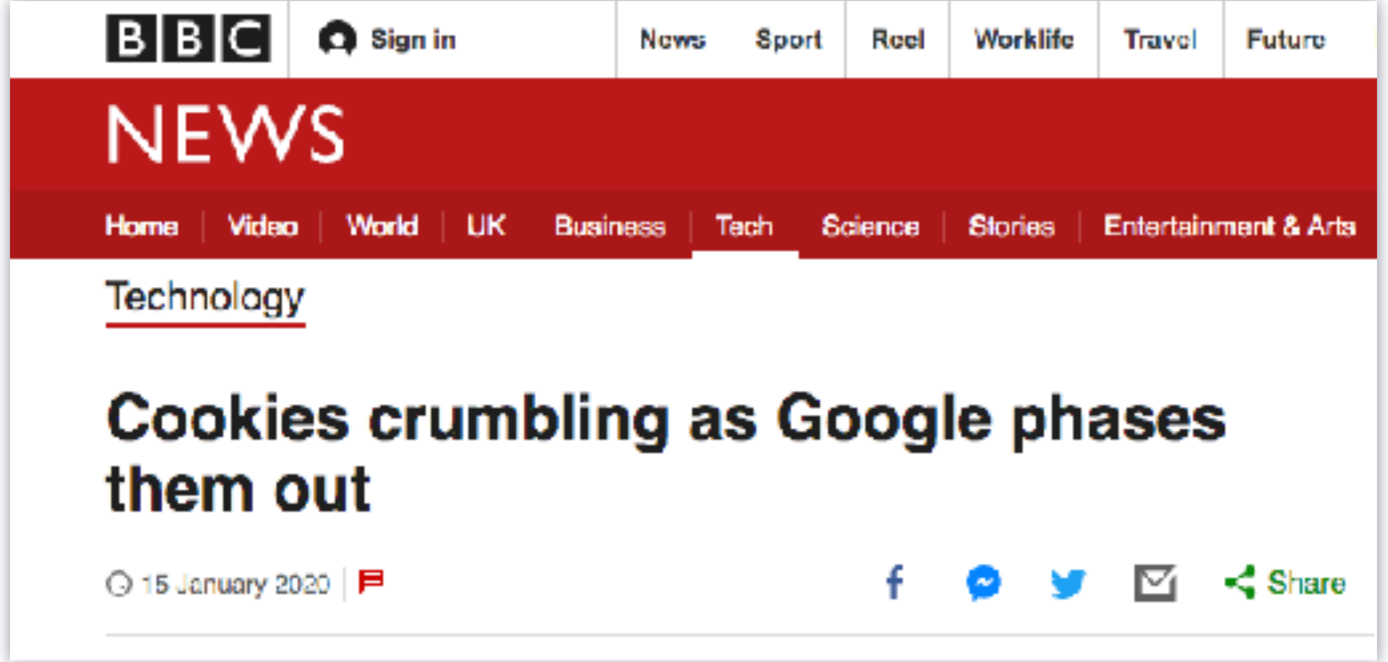
DR Nyheder TV Radio

VIDEN KROPPEN KLIMA TEKNOLOGI VORES NATUR

TEKNOLOGI

9 ud af 10 hjemmesider overholder ikke lov om cookies: 'Det kan virkelig give bagslag'

Hjemmesiderne gør det næsten umuligt for dig at sige nej til cookies, viser dansk undersøgelse.



BBC Sign in News Sport Reel Worklife Travel Future

NEWS

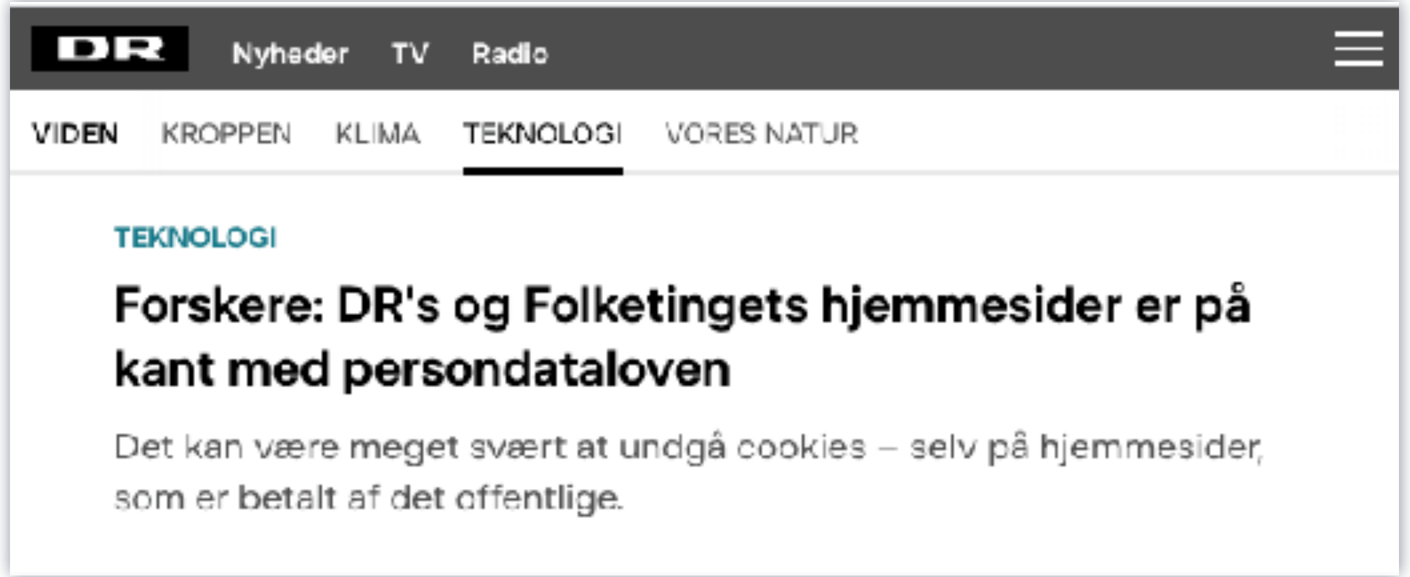
Home Video World UK Business Tech Science Stories Entertainment & Arts

Technology

Cookies crumbling as Google phases them out

15 January 2020

Share



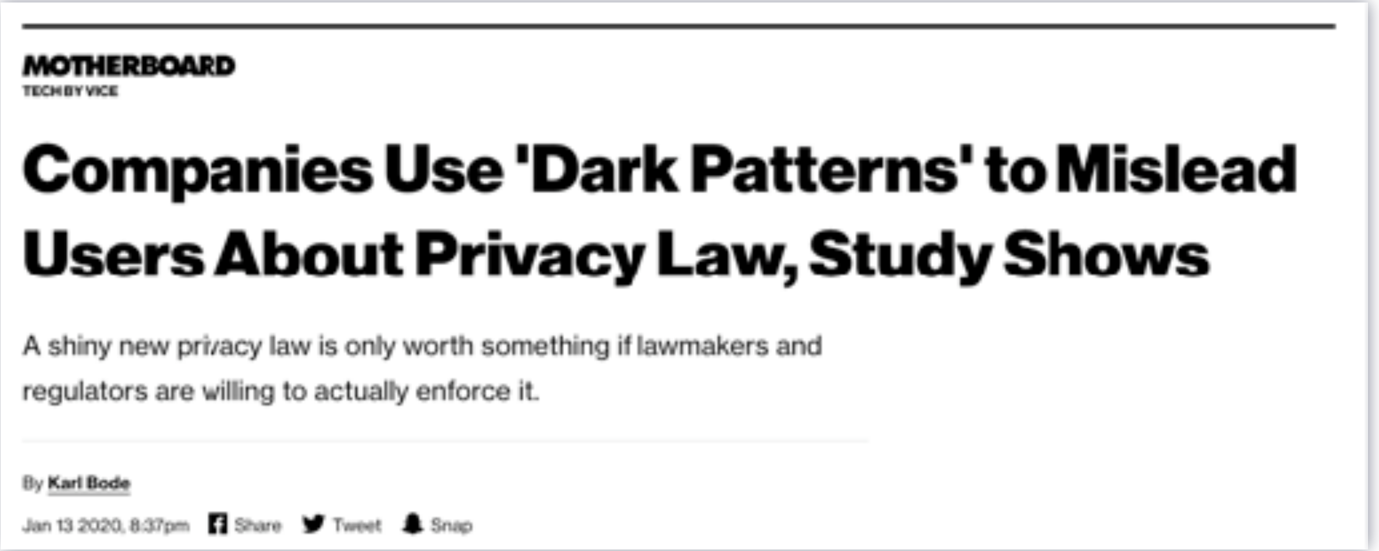
DR Nyheder TV Radio

VIDEN KROPPEN KLIMA TEKNOLOGI VORES NATUR

TEKNOLOGI

Forskere: DR's og Folketingets hjemmesider er på kant med persondataloven

Det kan være meget svært at undgå cookies – selv på hjemmesider, som er betalt af det offentlige.



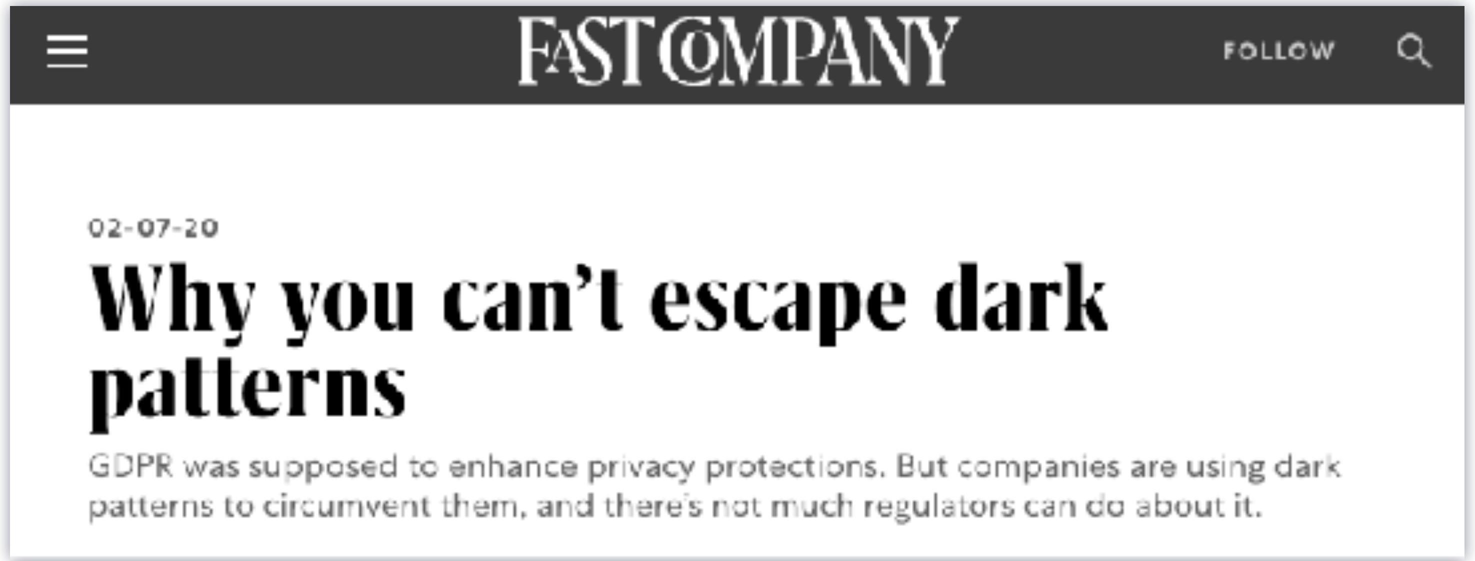
MOTHERBOARD
TECH BY VICE

Companies Use 'Dark Patterns' to Mislead Users About Privacy Law, Study Shows

A shiny new privacy law is only worth something if lawmakers and regulators are willing to actually enforce it.

By Karl Bode

Jan 13 2020, 8:37pm Share Tweet Snap



FAST COMPANY FOLLOW

02-07-20

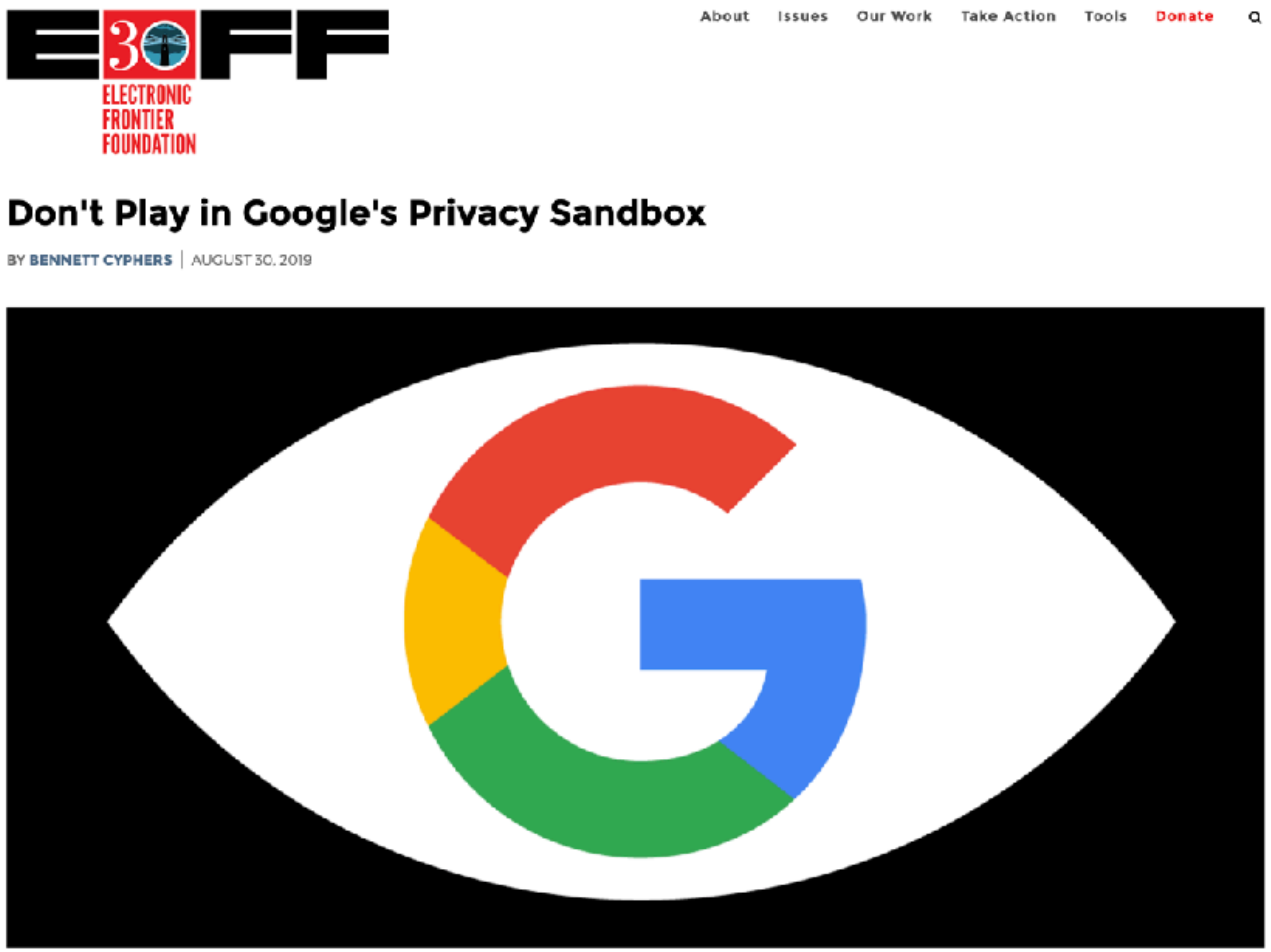
Why you can't escape dark patterns

GDPR was supposed to enhance privacy protections. But companies are using dark patterns to circumvent them, and there's not much regulators can do about it.

But does it lead to enforcement?

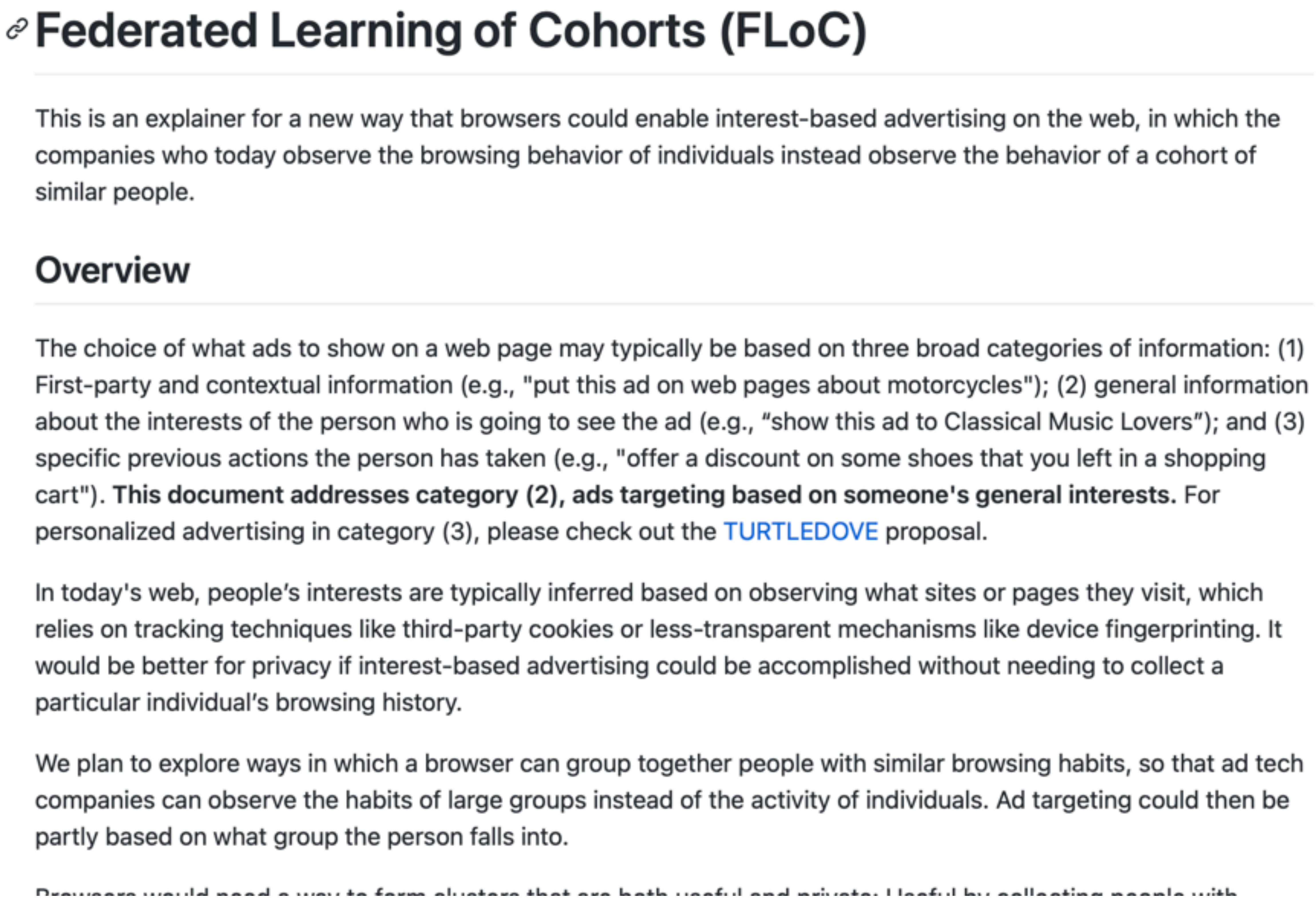
- Complaints we made to the Information Commissioner's Office led to a report (*Update Report on Adtech*) finding widespread illegality across the sector.
- However, no enforcement as of yet; and no change in the industry.
- ICO dropped the complaint having used no powers — we (with the Open Rights Group) are taking them to court to ensure they continue.

Postscript: Google FLoC



Don't Play in Google's Privacy Sandbox

BY BENNETT CYPHERS | AUGUST 30, 2019



Federated Learning of Cohorts (FLoC)

This is an explainer for a new way that browsers could enable interest-based advertising on the web, in which the companies who today observe the browsing behavior of individuals instead observe the behavior of a cohort of similar people.

Overview

The choice of what ads to show on a web page may typically be based on three broad categories of information: (1) First-party and contextual information (e.g., "put this ad on web pages about motorcycles"); (2) general information about the interests of the person who is going to see the ad (e.g., “show this ad to Classical Music Lovers”); and (3) specific previous actions the person has taken (e.g., "offer a discount on some shoes that you left in a shopping cart"). **This document addresses category (2), ads targeting based on someone's general interests.** For personalized advertising in category (3), please check out the TURTLEDOVE proposal.

In today's web, people’s interests are typically inferred based on observing what sites or pages they visit, which relies on tracking techniques like third-party cookies or less-transparent mechanisms like device fingerprinting. It would be better for privacy if interest-based advertising could be accomplished without needing to collect a particular individual’s browsing history.

We plan to explore ways in which a browser can group together people with similar browsing habits, so that ad tech companies can observe the habits of large groups instead of the activity of individuals. Ad targeting could then be partly based on what group the person falls into.

Browsers would need a way to form clusters that are both useful and private: Useful by collecting people with

Who should be responsible?

Controllership

- Data controllers are the responsible ones but unlike in PETs, we don’t think of data controllers as organisations who can see the cleartext of data.

Case C-25/17 Jehovan todistajat ECLI:EU:C:2018:551.

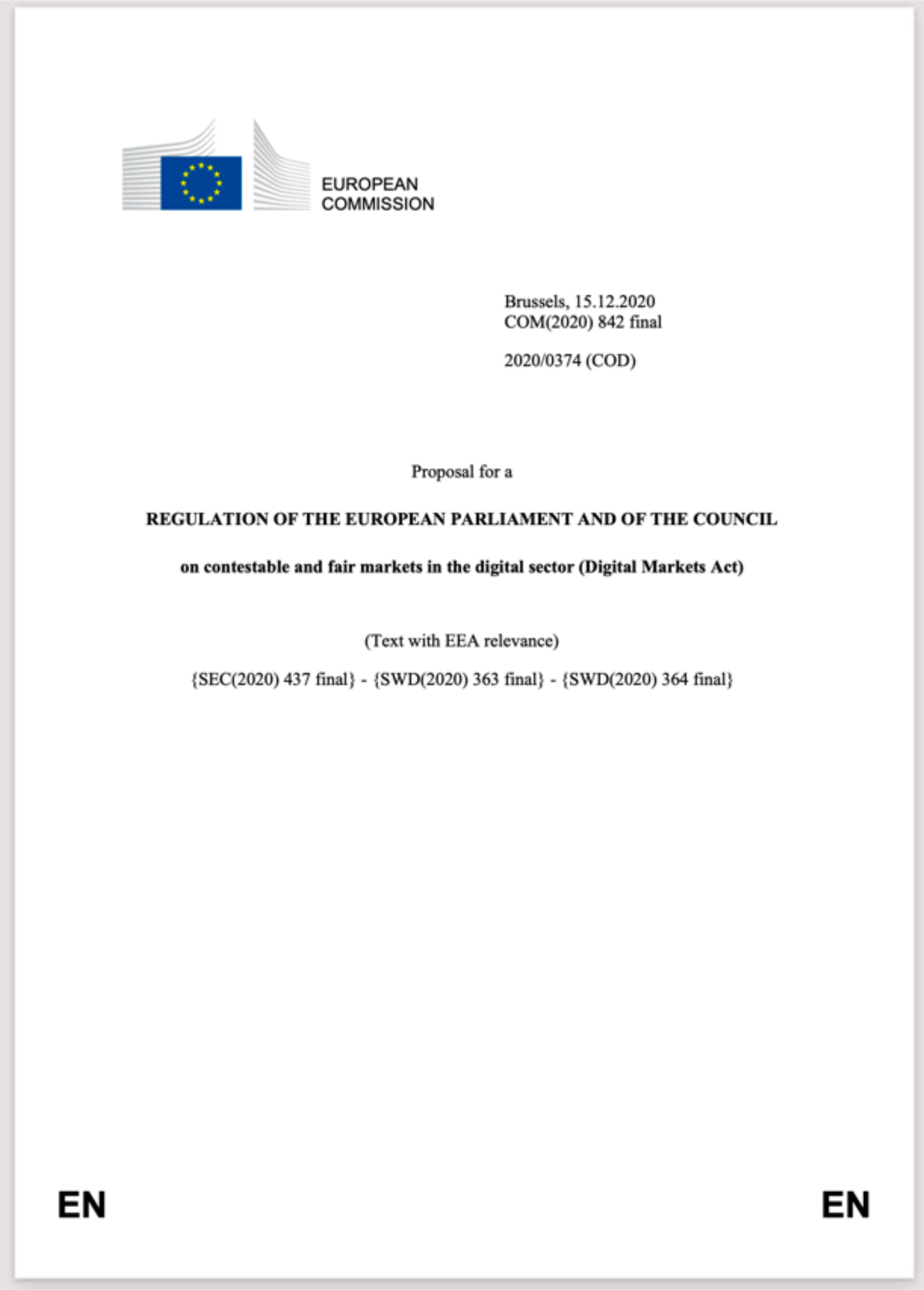
- Door-to-door preachers take notes about individuals as an *aide-memoire*.
- The broader Jehovah's Witnesses communities provides guides, forms, training for this.
- Court found that
  - *a religious community is a controller, jointly with its members who engage in preaching, for the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community,* ***without it being necessary that the community has access to those data****, or to establish that that community has given its members written guidelines or instructions in relation to the data processing.*

Case C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH ECLI:EU:C:2018:388.

- Business school in Germany had a Facebook page which laid cookies.
- The Court found that the school was a *joint* controller with Facebook because it both facilitated people to use this page (and take a cookie laid) and influenced some aggregate statistic creation.
- In a similar case, *Fashion ID*, a website owner was co-controller with Facebook because it embedded a *Facebook Pixel*. However, the website was not responsible at all for any illegality Facebook later caused; which drew criticism as the Court made artificial ‘stages’ of data processing.

Emerging challenges

Digital Markets Act



EUROPEAN
COMMISSION

Brussels, 15.12.2020
COM(2020) 842 final

2020/0374 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on contestable and fair markets in the digital sector (Digital Markets Act)

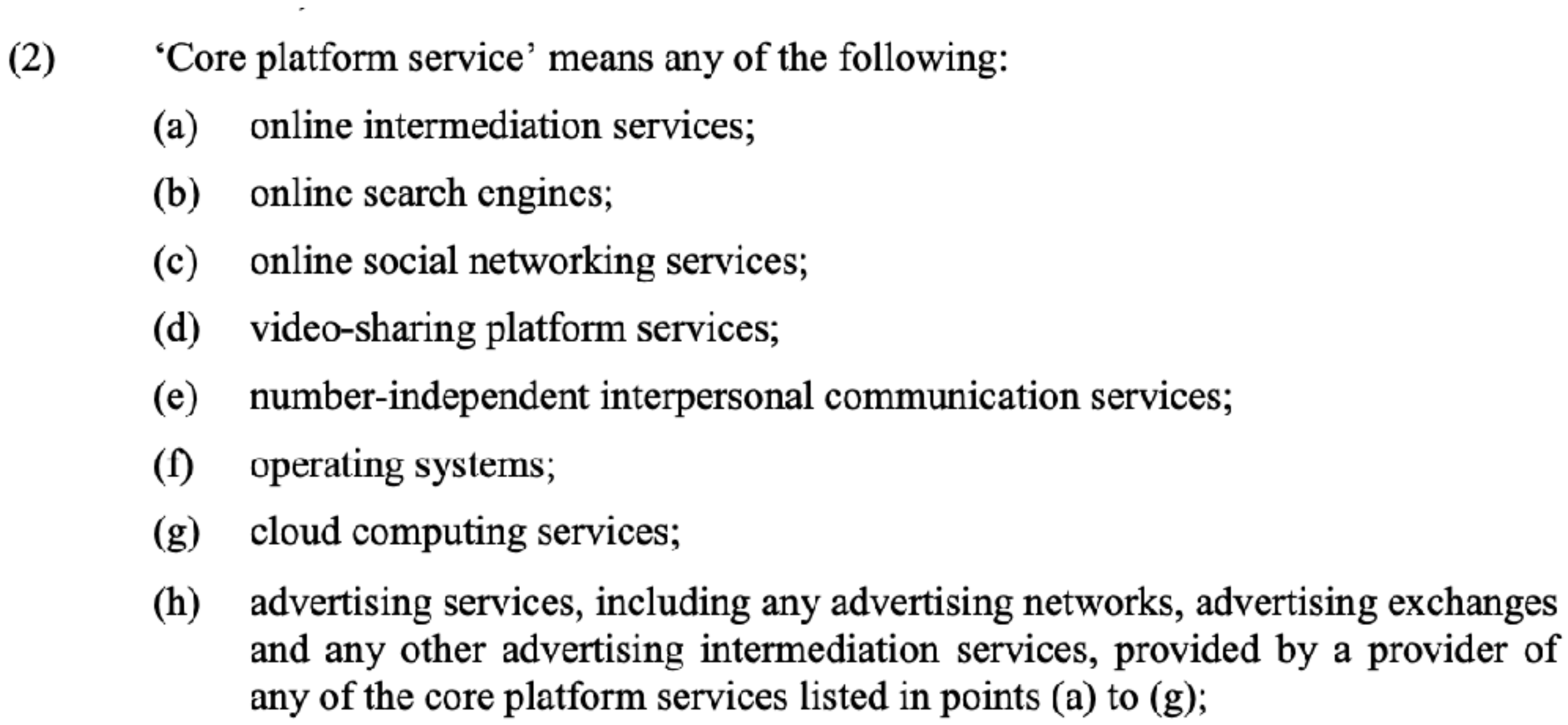
(Text with EEA relevance)

{SEC(2020) 437 final} - {SWD(2020) 363 final} - {SWD(2020) 364 final}

EN **EN**

Structure of the DMA

- Defines core services
- Large, powerful providers of these are *gatekeepers*. Subject to specific provisions (in arts 5–6)



(2) ‘Core platform service’ means any of the following:

(a) online intermediation services;

(b) online search engines;

(c) online social networking services;

(d) video-sharing platform services;

(e) number-independent interpersonal communication services;

(f) operating systems;

(g) cloud computing services;

(h) advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by a provider of any of the core platform services listed in points (a) to (g);

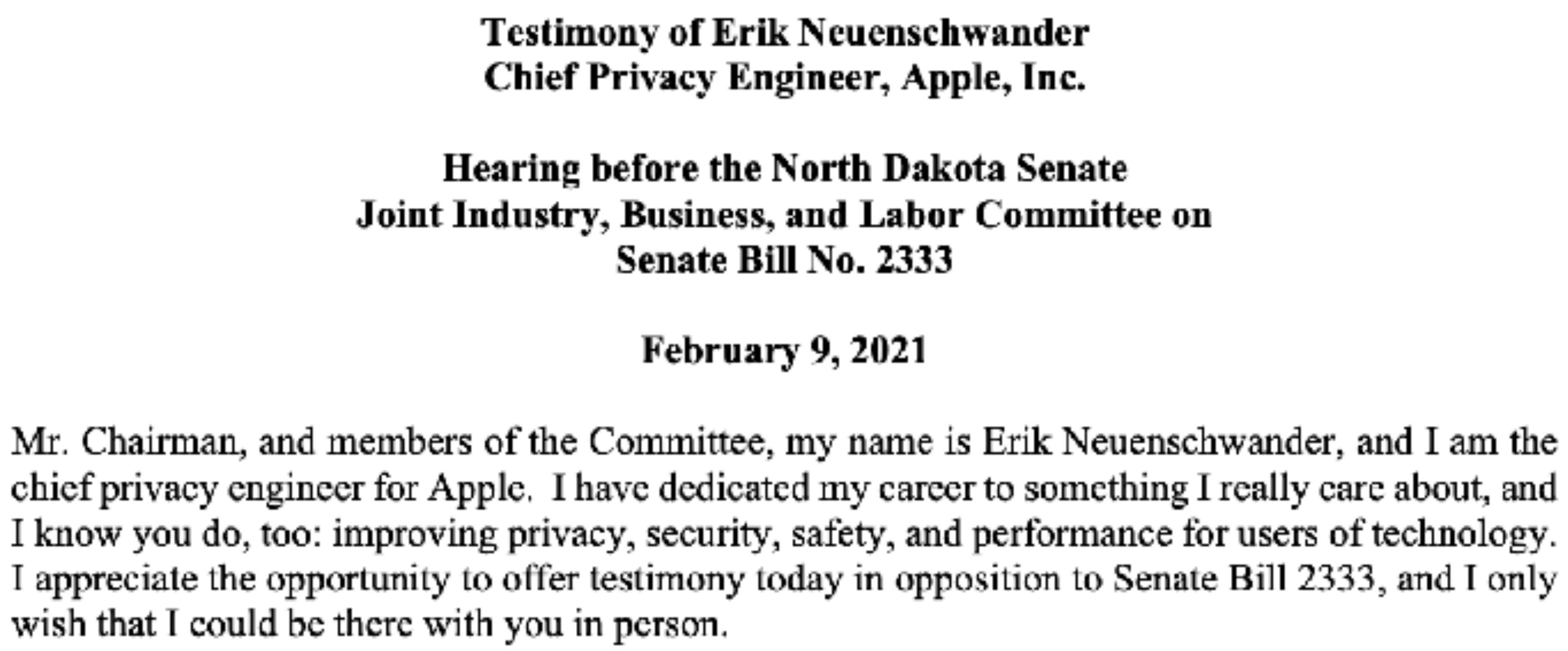
OS provisions

- Must allow users to **uninstall pre-installed software** unless it is technically necessary for the functioning of the OS/device AND cannot be offered on a standalone basis by third parties.
- Allow effective installation and use of **third party software** and app stores, and allow these to be accessed other than through the core service of the gatekeeper. BUT can take ‘proportionate measures’ to ensure integrity of hardware/OS.
- Must not technically restrict users from “switch[ing] between and subscrib[ing]” to different software applications and services accessed using the OS, including Internet access provider (device neutrality).

Where does this leave us?

- Less power for operating systems as gatekeeper?
- Less ability to penalise users for not running protocols?
- Big questions for system design, security, operating systems.
- Potential new avenues for conditionality of third party software without app stores as proxy privacy regulators.
- **Expect platforms to double down on PETs to create privacy and security reasons to eliminate competition and not be able to follow rules to open up and limit their power. PETs researchers need to engage with this to create protocols which don't have centralising tendencies.**

Already seeing big fights

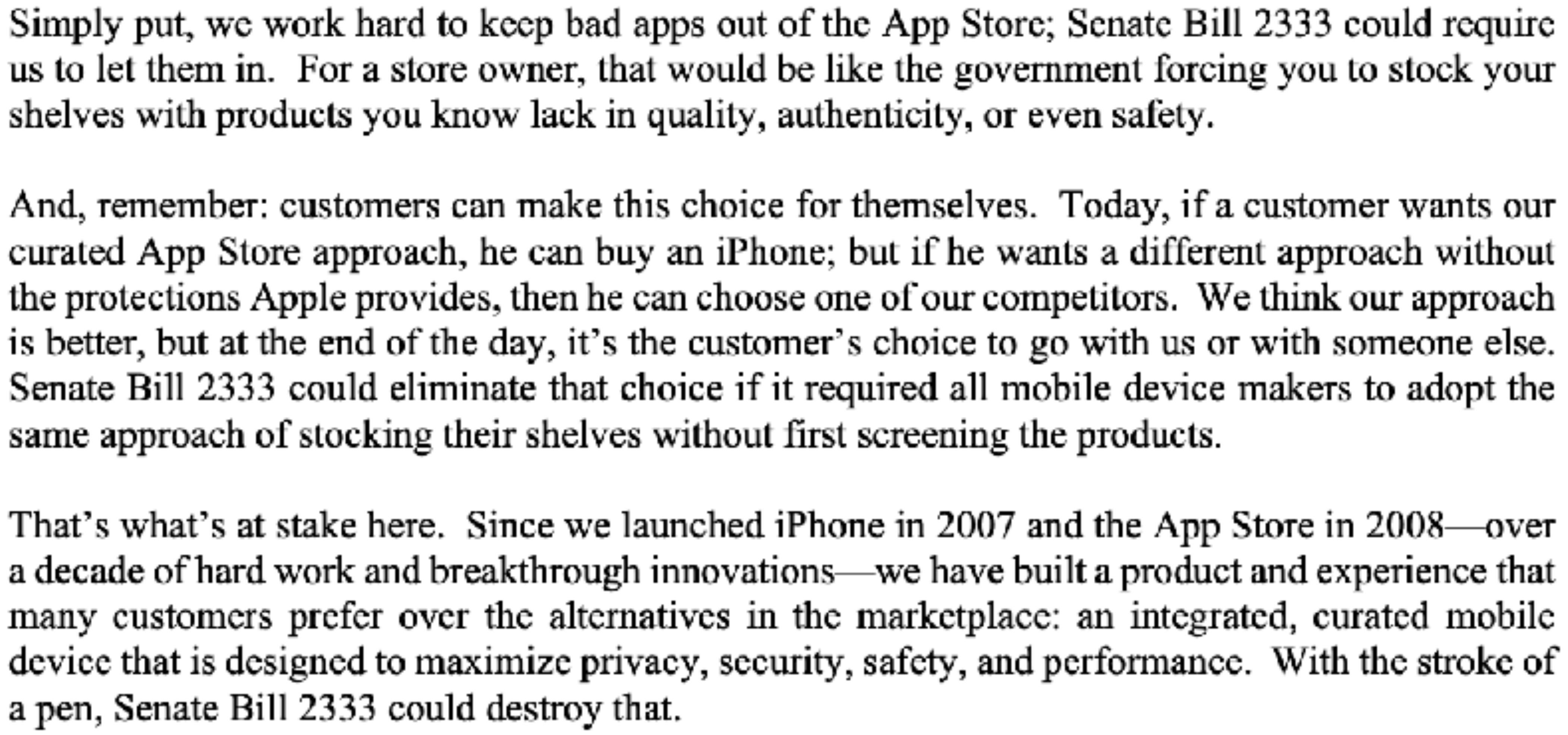


Testimony of Erik Neuenschwander
Chief Privacy Engineer, Apple, Inc.

Hearing before the North Dakota Senate
Joint Industry, Business, and Labor Committee on
Senate Bill No. 2333

February 9, 2021

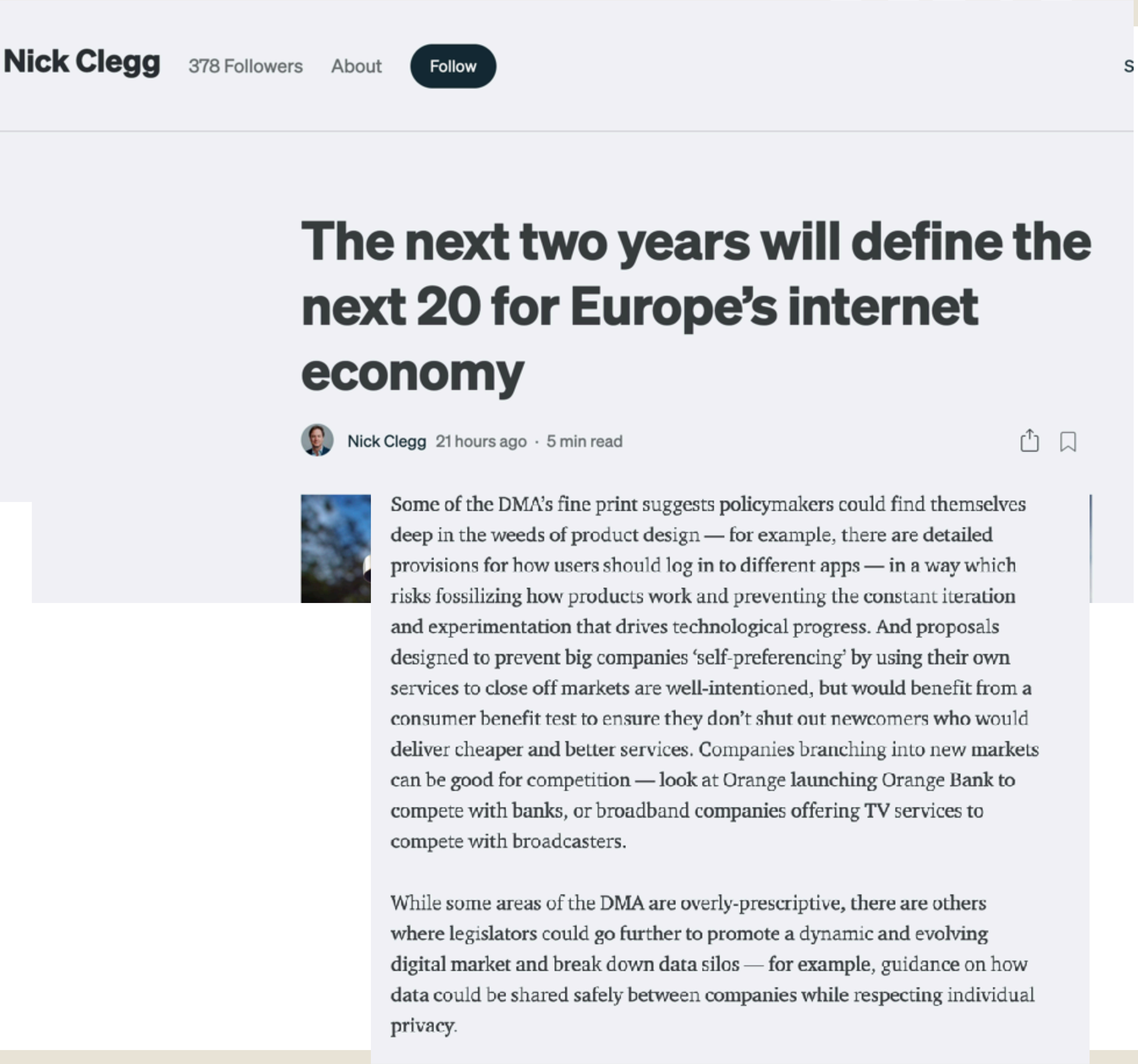
Mr. Chairman, and members of the Committee, my name is Erik Neuenschwander, and I am the chief privacy engineer for Apple. I have dedicated my career to something I really care about, and I know you do, too: improving privacy, security, safety, and performance for users of technology. I appreciate the opportunity to offer testimony today in opposition to Senate Bill 2333, and I only wish that I could be there with you in person.



Simply put, we work hard to keep bad apps out of the App Store; Senate Bill 2333 could require us to let them in. For a store owner, that would be like the government forcing you to stock your shelves with products you know lack in quality, authenticity, or even safety.

And, remember: customers can make this choice for themselves. Today, if a customer wants our curated App Store approach, he can buy an iPhone; but if he wants a different approach without the protections Apple provides, then he can choose one of our competitors. We think our approach is better, but at the end of the day, it's the customer's choice to go with us or with someone else. Senate Bill 2333 could eliminate that choice if it required all mobile device makers to adopt the same approach of stocking their shelves without first screening the products.

That's what's at stake here. Since we launched iPhone in 2007 and the App Store in 2008—over a decade of hard work and breakthrough innovations—we have built a product and experience that many customers prefer over the alternatives in the marketplace: an integrated, curated mobile device that is designed to maximize privacy, security, safety, and performance. With the stroke of a pen, Senate Bill 2333 could destroy that.



The next two years will define the next 20 for Europe's internet economy

Nick Clegg 21 hours ago · 5 min read

Some of the DMA's fine print suggests policymakers could find themselves deep in the weeds of product design — for example, there are detailed provisions for how users should log in to different apps — in a way which risks fossilizing how products work and preventing the constant iteration and experimentation that drives technological progress. And proposals designed to prevent big companies 'self-preferencing' by using their own services to close off markets are well-intentioned, but would benefit from a consumer benefit test to ensure they don't shut out newcomers who would deliver cheaper and better services. Companies branching into new markets can be good for competition — look at Orange launching Orange Bank to compete with banks, or broadband companies offering TV services to compete with broadcasters.

While some areas of the DMA are overly-prescriptive, there are others where legislators could go further to promote a dynamic and evolving digital market and break down data silos — for example, guidance on how data could be shared safely between companies while respecting individual privacy.