Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Visiting Fellow, Yale University (Information Society Project)
Associate, Oxford Martin School, University of Oxford

Why the UK First-Tier Tribunal was fundamentally wrong to hold that the use of Clearview by foreign states is outside the scope of EU and UK law

1. Introduction

On 17 October 2023, the UK First-Tier Tribunal (General Regulatory Chamber) (hereafter: "the FTT") held that prior to the completion of the Brexit implementation period on 31 December 2020 ("IP completion day") – until when the EU General Data Protection Regulation (EU GDPR) still applied in the UK – the use of the surveillance system offered by the US company Clearview by non-UK law enforcement and intelligence agencies constituted "an activity which, immediately before IP completion day, fell outside the scope of EU law", and thus also outside the EU GDPR (para 154); and that after that date, when the modified UK GDPR applied, it was also outside the scope of the latter instrument (para. 156) – in spite of the fact that the FTT also held that the system was also, "inevitably", used to monitor the behaviour of UK residents (para. 103).

Below, at 2, I summarise the Clearview system and its uses (which are described in some detail in the decision itself, to which I therefore simply cross-refer).

At 3, I look at the reason why the FTT came to this conclusion, and show that that conclusion is actually fundamentally flawed. I provide some final comments at 4.

2. Clearview

Clearview (referred to in the FTT decision and the quotes from that decision, below, as "CV") collects billions of facial images that its automated systems "scrape" from the Internet, and also obtains such images from contractors (para. 30).

It stores these images in a database with "vectors" relating to each face that are also created automatically by algorithm and that allow similar faces to be indexed and correlated.

Clients who obtain Clearview's services can upload a facial image of an individual to Clearview's system; this is known as a "probe image" (para. 42). Upon that:

> The system will create vectors for the face in the Probe Image. These vectors are then compared to the vectors created from the Stored Images using a machine learning facial recognition algorithm with a view to delivering a match or matches to the client. The results of that comparison are delivered to the client as search results that show the Probe Image alongside thumbnails of any Stored Images that the system has identified as having sufficient similarity to it. The number of results is capped at 120 for each search due to technical reasons.
>
> The search results will include an assessment of the degree of similarity between each of the Stored Images returned by the search and the Probe Image, they will be presented in order of degree of similarity but no assessment of the accuracy of the matches is provided, the system does not indicate that the person in the Probe Image has been identified nor give a numerical percentage of confidence. The degree of similarity is represented by a coloured circle; a green circle indicates very close likeness between the vectors, whereas an amber circle would indicate a less strong likeness. The system does not say whether the images are of the same person, that decision is left to the client.
>
> (Paras. 42 – 43)

The ruling says that "[o]n a test by the US National Institute of Standards and Technology, a globally recognised test for facial recognition accuracy, CV's service achieved 99%+ accuracy statistics" (para. 44). That seems dubious to me, given the general low level of accuracy of algorithm-based matches of data[1] – but I will leave that aside here. More importantly:

> A client may use the results of the search to assist in making an identification or to assess what the person is doing when the photograph was taken from objects or activity shown within the image(s). Conclusions or inferences may be drawn from one, or more than one, image provided to the client as the results of their search, or from further information discovered by the client following the links provided with the search results. However, any such conclusions or inferences are made solely by the client and not by CV or its system.
>
> For example, the search may return numerous photographs of an individual participating in a sport from which a client may conclude that the person does so regularly, or is proud of so doing, as they frequently post pictures of themselves engaged in the activity.
>
> (Para. 48)

Given that Clearview is said to be used only by law enforcement and intelligence agencies (see below), a better example would be "numerous photographs of an individual participating in certain political demonstrations"; cf. the reference below to the system flagging up "whether the person has been arrested". But let me continue the quote:

> However, those would be deductions made by the human client who is viewing the results of the search.
>
> Each CV client has an administrator that liaises with the client and can access details of the search history, but CV does not have access to the results of the searches, even though these are retained on its infrastructure, this is as a matter of choice built into the system. CV has been provided with some examples of successful searches by clients. Examples of the results of searches that we were provided with demonstrate that information and inferences may be drawn (from the images returned by the search coupled with the additional information and visiting the sources of the images) about:
>
> a. The person's name;
> b. The person's relationship status, whether they have a partner and who that may be;
> c. Whether the person is a parent;
> d. The person's associates;
> e. The place the photo was taken;
> f. Where the person is based/lives/is currently located;
> g. What social media is used by the person;
> h. Whether the person smokes/drinks alcohol;
> i. The person's occupation or pastime(s);
> j. Whether the person can drive a car;
> k. What the person is carrying/doing and whether that is legal;
> l. Whether the person has been arrested.

[1] Cf. the statement that an "image enhancement tool" can "improve the effectiveness of the search" (para. 47). It would seem hardly feasible to "improve" on 99%+ accuracy.

> These pieces of information are gleaned by deduction from the image or images returned by the search coupled with the additional information and also may require visiting the sources of the image(s). It would be unlikely for a single image to reveal all of the above. Such information may alternatively be discovered by way of a manual internet search, but this would be more time consuming and would depend on the effective construction of the search terms.
>
> The search results may assist in the client making an identification of the person in the Probe Image, but it is for the client to make their own assessment using the results of the search in combination with other evidence they have gathered or will gather to establish the identity of the person. The search results may be the starting point for investigative steps that might not otherwise have been undertaken and may well be of importance to the eventual identification of the person in the Probe Image. The Service does not provide a definitive answer to the question of the identity of that person.
>
> (Paras. 48 – 51)

(Note; The Information Commissioner, in his submission to the FTT, distinguished two types of activity in relation to the above:

> a. Activity 1 processing, covering the creation, development and maintenance of the Database;
>
> b. Activity 2 processing, namely CV's receipt of the Probe Image from the client, matching the Probe Image against the Database, and then providing the search results to the client.
>
> (Para. 98) –

and considerable space is taken up by the analyses of the implications of this distinction. But since this short note addresses mainly the issue of whether or not the processing is, or is not, outside EU and UK law (as discussed below, at 3), I will not here go into these issues.)

Suffice it to note that Clearview's systems clearly allow for the gathering of highly intrusive personal information. Indeed, the FTT accepts that:

> CV is not simply processing the personal data in relation to one data subject … , but of millions if not billions of data subjects to facilitate the monitoring of behaviour by their clients.
>
> There is such a close connection between the creation, maintenance and operation of the Database and the monitoring of behaviour undertaken by the clients that CV's processing activities are related to that monitoring.
>
> (Paras. 142 – 143)

Clearview claimed that:

> as a matter of fact, the Service is only provided to non-UK/EU law enforcement or national security bodies and their contractors. There was no evidence to the contrary tendered on behalf of the Commissioner. We have accepted [Clearview's] unchallenged evidence that all of CV's current clients carry out criminal law enforcement and/or national security functions, and use the Service in furtherance of those functions. That is the evidence placed before us by CV and while the Commissioner submits that there is an indication (in other words an inference) that any such contractors engaged by the clients are private sector bodies we are

> satisfied that any such contractors themselves carry out criminal law enforcement and/or national security functions. There is insufficient evidence on which to suggest otherwise.
>
> (Para. 146)

One may have one's doubts about this: the FTT accepts that "there is nothing that would prevent the Service being offered to commercial clients in the future" (while being "not satisfied that there is any present intention to do so"), but again, I will not here go into that any further.

Rather, let me turn to the core issue for this short paper: the ruling that the activities of Clearview and its clients are outside the scope of EU or UK law.

3. "Outside the scope of EU/UK law"

Both the EU GDPR and the UK GDPR apply in principle to:

> the processing of personal data of data subjects who are in the [EU/UK] by a controller or processor not established in the [EU/UK], where the processing activities are related to … the monitoring of their behaviour as far as their behaviour takes place within the [EU/UK].
>
> (Article 3(2)(b) in both instruments, with the EU GDPR referring to the EU, and the UK GDPR to the UK, as indicated in the square brackets)

The FTT concluded:

> a. as a matter of law Art (3)(2)(b) can apply where the monitoring of behaviour is carried out by a third party rather than the data controller; [and]
>
> b. as a matter of fact the processing of data by CV was related to the monitoring of behaviour by CV's clients.
>
> (Para. 157(a) and (b))

Therefore, in principle, the EU GDPR (prior to IP completion day) and the UK GDPR (after that date) would apply under the above-mentioned provisions. Indeed, the FTT ruled that:

> Action could be taken by the Commissioner pursuant to the Law Enforcement Directive (LED) against a UK established "competent authority" who used the Service were he to be of the opinion that such activity breached the LED.
>
> (Para. 149)

However, the FTT also held that:

> c. the processing is outside material scope of the Regulation as provided for in Article 2 GDPR and is not "relevant processing" for the purposes of Article 3 UK GDPR, as defined in Article 3(2A) thereby removing the processing from the scope of UK GDPR.
>
> Therefore, it is our conclusion that the Commissioner did not have jurisdiction to issue the [Enforcement Notice] or [Monetary Penalty Notice].
>
> (Para. 157(c) and 158)

The basis for this latter conclusion is provided, rather perfunctorily, as follows:

> Article 2(2) [EU] GDPR sets out types of processing to which the Regulation does not apply, excluding processing that would otherwise be caught by Article 3 from the application of the GDPR. In this case the relevant exemption that is relied upon is that processing was in the course of an activity which falls outside the scope of Union law.
>
> [T]he UK GDPR is constructed differently and it is Article 3(2A) that removes processing in the course of an activity which fell outside the scope of Union law before IP completion day from

> the scope of the Regulation by excluding such processing from the definition of relevant processing in Article 3 UK GDPR.
>
> Therefore, the question for us remains the same. It is foremost a question of fact as **neither party contends that the acts of foreign governments would be within the material/territorial scope of the Regulations because the activities of foreign governments fall outside the scope of Union law. It is not for one government to seek to bind or control the activities of another sovereign state.**
>
> (Paras. 151 – 153, emphases added)

It may well be that, for some reason, the ICO accepted that "acts of foreign governments are outside the scope" of both the EU and the UK GDPR, on the basis that it felt that "[i]t is not for one government to seek to bind or control the activities of another sovereign state.

But this view is nevertheless fundamentally wrong.

States are of course sovereign in their actions within their territories and (largely) in relation to their own nationals and residents, provided that in these they act in accordance with public international law, international human rights law and international humanitarian law. Other than reminding other states of these international legal obligations, and if needs be imposing sanctions for breaches of those obligations, etc., it is indeed "not for one government to seek to bind or control the activities of another sovereign state" in these regards.

However, this is not true in relation to actions of state that take place outside their territory or that have effects outside their territory – in particular if those actions have effects on the fundamental rights of individuals in other countries.

No-one in the UK has argued that the UK did not have the right to take action over the attempted murders of the persons in the UK by alleged Russian agents: the UK has every right to "bind or control" the activities of such agents of a foreign state on its soil.

The same can be said of polluting activities by one state that affect (citizens and others in) another state: such polluting acts can constitute an internationally unlawful act for which the polluting state can be responsible and liable.

The same applies in relation to the collecting of personal information on persons in one state (a targeted state) by agents (including sub-agents) of the collecting state. I have addressed this some years ago in a presentation to the German *Bundestag* committee of enquiry into the Snowden revelations as follows (with minor edits):[2]

> As its traditional name, the law of nations (*Völkerrecht*), already indicates, general public international law is the law that regulates the relations between states. It is firmly founded on the principle of respect for national sovereignty: in principle, and with only very limited exceptions, states are their own masters; no other state may interfere in matters that lie within the sovereign power of another state.

---

[2] Douwe Korff, Expert Opinion, prepared for the Committee of Inquiry of the German Bundestag into the "5EYES" global surveillance systems revealed by Edward Snowden, presented at the Committee Hearing, Berlin, 5 June 2014 (headings omitted, original emphases, words in square brackets added), available at: http://www.bundestag.de/blob/282874/8f5bae2c8f01cdabd37c746f98509253/mat_a_sv-4-3_korff-pdf-data.pdf (full text in English, in spite of what it says on the cover page):

Although sovereign, states are subject to law, in particular to treaty law and to customary international law. The latter includes peremptory norms of international law, *ius cogens*. States are bound by their treaty obligations: *pacta sunt servanda*. States can depart from ordinary customary law by treaty, but they cannot set aside *ius cogens*, such as the prohibition of aggression, and the prohibition of the use of torture.

There is probably a rule of customary law that allows states involved in an international (i.e., an inter-state) armed conflict to spy on each other.[3] States can of course also target non-state entities within their own borders, with which they are engaged in a non-international armed conflict: this does not affect the sovereignty of any other nation.

However, … the customary rule allowing spying on an enemy state cannot be invoked by a state claiming to be involved in an armed conflict with an internationally operating non-state group (such as the USA claims to be with al Qaeda), to carry out Internet and electronic communications surveillance in another country (such as Germany) that is far removed from any actual battlefield and that does not regard itself to be involved as a beligerent party in this armed conflict.

States are especially not allowed to carry out, on the territory of another state, acts that are typically the preserve of states and state agencies (*Hohheitsakte*); that would amount to an unlawful exercise of "enforcement jurisdiction". The basic, fundamental principle in that regard is that a state "*cannot take measures on the territory of another state by way of enforcement of national laws without the consent of the latter*."[4] As the International Law Commission said:[5]

---

[3] See the Legal Authorities Supporting the Activities of the National Security Agency described by the President, attached to the Communication from the US Attorney-General to Congress of 19 January 2006, referred to in the Human Rights Committee's General Comment No. 34, CCPR/C/GC/34, 12 September 2011, paras. 24 – 26: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fGC%2f34&Lang=en

[4] Ian Brownlie, *Principles of Public International Law*, 6th ed., 2006, at p. 306. The classic expression of the principle can be found in the award of the sole arbitrator in the Palmas Island case, Max Huber:

> "Sovereignty in the relations between states signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other state, the functions of a state. The development of the national organization of states during the last few centuries and, as a corollary, the development of international law, have established this principle of the exclusive competence of the state in regard to its own territory in such a way as to make it the point of departure in settling most questions that concern international relations."

Island of Palmas Case (Netherlands/United States of America), Award of 4 April 1928, UNRIAA, vol. II (1928), pp. 829-871, at p. 838, available at: http://legal.un.org/riaa/cases/vol_II/829-871.pdf.

The same principle was also unambiguously expressed in what is still the leading case in this regard, the judgment of the Permanent Court of International Justice (the forerunner of the International Court of justice) in the *Lotus* case:

> **Now the first and foremost restriction imposed by international law upon a State is that - failing the existence of a permissive rule to the contrary - it may not exercise its power in any form in the territory of another State.** In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention [i.e., a treaty].

PCIJ, *The Case of the S.S. "Lotus"*, judgment of 7 September 1927, pp. 18-19, emphasis added, available at http://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf)

[5] See the 2006 Report of the International Law Commission (58th session), *Annex E – extraterritorial jurisdiction*, para. 22, on p. 526, available at: http://legal.un.org/ilc/reports/2006/2006report.htm (emphasis added).

> With regard to the jurisdiction to enforce, a State may not enforce its criminal law, that is, *investigate* crimes or arrest suspects, in the territory of another State without that other State's consent.

Rather than states acting by themselves in these ways, the proper channel for cross-border action in such matters is to go through so-called Mutual Legal Assistance Treaties or MLATs. These can be bi- or multilateral.

A fortiori, agents of any state that operate on the territory of another state, including diplomats, are required to abide by the domestic law of the latter country. They are not allowed to indulge in forms of "intelligence gathering" that violate those laws – such as illegal interference with computer systems or illegal interception of communications [or breaches of the target state's data protection law].

To put it simply: Surveillance by one state over the Internet activities and electronic communications of citizens and officials of another state with which the first state is not at war at that time, without the express consent of the other state, and which involve illegal activities by agents of the first state perpetrated within the territory of the other state, is a violation of the sovereignty of the targeted state. This is a rule of primary international law.

The above applies to illegal interference with computer systems and illegal interception of communications by a spying state on the territory of a target state. However,we should also address the question of whether the above rule also applies if the first state carries out such surveillance over the Internet activities and electronic communications of citizens and officials of the other state, *but without this involving activities of the first state within the territory of the other state*.

This would cover the tapping into – or the full "splitting" – of the major undersea Internet cables that form the "backbone" of the Internet and that carry most of the world's (including Germany's) electronic communications, not in Germany, but on the territory of the states performing this interception. It is reported that such interception is performed on the main Europe to USA undersea cable where this lands in the UK, at Bude, in Cornwall, UK, in a facilty operated jointly by the UK and the USA.[6]

In my opinion, such interception of German (and other continental-European and other) communications data as they pass through structures outside Germany (or the other countries) probably does not constitute a violation of the sovereignty of Germany (or the other states), because the activities do not take place on German territory (or the territory of those other states), but on the territory of the state (on *in casu*, of one of the states) that perpetrate the interception.

However, such Internet and electronic communications surveillance can still constitute an **internationally wrongful act**, entailing the responsibility and liability of the state(s) perpetrating the acts, if the surveillance is unlawful in some other way – in particular, if the interception were to be in breach of any international obligations of the state carrying out

---

[6] See:
http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

the interception *vis-à-vis* the state that is (or whose officials or citizens are) affected by the act.[7]

As further explained [later in the Expert Opinion], under the heading "*International and European human rights law*", the untargeted mass surveillance perpetrated by the USA and the UK (and probably others, in particular their partners in the "5EYES" group) against essentially all "NON-USPERS[ons]" is in blatant violation of international human rights law – and of international human rights treaties to which both the spying states (the USA and the UK) and the spied-on states (such as Germany) are a party – and affects the fundamental rights of citizens of the targeted countries as well as officials of those countries, and the institutions they represent, irrespective of where the acts of interference and/or interception take place.

In my opinion, surveillance of citizens and officials of one state-party to an international human rights treaty by agents of another state-party to that treaty, from the territory of the latter state, but which violates the obligations of the latter state party under that treaty, not only violates that treaty but (since it harms the interests of the targeted state and its officials and citizens) also constitutes an internationally unlawful act against the state whose citizens and officials are affected. That is a rule of secondary international law.

In casu, in my opinion, the Internet and electronic communications surveillance reportedly perpetrated by the USA and the UK (et al.) against Germany and many other countries, from the territory of the USA and the UK (et al.), constitutes a whole series of internationally unlawful acts against Germany and those other countries.

Here, I conclude, on the same basis as above, that the "scraping" from the Internet of facial images of nationals or residents from one state (the targeted state) and the subsequent monitoring of those individuals, by or on behalf of law enforcement or national intelligence agencies of another state (the targeting state), without the consent of the targeted state and in violation of the laws – *in casu*, the data protection laws – of the targeted state, also constitutes an internationally unlawful act by the targeting state against the targeted state. The scraping and monitoring activities of the targeting state do not fall outside the scope of the law of the targeted state (or in the case of the EU, the regional entity).

The applying, by the targeted state, of its domestic law (*in casu*, its data protection law) to such extra-territorial activities of the targeting state that affect the fundamental rights of individuals in its (the targeted state's) territory and under its (the targeted state's) jurisdiction does not amount to unlawful interference in ("binding" or "controlling" of) the sovereign activities of the targeting state.

[7] See the Draft Articles on the Responsibility of States for Internationally Wrongful Acts, drawn up by the International Law Commission (ILC) in August 2001, which are largely a codification of existing customary law in this regard, and have been cited by the International Court of Justice. For the text of the Draft principles, see: http://legal.un.org/ilc/texts/instruments/english/draft%20articles/9_6_2001.pdf

4. Final comments

The UK Information Commissioner and the First-Tier Tribunal were wrong to simply accept that "the activities of foreign governments fall outside the scope of [EU/UK] law". On the contrary, if one country collects information on citizens of another country (also) from websites and social media used by those foreign citizens, without the consent of the targeted country/home of those foreign citizens (such consent typically being given in the form of Mutual Legal Assistance Treaties, MLATs, applied in accordance with the procedures set out in such treaties), that constitutes an internationally wrongful act. The laws of the targeted country, and more specifically any privacy or data protection laws of that country, apply to such extra-territorial collection of (often highly sensitive) personal data.

The ICO and the FTT could and should have seriously addressed this important issue. They might have asked for advice from the Foreign Office, or an opinion from a leading international lawyer. To simply dismiss the issue is dangerous and supports the widespread illegal spying by US and other intelligence agencies.

It is to be hoped that the case is taken further and that these issues are then properly addressed.

- o – O – o -

Douwe Korff (Prof.)
Cambridge, UK, 18 October 2023