UNSW Law & Justice Research Series

Global Data Privacy Laws: EU Leads US and the Rest of the World in Enforcement by Penalties

Graham Greenleaf

[2023] *UNSWLRS* 47
(2023) 181 *Privacy Laws & Business International Report* 24

UNSW Law & Justice
UNSW Sydney NSW 2052 Australia

E: LAW-Research@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Global data privacy laws: EU leads US and the rest of the world in enforcement by penalties

Graham Greenleaf, Professor of Law & Information Systems, UNSW Sydney

(2003) 181 *Privacy Laws & Business International Report* 24-29*

Data privacy laws on paper mean little by themselves, even if they are ubiquitous.[1] It is only through evidence of their enforcement, or through convincing evidence of compliance with them irrespective of enforcement, that we can be satisfied that they cause behavioural change. Evidence of compliance requires large-scale sociological enquiry and is available very rarely. Evidence of enforcement is easier to obtain (though still a non-trivial task), and can be extracted from the records of courts, data protection authorities (DPAs), government agencies, and other authorities responsible for data privacy enforcement, and from non-government organisations (NGOs) and academic institutes which keep track of such matters. Cases that are settled before a penalty or compensation verdict is announced will also often have financial settlement that are public, particularly in the US.

This article gives a snapshot of the penalties and settlements included in recent data privacy decision across the globe. It lists enforcement instances only for the last two years, from 1 February 2021-31 January 2023 (abbreviated as '2021-02'), to better allow comparisons across this study, and with its future editions.

The focus of this article is the large multinational companies that dominate the Internet, often described as 'platforms', such as Google, Meta/Facebook, Twitter, Microsoft,WhatsApp, *youtube*, TIK TOK, Clearview, Grindr, Apple and Uber. These platforms need to be distinguished from companies, often large, that have a primarily 'domestic' customer base or audience.

What is the minimum quantum of penalties likely to have a 'dissuasive effect' on the continuation of abusive surveillance activities by such platforms? This is necessarily a subjective asdsessment, because it is too early in the study of the effects of enforcement for there to be sufficient useful data for an objective assessment. The financial resources of the leading firms (platforms) that rely on customer and citizen data (and of states that use their

* This version contains details of three extra US cases than the published version, omitted for space reasons, and some typographical errors have also been corrected.

[1] G. Greenleaf 'Global data privacy laws 2023: Ubiquity near with 162 countries' laws, 20 Bills' (2023) *Privacy Laws & Business International Report* 181 (in publication)

methods) is so high that it is difficult to imagine that penalties of less than €5 million or US$5 million (usually within 10% of each other), would have any effect, and only then if repeated regularly and in different countries. The enforcement examples below therefore have a minimum of €/US$5 million penalties (though some between €/US$5 and €/US$1M are also noted). Some decisions with penalties much lower than €/US$5M may have a very valuable domestic effect, but it is the global effect that is the focus of this article. Whether this threshold is too high or too low, and other criticisms of this approach, deserves further discussion.

There are few known examples outside Europe or the United States which meet the criterion of €/US$5M (million) in penalties, therefore they have been grouped together as 'Rest-of-the-World (ROW) enforcement'. The US is considered after the EU, then the ROW.

European Union enforcement

The three main sources for EU enforcement data are, first, the decisions aggregated by the European Data Protection Board (EDPB)[2] of most[3] national DPAs in the EU (including the UK, for this time period). The second source is the 'GDPR Hub' website[4] of the NGO None of Your Business (NOYB), which aggregates summaries of decisions from the same sources (but includes all national DPAs[5]), and national and European courts. The third source is the CMS Law[6] GDPR Enforcement Tracker,[7] which has similar coverage. In the decisions noted below, these sources are identified as 'EDPBsite', 'GDPRHub' and 'ETracker'. Each extensive site summarises many hundreds of decisions involving penalties,[8] but none of the three are comprehensive.

All of the 25 decisions listed below involve penalties of at least €5M, summarised below (paraphrased from the three aggregators' website data). The decisions are ordered by the amount fined.

> NCPD (Luxembourg) 01.07.2021 reported (by Amazon) to have fined **Amazon** €746 million for using customer's data without explicitly telling them; without a viable way to opt out without penalty and numerous other GDPR breaches (numerous news sources).

---

[2] EDPB national decisions <https://edpb.europa.eu/edpb_en>

[4] GDPR Hub <https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub> is a wiki in which the summaries are written by volunteers, under the general supervision of editor Jennifer Baker. As at January 2023 it contains summaries of over 2,000 decisions,

[5] GDPR Hub lists the DPAs of all 30 countries in the EU and EEA, plus the UK, and the EDPS and EDPB; https://gdprhub.eu/index.php?title=Category:DPA_Decisions. It allows the decisions of 56 DPAs to be separately inspected. However, whereas there are 127 decisions by the Garante (Italy), there are only 19 from all Germany's DPAs, so the completeness of the data is called into question.

[6] CMS is an international law firm < https://cms.law/en/int/>

[7] CMS Law GDPR Enforcement Tracker < https://www.enforcementtracker.com/>

[8] Of the 2,000 decisions summaries recorded by *noyb***,** 209 decisions involving penalties were made in the two year period 1/2/2021 – 31/1/2023.

EDPB/DPC (Ireland) 12.01.2023 fined **Meta** a total of €400M (**Facebook** €210 million and **Instagram** €180 million) for activities including lack of lawfulness and transparency of processing for behavioural advertising. DPC adopted European Data Protection Board (EDPB) binding decision.[9] (EDPBsite; ETracker).

EDPB / DPC Ireland 28.07.2022 – 'The EDPB adopted a binding decision, following which the Irish DPC fined **Meta** €405M for the lack of legal grounds for processing contact information on children's business accounts and 'public by default'-settings for child users'. (GDPRHub; ETracker).

DPC (Ireland) 25.11.2022 fined **Meta** €225M for inadequate security when a dataset containing personal data from up to 533 million Facebook users was made available on a hacking platform (ETracker).

EDPB/DPC (Ireland) 20.08.2021 fined **WhatsApp** Ireland Limited €225M for negligently violating various GDPR articles, particularly the transparency requirements, and ordered compliance within 3 months. The EDPB reviewed the DPA's decision and required a higher fine (GDPRHub; ETracker).

CNIL (France) 31.12.2021 fined **Google LLC** €90M and **Google Ireland Limited** €60M (total €150M) because (*inter alia*) of their failure to offer French users a means of refusing to give consent that is as simple as the mechanism provided for their acceptance, on google.fr and on youtube.com (GDPRHub).

CNIL (France) fined **Microsoft** €60M for installing on "bing.com" non-essential cookies without valid consent (GDPRHub).

Garante (Italy) 16.12.2021 fined **Enel Energia** €26.5M for unlawfully processing the personal data of millions of users for telemarketing purposes and imosed multple corrective measures (GDPRHub).

Garante (Italy) 10.02.2022 fined **Clearview** €20M for conducting facial recognition on public web sources, prohibited further processing, and required deletion of personal data already collected (GDPRHub).

Hellenic DPA (Greece) 13.7.2022 fined **Clearview AI** Inc €20M for processing images taken from the web without a valid legal basis, failing to provide transparency, and failure to provide access to data subjects (ETracker).

CNIL (France) fined **Clearview AI Inc** €20M for processing images taken from the web without a valid legal basis, and for restricting the exercise of data subject's rights (ETracker).

DPC (Ireland) fined **Meta** €17M for inadequate security measures, resulting in twelve data breach notifications. The EDPB became involved due to cross-border factors requiring the co-decision procedure (Etracker).

DPA of Lower Saxony (Germany) 8.1.2021 fined electronics retailer **notebooksbilliger.de** €10.4M for video-monitored its employees for at least two years without having a legal basis (ETracker).

AEPD (Spain) fined **Google** €10M after data subjects complained **Googl**e had disclosed their personal data to Harvard's Berkman Klein Center without authorization (ETracker).

DPA (Austria) 28.09.2021 fined **Austrian Post** €9.5M for not allowing data protection-related inquiries via e-mail (ETracker).

---

[9] EDPB *Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service* (Art. 65 GDPR)

ICO (UK) 18.05.2022 fined **Clearview** €9M for operation of a facial recognition database without a proper legal basis, with inadequate transparency, and other breaches (ETracker).

AEPD (Spain) 11.03.2021 fined **Vodaphone** €8.5M arising from 191 complaints about direct marketing calls without consent (ETracker).

DPA (Austria) fined REWE International AG €8M for various breaches (unknown) (ETracker).

CNIL (France) 19.12.2022 fined **Apple** Distribution International €8M for implementing its advertising identifiers on Apple devices without prior consent from French users (GDPRHub).

Datatilsynet (Norway) 13.12.2021 fined **Grindr** over €6M for failing to collect users' valid consent for sharing data with third parties for profiling and advertising purposes (GDPRHub).

Hellenic DPA (Greece) 27.01.2022 fined **Cosmote Mobile Telecommunications** €6M for inadequate security and numerous other breaches, arising from a data breach (ETracker).

AEPD (Spain) 13.01.2021 fined **Caixabank** €6M for requiring customers to accept new privacy policies allowing the controller to transfer their personal data to all companies within the CaixaBank Group, with very limited means to opt out (ETracker).

EDPB/DPC (Ireland) 19.01.2023 fined **WhatsApp** Ireland Ltd. €5.5M, following a complaint filed by NOYB concerning WhatsApp compelled users to agree to new terms of service (ToU) in order to continue use but argued that its lawful basis for processing (which could not be consent) was a contract arising from the ToU. Six other DPAs disagreed and the EDPB's dispute resolution procedure was used, holding that contract could not be the lawful grounds for processing, and that there was inadequate transparency concerning the ToU, and insufficient attention to the principle of fairness. The DPC is to further investigate remaining issues and issue appropriate fines which are 'effective, proportionate and dissuasive, in the sense that this amount can simply be absorbed by the undertaking as an acceptable cost of doing business'.

ICO (UK) 24.10.2022 fined **Interserve** Group Limited €5.1M for 57K unsolicited direct marketing calls where there was no informed valid consent (GDPRHub).

CNIL (France) 9.12.2022 fined **TikTok** €5M for implementing advertising identifiers on devices without prior consent of users who visited TikTok's main website, and for other breaches. (GDPRHub).

Comments on the EU penalty decisions

The decisions in 2021-22 involving the largest fines are against Amazon (€746M), Meta (€400M); WhatsApp (€225M); Google (€150M); Microsoft (€60M); and Clearview (3 €20M decisions).

Twenty of these 25 decisions involving penalties of at least €5M have defendants with international operations, platforms who are involved in economic surveillance. The parties to these decisions indicate that the €5M penalty threshold is largely restricted to cases involving the 'whales' of internet surveillance: Microsoft; Google (multiple times); Facebook/Meta (multiple times); WhatsApp; *youtube*; TIK TOK, Vodaphone; Clearview A.I.; Grindr; and Apple.

There are numerous decisions (at least 50) where DPAs issue fines less than €5M but at least €1M. With only a few exceptions (Uber, various government ministries; Deliveroo,

Ticketmaster) these decisions are not against 'platforms' but against essentially 'domestic' defendants that do not have an international presence, even though they might be large economic players nationally. They include defendants such as a Polish marketing company; a Spanish supermarket chain; Italian telecoms, energy, fragrance and digital food distribution companies, and a French software company.

It seems therefore, that whether fines are more or less than €5M is a reasonably good discriminator between 'platform' and 'domestic' decisions.

Penalties over €5M are primarily from the CNIL (France), ICO (UK), Garante (Italy), AEPD (Spain) and DPC (Ireland) (sometimes as required by the EDPB), but the three aggregation sites do include decisions from many other EU DPAs.[10]

The decisions concerning the DPC (Ireland) which require co-decision-making by the EDPB because of their cross-border elements, and may involve the GDPR's dispute resolution procedures, are demonstrating how an effective EU-wide result is being achieved. These complaints are also generating the highest fines, without one DPA having to take all the responsibility for the decision. The three €20M fines against Clearview from three different DPAs also show another means by which DPAs can reach consistent decisions.

United States enforcement examples

US enforcement decisions come from different courts and authorities. Penalties agreed to in settlements (particularly of class actions) also have to be taken into account in the US context, as indicated in the list following. The decisions noted here include all Federal Trade Commission decisions involving penalties of more than $5M in 2021-22 included by the FTC on its 'Privacy and Security Enforcement' page.[11] FTC also enforces the COPPA legislation.

These decisions are presented in order of the size of the penalty.

> FTC 19.12.2022 secured a settlement requiring **Epic Games**, Inc, creator of Fortnite 'to pay a total of $520 million in relief over allegations the company violated the Children's Online Privacy Protection Act (COPPA) and deployed design tricks, known as dark patterns, to dupe millions of players into making unintentional purchases.' Epic will pay a $275 million monetary penalty for violating the COPPA Rule - 'the largest penalty ever obtained for violating an FTC rule' and adopt strong privacy default settings. 'Epic will pay $245 million to refund consumers for its dark patterns and billing practices, which is the FTC's largest refund amount in a gaming case, and its largest administrative order in history'.[12]
>
> Forty US state governments 14.11.2022 announced settlement with **Google** of a of US$391.5M class action, location tracking practices, alleging it tracks users based on their

[10] These include decision, for those that have awarded penalties in 2021-22, from; AP (The Netherlands); UODO (Poland); Datatilsynet (Norway); NAIH (Hungary); IMY (Sweden); DVI (Latvia); Tietosuojavaltuutetun toimisto (Finland); DSB (Austria); and APD/GBA (Belgium).

[11] FTC Privacy and Security Enforcement' <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement>

[12] Epic Games, In the Matter of <https://www.ftc.gov/legal-library/browse/cases-proceedings/1923203-epic-games-matter> ; FTC Press Reslease <https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations>

phone location to serve ads, despite users explicitly opting out of such tracking. This is the largest multi-state privacy settlement in US history.[13]

In *Rogers v* ***BNSF Railway Co***, No. 1:19 CV3083 (NDILL 2022) an Illinois jury in December 2022 awarded a US$228M class action verdict under the Illinois *Biometric Information Privacy Act* (BIPA) because BNSF scanned and retained employees' fingerprints over 45,600 times without obtaining written informed permission, and without publishing a retention and destruction notice. This is the first verdict under BIPA. (Anderson Kill website)

FTC 25.05.2022 imposed on **Twitter** a US$150 million civil penalty for collecting personal data on the ostensible basis of security protection, then used it for marketing purposes.[14]

Northern District of Illinois District Court July 28.07.2022, approved a US$121M class action settlement **by TikTok** (Chinese company ByteDance) of various privacy claims under state and federal law. Tik Tok violated the Illinois Biometric Information Privacy Act (BIPA) and the federal Video Privacy Protection Act (VPPA) by improperly harvesting users' personal data.[15].

Northern District of California District Court 14.11.2022 approved a US$90M privacy settlement against **Meta** Platforms, Inc. (formerly Facebook, Inc.) for unlawfully tracking user information when users were logged out of the site (Hunton).

US District Court in San Jose, California 03.11.2021 refused to dismiss claims that **Zoom** had breached contract and good faith with users entrusting it with their data, resulting in 'Zoombombing' of conferences with embarrassing content by third parties. The case was settled for US$85M.[16]

US District Court, Southern District of New York 14.02. 2022, Noom Inc., a popular weight loss and fitness app, agreed to pay US$56M for using 'dark patterns' to prevent users from unsubscribing.[17]

In plaintiffs v **Snapchat** (US District Court, N. Dist. Illinois), a court-approved settlement in November 2022, Snapchat agreed to pay US$35M to settle an action under the Illinois *Biometric Information Privacy Act* (BIPA) in an action alleging Snapchat features like 'lenses' and 'filters' were used to collect user's unique biometric facial features without consent, and to store them. Snapchat denies breaching BIPA. (5Chicago website, 23 January 2023)

FTC 29.04.2021 reached a settlement with smart home security and monitoring company **Vivint Smart Homes** Inc. by which it agreed to pay US$20 million to settle FTC allegations

---

[13] Sumeet Wadhwani 'Why Google's $391.5M Settlement With 40 States Over Privacy Concerns is Just a Smokescreen' *Spiceworks Ziff Davis* 15 November 2022 < https://www.spiceworks.com/it-security/data-security/news/google-privacy-settlement-with-us-states/

[14] Federal Trade Commission (FTC) 'Twitter to pay $150 million penalty for allegedly breaking its privacy promises – again' FTC blog <https://www.ftc.gov/business-guidance/blog/2022/05/twitter-pay-150-million-penalty-allegedly-breaking-its-privacy-promises-again>

[15] Summarised in Hunton Andrews Kurth *Security Law Blog* https://www.huntonprivacyblog.com/tag/class-action/>

[16] Carlo Massimo 'The Top 5 Data Privacy Penalties Post-GDPR' *Information Week*, 7 December 2022 <https://www.informationweek.com/strategic-cio/the-top-5-data-privacy-penalties-post-gdpr>

[17] Hunton Security Law Blog op cit

that the firm misused credit reports to help unqualified customers obtain financing for its products and services.[18]

Forty State Attorneys-General, in January 2023, obtained a US$16M class action settlement with **Experian and T-Mobile** because of a data security breach when an unauthorised third party accessed the records of around 15 million people, obtaining Social Security and other identity numbers of T-Mobile customers, for data stored on Experian's servers. (Top Class Actions website)

FTC 15.12.2022 lawsuit shut down **The Credit Game**, a fraudulent credit repair scheme, and included a monetary judgment of nearly US$19M against the operators.[19]

Because there are few US cases of US$5M or more, decisions over US$1M are also worth mention.

FTC 01.07.2021 settled allegations against providers of **online colouring book Recolor** that it collected children's information in breach of COPPA (Children's Online Privacy Protection Act) by not obtaining parental consent. The settlement included a US$3M penalty.[20]

FTC 15.12.2021 ordered that **OpenX Technologies**, Inc. be required to pay US $2M over allegations that the company collected personal information from children under 13 without parental consent, and that the company collected geolocation information from users who specifically asked not to be tracked.[21]

California Attorney General 30.08.2022 obtained a US$1.2M settlement against **Sephora USA**, Inc, set out in a final judgement in the California Superior Court. This was the first court order enforcement of a California Consumer Privacy Act (CCPA) settlement. The Act provides for fines of up to $2,500 per violation and up to $7,500 per intentional violation, and cumulatively the violations amounted to US$1.2M. The numerous breaches related to the use of cookies, defined as personal information in the Act, their sale, the lack of agreements limiting further use, and the lack of an opt-out.[22]

There are also some important FTC cases not listed here because no penalty was included in a settlement (eg Everalbum's use of facial recognition technology; the SpyFone 'stalkerware').[23]

---

[18] FTC: Vivint Smart Home, Inc. < https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3060-vivint-smart-home-inc>

[19] BoostMyScore LLC < https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3059-boostmyscore-llc>

[20] Kuuhuub, Inc., et al., U.S. v. (Recolor Oy) < https://www.ftc.gov/legal-library/browse/cases-proceedings/182-3184-kuuhuub-inc-et-al-us-v-recolor-oy>

[21] FTC: 'OpenX Technologies, Inc'. < https://www.ftc.gov/legal-library/browse/cases-proceedings/1923019-openx-technologies-inc>

[22] Benesch Attorneys at Law 'First Civil Penalties Under the CCPA Through $1.2 Million Settlement For Cookie "Sale" Violations' *Lexology***,** 7 September 2022

[23] These include cases in which the FTC issues an administrative complaint because it has 'reason to believe' that the law has been or is being violated, and it appears to the Commission that a court proceeding is in the public interest. When the Commission issues a consent order on a final basis, it carries the force of law with respect to future actions. Each violation of such an order may result in a civil penalty of up to $43,280. Such penalties do not meet the criteria of a US$1M fine.

The number of FTC decisions in 2021-22 is considerably fewer than in previous years, when they averaged about two decisions per month. Scholars have concluded that FTCs fines do not cause general or even specific deterrence.[24]

Two valuable websites track penalties and settlements for violations in 2022-23 of the *Health Insurance Portability and Accountability Act of 1996* (HIPAA). Although it is a sectoral law, rather than a general data privacy law it is a significant long-established law. The HIPAA Fines Listed by Year database[25] lists what it calls 'large scale' HIPPA fines. Three fines listed are for more than US$250,000, the largest being for 875,000. The rest are all under US$100,000, typically about US$40,000. The Resolution Agreements database[26] is a government (HHS) database from which all data in the HIPPA fines database is derived. So there are no HIPPA fines in 2021-22 of US$1million or more, although there have been in past years. It does not appear that there are similar databases for breaches of other significant US privacy laws (federal Privacy Act; GLBA; COPPA; or FACTA).[27]

The largest US penalties (US$20M or more) in 2021-22 concern Epic Games (US$275M); Google (US$391.5M); *Rogers v BNSF Railway Co* (US$228M); Zoom (US$85M); Tik Tok (US$121M); Meta (US$90M); and Twitter (US$50M). Five of largest six decisions or settlements are against Internet 'whales', one of more of domestic concern. They are fewer large decisions than in the EU (10 of at least €20M). Data privacy enforcement in the US still lags well behind Europe, but the development of 'comprehensive' US state laws may change this, as may a potential federal law.[28] Some sectoral US state laws, such as the Illinois Biometric Privacy litigation, also result in significant penalties. Class action litigation, is likely to result in the highest privacy remedies, and many large cases are still awaiting completion of settlements. The US Supreme Court has restricted standing to bring federal cases in a 2021 case on the FCRA (TransUnion LLC v. Ramirez), so it is more likely that future class actions will be before state courts.[29]

Rest-of-the-World enforcement

Privacy invasion by large Internet platforms is a global phenomenon and can only be put fully into decline if many of the of the 131 countries with data privacy laws outside the EU and the US refuse to accept its practices.[30]

---

[24] Chris Jay Hoofnagle 'The Federal Trade Commission's Inner Privacy Struggle' in Selinger, Polonetsky and Tene (2018, Cambridge University Press

[25] HIPPA fines < https://compliancy-group.com/hipaa-fines-directory-year/>

[26] HIPPA Resolution Agreements and Civil Money Penalties < https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html>

[27] See Amakiri Welekwe 'A Guide to the Federal and State Data Privacy Laws in the U.S.' *Comparitech website*, 19 October 2022 < https://www.comparitech.com/data-privacy-management/federal-state-data-privacy-laws/ > for brief details of each of these laws.

[28] G. Greenleaf 'Global data privacy laws 2023: Ubiquity near with 162 countries' laws, 20 Bills', cited above

[29] Fred D Bellamy 'Data breach class action litigation and the changing legal landscape' *Westlaw Today*, 28 June 2022

[30] Greenleaf, op cit

There are as yet very few decisions from the rest of the world involving penalties above the threshold of €1M (or US$1M). This is sometimes because local laws do not have provision for penalties of that magnitude, but sometimes (as in Australia) such provisions exist but have never been used.

Here are some of the few decisions involving penalties exceeding or approaching US$5M during 2021-02:

> China's CAC (Cyberspace Administration of China) 21.07.2022 fined China's largest **ride-hailing company Didi** around US$1.2 billion (RMB 8.026 billion) for violating data protection laws, including the Cybersecurity Law, Data Security Law and Personal Information Protection Law. In addition, the CEO and the President of the company were each personally fined RMB 1 million (around $150,000 USD). Sixteen violations included illegal collection of large volumes of data on passengers, such as screenshots from albums on mobile devices, user clipboard information and application list information, facial recognition data, and age-related data. Didi also failed to accurately specify the processing purposes for 19 different types of personal information.[31]
>
> South Korea's PIPC 14.09.22 fined **Google and Meta** a total of US$72M (100 billion won), comprised of US$50M against Google and US$22M against Meta. 'This is the largest penalty in South Korea for violating personal information protection laws and the country's first sanction pertaining to the collection and use of behavioural information on online customized advertising platforms, according to the [PIPC]'[32].They ordered the companies to correct the violations. Some earlier decisions by the PIPC and previous Korean regulators had exceeded US$6M. In 2020 PIPC fined Facebook US$5.arising from the Cambridge Analytica breach affecting about 3 million Korean users.
>
> South Korea's PIPC 01.09.2021 fined **Facebook** US$5.6M for violations of PIPA, including collecting facial recognition data without users' consent; collecting Social Security numbers in violation of the law; and failing to disclose information about its transfer of personal data to third parties or overseas[33]. Sources indicate the PIPC also is requiring Facebook to destroy the facial recognition information and identity numbers and to disclose to users information about any transfer of personal data to third parties.
>
> South Korea's PIPC 28.10.2021 fined '**Genius Textbook'** about US$750,000 for allowing another company Genius Education to access its student-user database of about 23,000 users.[34]

The Chinese and South Korean decisions illustrate that DPAs and PEAs outside the EU or US are capable of issuing penalties comparable with those that would be issued in the EU or US, and occasionally do so. The only 'billion dollar data protection fine' in 2021-22 came from China, not from the EU or US. All of these decisions are against Internet 'whales'.

---

[31] Paraphrased from Yan Luo, Xuezi Dan & Nicholas Shepherd 'China Imposes $1.2 Billion Fine for Data Violations' Covington website, July 25, 2022 < https://www.insideprivacy.com/data-privacy/china-imposes-1-2-billion-fine-for-data-violations/>

[32] Kate Park 'Google, Meta fined $71.8M for violating privacy law in South Korea' TechCrunch 14 September 2022. <https://techcrunch.com/2022/09/14/google-meta-fined-71-8m-for-violating-privacy-law-in-south-korea/ >

[33] Hunton and Williams blog 'South Korean Privacy Regulator Fines Netflix and Facebook' 1 September 2021 <https://www.huntonprivacyblog.com/2021/09/01/south-korean-privacy-regulator-fines-netflix-and-facebook/>

[34] KS Park has assisted with information about these Korean cases.

Singapore's very transparent system for reporting enforcement decisions[35] shows that in 2021-22 its PDPC made no decisions involving penalties over S$100K (less than US$100K). In 2020 it imposed one fine of S$120K and in 2019 one decision with total fines of S$1M against two parties (SingHealth and IHiS)**.** Prior to 2019 it made no decisions with penalties over S$100K. We can see from its website that the 'whales' of surveillance capitalism do not appear as parties before its PDPC, and for its 'domestic' cases it is capable of fines over US$1M, but has only once approached that.

Until 2022 Japan's PPC had no power to make penalty decisions over JPY500K (about US$5,000), but 2021 amendments to Japan's law (in force April 2022) raised this maximum to approximately US$775,00 (100M JPY). PPC's English language website contains no information about enforcement decisions or penalties, but its Japanese language website does.[36] It lists only one case: PPC filed a criminal proceeding 11.01.2023, for publishing and locating bankrupts' personal data (originally published in the Official Gazette) on Google Maps. The Prosecutor's Office must decide whether to prosecute, and the courts whether to inflict a penalty. PPC has never previously published any monetary penalty cases. Settlements arising from the equivalent of class actions are possible, but details are not known.[37]

No decisions involving fines over US$5M (or even US$1M) are known from elsewhere: the rest of Asia; Africa; the Mid-East; the Caribbean; Latin America, Central Asia or the non-EU/EEA Council of Europe countries. In many countries the data privacy laws set maximum limits on penalties, or on compensation, that is much lower than US$1M. For example, under Canada's PIPEDA, and some provinces like Alberta, the maximum fine allowed is C$100K. Australia has legislated to increase privacy penalties for serious or repeated interferences with privacy, with maximum penalties now the greater of (i) A$50m, or (ii) three times the benefit of a contravention, or (iii) where the benefit can't be determined, 30% of domestic turnover. No decisions have yet been made under these provisions, so fines of US$1M are for the future.

The largest African fine may be that Angola's National Data Protection Agency (APD) 29.04.2022, fined Banco de Poupança e Crédito, a government-owned bank US$525,000 for public disclosure of employee data.[38] More typical is the first fine imposed by Kenya's OCPD 21.12.2022, US$43,000 against OPPO Kenya.[39]

---

[35] PDPC (Singapore) <https://www.pdpc.gov.sg/All-Commissions-Decisions>

[36] Korea's PIPC English language website has also removed all enforcement decisions from its site, but at least we know it make such decisions.

[37] Hiroshi Miyashita has provided information on which this paragraph is based.

[38] Angola decision <https://www.dataguidance.com/news/angola-apd-fines-bpc-525000-public-disclosure-employee>

[39] Kenya decision; <https://bowmanslaw.com/insights/data-protection/kenya-the-office-of-the-data-protection-commissioner-issues-decisions-in-the-determination-of-complaints/ >

In the 18 Council of Europe countries that are outside EU/EEA,[40] there are no fines over US$1M. In many of these countries the legislation sets lower maximum limits on fines.[41]

There are two significant decisions on penalties, though for less than US$1M:

> Personal Data Protection Board (Turkey) 03.09.2021 fined **WhatsApp** approx. €200,000 (TRL 1,950,000). The Board held that WhatsApp's explicit consent requirement did not meet the condition of 'free will' and that no explicit consent was obtained for transfer of data abroad, or concerning processing via cookies for profiling purposes.
>
> A Moscow Magistrate's Court (Russia) 16.06.2022 fined **Google LLC** €250,000 (15M rubles), applying administrative protocols drawn up by Roskomnadzor, for repeatedly refusing to localize the databases of Russian users on the territory of the Russian Federation.[42] Previously, in 2021 Google was fined 3 million rubles for violating the localization requirement.

From Latin America, no fines over US$1M are known for 2021-22, and in some countries the legislation sets lower maximum limits on fines.[43] However, in 2015 Mexico's DPA fined three financial institutions US$1.9M (M$36.424.892) for transfers of data without consent.

Enforcement other than by penalties or settlements

Enforcement serious enough to threaten the business model of global platforms is not restricted to financial penalties or compensation/settlements. Some of the most threatening forms of enforcement are (i) injunctions against practices; (ii) account of profits; (iii) prison sentences on individuals; and (iv) loss of a businesses' licence to operate. Examples of each have occurred, but are not so readily locatable as penalties, particularly if only for 2021-2. They are not covered in this article.

Conclusions about global enforcement

Many countries, in all regions, have legislated for low upper limits (under US$1M) for fines (or compensation), preventing penalties in these countries for being any more than a nuisance for global platforms, even though they may be effective deterrents to 'domestic' companies. The European Union is the only region in which countries make decisions which very regularly impose fines of €5M or more, and in some cases between €100M and €500M. The US (which is a region, not only a country) is somewhat behind the EU but nevertheless delivers settlements of US$5M or more with increasing frequency. North Asia (China and Korea) is the only other region as yet with decisions imposing such penalties, and the *Didi decision* (China) is the only penalty in excess of US$1 billion as yet.

---

[40] Tamar Kaldani provided the data for this section.

[41] For example, Albania, Georgia, Montenegro, and Serbia.

[42] Part 9 of article 13.11 of the Code of Administrative Offenses of the Russian Federation; see <https://rkn.gov.ru/news/rsoc/news74356.htm>

[43] For example, in Argentina, the maximum fine is uS$1,200. Ana Brian Nougreres, Pablo Palazzi and Gonzalo Sosa provided information concerning Latin America.

Greenleaf – Global data privacy laws: EU leads US and ROW in enforcement by penalties

We can conclude that, globally, only the EU, US and some North Asian countries are currently significant in terms of whether the enforcement of their law might have a serious dissuasive effect on global platforms continuing objectionable privacy invasive practices. A more comprehensive global assessment of in which countries all fines (and other enforcement methods) in actual use are effective in dissuading 'domestic' companies from breaching data privacy laws might produce a different result. This study does not attempt that.

Like countries that do little to prevent cigarette smoking, some countries will continue to allow privacy-abusive practices, even when most countries globally have banned them. Even where they do ban certain practices in theory, low maximum penalties are the *de facto* way by which companies can continue those practices with impunity.

Valuable comments have been provided by Marc Rotenberg, Ana Brian Nougreres, Hiroshi Miyashita, Ian Brown, Tamar Kaldani, Chris Hoofnagle, Kyungsin Park, Gonzalo Sosa, Bob Gellman, Eduardo Bertoni and Pablo Palazzi, but all responsibility for content remains with the author.