UiO : Det juridiske fakultet

Real-Time Facial Recognition for Counterterrorism and the Right to Privacy

How could real-time facial recognition be used in public by law enforcement under the proposed exemption for counterterrorism in the general prohibition in Article 5(1)(d)(ii) of the European Commission's proposed AI Act according to Article 8 of the European Convention of Human Rights?

Candidate number: 635

Deadline: 25.11.22

Word count: 17 979

Table of Contents

1 Intro

1.1 Theme and actuality

The introduction of real-time facial recognition technology (or facial recognition (FRT)) has sparked a fierce debate in the European Union (EU) about how to regulate it, especially its use for the purpose of law enforcement.[1] The technology is controversial and one of the greatest concerns for the critics of real-time FRT, is its' implications for privacy due to its' potential for (secret) mass surveillance by law enforcement and intelligence agencies. Daniel Leufer, a campaigner for Access NOW, an NGO advocating for privacy rights,[2] stated that "*if* [real-time FRT is] *allowed to be used even for exceptional purposes it means that the infrastructure will be there and you as a citizen will never know if it's turned on.*"[3] European intelligence agencies have committed illegal mass surveillance before with their participation in the PRISM program,[4] and one could never be sure they would not do it again or if they are doing it right now.

Critics have also highlighted FRT's potential impact on other fundamental freedoms such as the right to assembly and protest.[5] Law enforcement agencies have already used FRT in different ways to monitor protestors, and charging them with disturbance of public order, or just simply intimidating them afterwards.[6] This has the potential to scare people from using their right to assembly and opinion to take part in anti-government protests.[7]

Furthermore, the accuracy of FRT poses a risk to the prohibition on discrimination. The accuracy of different FRT software operational today have been shown to be questionable at best.[8] The accuracy is further dependent on differences in age of the person, their poses or facial

[1] Goujard (2022)

[2] https://www.accessnow.org/

[3] Goujard (2022)

[4] Bigo (2013) page 39, 45, 49, 52-53 and 57.

[5] European Parliamentary Research Service (EPRS) (2021) page 8-9

[6] Guliani (2016)

[7] EPRS (2021) page 8-9

[8] Ibid page 6

expressions, and the distance, angles lighting and backgrounds of the photos being compared.[9] Skin color and sex have also been shown to further reduce the accuracy of FRT. FRT is generally most accurate when scanning adult white males, with difficulty in distinguishing women of color.[10]

The problems most FRT systems have with distinguishing people of color is concerning with regards to the prohibition on discrimination, especially when used for law enforcement purposes. Using FRT in law enforcement could lead to people of color disproportionally interacting with police, which has happened in the UK and US, and France.[11]

Despite these controversies, governments, both at the local and national level, have capitalized on the lack of regulation to test the technology. In 2019, the local government in Nice, France, installed more than 2.600 closed-circuit television (CCTV) cameras throughout the city, testing the technology on adults during the city's carnival.[12]

The use of real-time FRT by Welsh police also led to a legal challenge in 2019, which a UK court on appeal rendered the use illegal because it was not "*in accordance with the law*" cfr. Article 8 of the European Convention on Human Rights (ECHR).[13]

In 2019, these developments prompted president-elect of the European Commission, (the Commission), Ursula von der Leyen to state she would unveil legislation to regulate the use of AI, including real-time FRT, to provide a common European approach to it.[14] The Commission revealed a proposal for an AI Regulation (the AI Act (AIA)) on April 21st, 2021.[15] AIA proposed a prohibition on the "*use of 'real-time' remote biometric identification systems* [including FRT] *in publicly accessible spaces for the purpose of law enforcement.*"[16] However, the proposed prohibition did exempt a few situations where Member States could choose to authorize

[9] I.c.

[10] Ibid. page 7.

[11] Lindsey (2021) page 7

[12] Kayali (2019)

[13] R (on the application of Edward Bridges) v. the Chief Constable of South Wales Police [2020]

[14] Khan (2019)

[15] European Commission (2021)

[16] Cfr. AIA Article 5(1)(d).

such use of real-time "*remote biometric identification systems*". The details regarding the regulation would be left at their discretion.[17,18]

Instead of ending the debates, this proved a new battleground. Several influential groupings of people had clear objections to the proposed AIA. The European Data Protection Board (EDPB) and Wojciech Wiewiórowski the European Data Protection Supervisor (EDPS)[19] argued that AIA did not go far enough, and should include "*a general ban on "any use of AI for automated recognition of human features in publicly accessible spaces, such as recognition of faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals, in any context."*"[20] This was supported by 40 MEPs,[21] alongside other advocacy groups and NGO's.[22]

On the other side, national governments of some member states, pushed back in the Council of the European Union (the Council), e.g., France. The French government was worried that banning real-time FRT poses a great threat to national security. The government received support from top administrative court judges in the French judicial system, stating that "*it would be wrong to prohibit a technology that could help identify a known terrorist in a large crowd during a mass event.*"[23] The Council's latest AIA drafts even proposed wider exemptions from the prohibition on law enforcement's use of real-time FRT in public.[24]

However, despite the disagreement, some version of AIA seems likely to pass. The European Parliament (the Parliament) passed a non-binding resolution on October 6th, 2021, calling

[17] Cfr. AIA Article 5(4).

[18] EPRS (2021) page 30

[19] The EDPS' responsibility is to monitor and ensure compliance with the General Data Protection Regulation (GDPR) and other Union law by EU organs with regards to data processing cf. Regulation (EU) 2018/1725 Art 52 (3), whilst the EDPB's responsibility is to "*ensure the consistent application*" of the GDPR in general cf. GDPR Art 70 (1).

[20] EDPS and EDPB (2021) page 12

[21] Lomari (2021)

[22] Li (2021)

[23] Goujard (2022)

[24] The latest text from the Council removes the requirement of an "*imminent*" threat and added "*critical infrastructure*" as a protected target cfr. COD(2022) 13102/22 page 57

> "for a moratorium on the deployment of facial recognition systems for law enforcement purposes that have the function of identification, unless strictly used for the purpose of identification of victims of crime, until the technical standards can be considered fully fundamental rights compliant, results derived are non-biased and non-discriminatory, the legal framework provides strict safeguards against misuse and strict democratic control and oversight, and there is empirical evidence of the necessity and proportionality for the deployment of such technologies".[25]

Of 705 MEPs, 377 voted in favor, 248 against and 62 abstaining.[26] As of September 2022 there is a majority coalition in favor of a ban in the Parliament.[27] If the final version of AIA includes the exemptions, how could law enforcement in Member States use real-time FRT in publicly accessible places?

1.2 Research question

AIA Article 5(1)(d)(ii) prohibits the use of "real-time FRT by law enforcement "*in publicly accessible spaces, unless and in as far as such use is strictly necessary for… the prevention of a specific, substantial and imminent threat…. of a terrorist attack"*,

This is not a legal basis to use real-time FRT in these situations. AIA article 5(4) specifically states that if Member States want to use real-time FRT for counterterrorism, they have to authorize it in domestic legislation. The details of which is left to their discretion, although there are some requirements in Article 5 paragraph two, three and four.[28]

The proposed exemption for counterterrorism in AIA Article 5(1)(d)(ii) is vague and does not specify how real-time FRT can be used. This paper will analyze the AIA draft proposed by the Commission, and which constraints the right to privacy in ECHR Article 8 will place on the domestic legislation in Member States choosing to authorize the use of real-time FRT as defined by AIA Article 3(37) for counterterrorism. It will analyze the use of real-time FRT according to the legality and necessity criteria in ECHR to assess how it can be used, and the boundaries placed on it, specifically regarding:

[25] 2020/2016(INI) § 26

[26] Li (2021)

[27] European Parliament Press Release (2021)

[28] EPRS (2021) page 30

- If the proposed grounds for using real-time FRT, legal restraints and requirements in AIA Article 5(1)(d)(ii) (2) (3) would be "in accordance with the law" under ECHR Article 8?
- Where can real-time FRT be used?
- Who can be surveilled using real-time FRT?

For the purpose of this paper, I will define two different purposes for how real-time FRT can be used to "prevent" a terror attack, i.e., "point defense" and "preventative investigation" and assess the legality of these purposes according to the criteria of in accordance with the law and necessity.

"Point defense" will for the purpose of this paper be defined as the use of real-time FRT for secret surveillance limited to only protecting specific locations or events identified as planned or likely targets, e.g., large events, travel points, governmental headquarters, for an incoming attack. For this purpose, real-time FRT would be used to establish a defensive perimeter to stop suspected or known perpetrators before they reach the target.

"Preventative investigation" will be defined as city or country-wide secret surveillance for the purpose of investigating a terror plot in the planning phase[29] using a real-time FRT system to locate (a) suspect(s),[30] track their movement, identify contacts made by the suspect(s), and visual surveillance.

The reasoning behind my decision to divide the use of real-time FRT into these purposes is that they arguably represent the narrowest and broadest form of using real-time FRT for counterterrorism. Analyzing whether the broadest purpose is permissible, and if not, the narrowest purpose will provide an idea of how it can be used. If the broadest purpose is impermissible, but the narrowest purpose is not, the demarcation is somewhere in between. This seems like the best way to try to answer if and/or how real-time FRT can be used in the exemption for counterterrorism proposed in AIA Article 5(1)(d)(ii) according to ECHR Article 8 in general, and not in a specific case.

[29] Assuming planning happens domestically

[30] Robbins (2021) page 97

1.2.1 Delimitations

There are a few questions use of real-time FRT raises the paper will not discuss. These are *inter alia*:

1) The question of data security for a real-time FRT system.
2) The discussion amongst different EU institutions regarding different definitions of AI. in AIA, and how the final definition might impact what Article 5(1) prohibits.
3) The legality of using "*post*" FRT as a replacement for real-time FRT in the discussion in Chapter 3.2.2.[31]
4) The seriousness of the threat terrorism poses to European countries. The ECtHR does recognize the threat as serious, and consequently affords a wide margin of appreciation with regards to the measures adopted to stop it.[32]

1.3 Methodology

1.3.1 Legal basis — European Convention on Human Rights or EU Charter of Fundamental Rights and Freedoms?

Since EU law has primacy over domestic legislation, the Court of Justice of the European Union (CJEU) has jurisdiction to review if member state legislation breaches Union law.[33] Thus it would seem like the CJEU can review whether a domestic law breaches AIA. Every "version" of AIA Article 5(1)(d) includes the requirement that the domestic law in Member States choosing to authorize the use of real-time FRT in "*publicly accessible places*" by law enforcement cfr. Article 5(4) only do so when "*strictly necessary*". Article 5(3) further adds some requirements of the domestic laws to not violate AIA, e.g., a requirement for authorization only after independent judicial review, unless the decision is time critical. The CJEU seemingly has the competence to review if any domestic law breaches these requirements in AIA Article 5.

[31] Cfr. AIA Article 3(38)

[32] *Beghal v. the United Kingdom* § 92

[33] See e.g., Case *26-62* (Van Gend & Loos) and Case *6-64* (Costa v E.N.E.L.)

However, the CJEU's jurisdiction is not certain, especially with regards to the exemption for counterterrorism in Article 5(1)(d)(ii). National security and maintaining law and order usually falls outside the scope of Union law, and is the exclusive competence of the Member States.[34] The Council also proposes to leave matters of "*national security*" outside AIA's scope of application. The last updated version of the Council's "proposal" clearly states their opinion on this matter:

> "as regards national security purposes, the exclusion is justified both by the fact that national security remains the sole responsibility of Member States in accordance with Article 4(2) TEU and by the specific nature and operational needs of national security activities and specific national rules applicable to those activities".[35]

The line between law enforcement preventing terror attacks and national security and intelligence is blurry at best, so with or without this exemption, the CJEU's power of judicial review is unclear with regards to counterterrorism. In many countries, agencies tasked with national security and counterterrorism also have law enforcement powers, e.g., the Norwegian Police Security Service (PST). PST is a domestic intelligence service under the Directory of Police tasked with preventing and investigating;

> "Illegal acts under Chapter 17 of the Penal Code, [titled "Protection of Norway's autonomy and other fundamental national interests"] and the Security Act
> Illegal foreign intelligence activity on Norwegian soil,
> Illegal acts regarding the proliferation of weapons of mass destruction
> Enforcing the Export of Strategic Goods, Services, Technology Act, and
> Sabotage, political violence and illegal acts under Chapter 18 of the Penal Code, [titled "Terrorist acts and terrorism-related acts"].[36]

With regards to PST's jurisdiction of terrorism offences, "*open investigations*" are carried out by normal police.[37] However, the use of real-time FRT by law enforcement to prevent terror attacks might not be "*open investigations*" after the attack, but rather secret operations to stop it. If such use of real-time FRT for counterterrorism by an equivalent agency to the PST in an

[34] Cfr. TEU Article 4(2)

[35] COD(2022) 13102/22 page 17

[36] Cfr. Politiloven § 17b(1)

[37] I.c.

EU Member State to stop an attack would be considered to fall under the exemption provided for in AIA Article 5(1)(d)(ii) or national security, is unclear. If it were considered "*national security*", then the CJEU might not have jurisdiction in the matter.

However, the CJEU have struck down national laws in Member States allowing for mass surveillance and data retention for the purpose of national security before, and might do it with AIA as well, often with references to the ECHR. With regards to mass surveillance of location data, the CJEU has struck down domestic legislation allowing for or mandating the indiscriminate retention of real-time location data coming from telecommunications.[38]

Unlike the CJEU, the European Court of Human Rights (ECtHR) does not have any exemptions to its' jurisdiction cfr. Article 32(1), although the state's margin of appreciation vary, and is particularly wide with regards to national security.[39] However, the ECtHR can always overrule the states which are obligated to respect ECtHR judgements cfr. Article 46.

Furthermore, CJEU judgements, unlike AIA do not have direct effect for the EFTA-countries in the EEA-agreement[40,41,42] i.e., the legality of laws in EFTA-countries would be determined by the ECtHR or EFTA Court.[43]

The uncertainty about CJEU jurisdiction in matters concerning national security, in any case lack of jurisdiction over EFTA-countries, alongside the ECtHR's definitive jurisdiction are the reasons the paper will analyze the ECHR instead of the Charter.

[38] See e.g., Case C-511/18 - *La Quadrature du Net and Others* § 187

[39] *Beghal v. the United Kingdom* § 95.

[40] Norway, Liechtenstein, Iceland cfr. EEA-Agreement Article 2(b)

[41] Cfr. COD(2022) 13102/22 page 1

[42] Note that the EFTA Court and the CJEU is supposed to ensure homogenous application of all EU legislation relevant to the EEA cfr. EEA-Agreement Article 106.

[43] Cfr. EEA-Agreement Article 108(2).

1.3.2 Legal sources

The paper will analyze ECtHR case-law regarding ECHR Article 8 on the Right to Respect for Private and Family Life and ECHR Article 2 of Protocol 4 on the Right to Freedom of Movement.[44,45] The ECtHR has never heard a case regarding use of real-time FRT before. Therefore, case-law regarding cases comparable to the aforementioned purposes must be analyzed e.g., cases concerning GPS-tracking or retention of biometric data.

Domestic case-law from signatory states to the ECHR will also be used. Domestic courts dynamically interpret the Convention in the same way as the ECtHR.[46] The ECtHR might be influenced by the arguments of domestic courts, even though the ECtHR has the final word on matters regarding the ECHR.

1.3.3 Discussion format

The first section of this paper will start with a technical explanation of how real-time FRT works. Following this, the paper will discuss how AI and real-time FRT are regulated in AIA, and examine the proposed exemption in AIA Article 5(1)(d)(ii), including a discussion regarding the differentiation between "real-time" and "post" FRT proposed in AIA.

The second section will analyze the two purposes the use of real-time FRT in publicly accessible places could serve under the notion of "*preventing* [a] *terror attack"*, i.e., "point defense" and "preventative investigation" according to ECHR Article 8. The analysis under Article 8 will follow the standard format with assessing the two purposes with regards to the criteria of necessity, pursuit of legitimate aim, and accordance with the law. The order of these requirements will be legitimacy first, followed by necessity, and lastly legality. The reason why necessity comes before legality, opposite of how the ECtHR normally assesses cases, is because this paper analyses the legality of a hypothetical law(s) concerning secret surveillance, not a concrete case.

[44] ECHR Article 8 offers mostly the same protection as Article 2 of Protocol 4. If a State has not ratified Protocol 4, Article 8 can be used instead of Article 2 Protocol 4.

[45] "Guide on Article 2 of Protocol No. 4" page 18, see *Colon v. the Netherlands*.

[46] See e.g., Rt-2005-846 § 45

When assessing the legality of secret surveillance, the ECtHR has stated that the necessity- and legality-requirement are so closely related that it is beneficial to address them simultaneously. The Court assesses whether the law in question includes adequate safeguards and if it is sufficiently clear and accessible as to keep the interference secret surveillance cause to what is necessary.[47] This paper will structure the discussion a bit differently. The paper will address whether secret surveillance using real-time FRT is in principle legal presuming the law has adequate safeguards first, and then assess whether the ground of "*prevention of a terror attack*" and the safeguards AIA Article 5 requires domestic laws to incorporate are sufficient to keep the interference to a minimum for what is necessary. This seems to be the most logical structure.

2 The proposed AI Act and Real-Time Facial Recognition

AIA is supposed to "*guarantee the safety and fundamental rights of people and businesses, while strengthening AI uptake, investment and innovation across the EU*"[48] and to "*improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with Union*."[49]

To do this, AIA will introduce "*harmonized rules*"[50] for placement, sale, use and prohibition on certain use of AI systems in the single market.[51] AIA is a risk-based regulation i.e., the regulation's strictness depends on the risk a system or its use poses to fundamental rights.[52] "High-risk" AI-systems must conform with the entirety of AIA, whilst limited risk systems are exempt from most of it. Low-risk systems must only conform with existing legislation.[53]

2.1 Technical definition and explanation of real-time facial recognition

[47] See *Big Borther Watch v. the United Kingdom* § 334

[48] European Commission Press Release (2021)

[49] Recital 1 AIA

[50] Cfr. AIA Art 1(a)

[51] Cfr. AIA Art 1(a)

[52] Cfr. AIA Art 1(b)

[53] EPRS (2021) page 24

Most modern FRT systems are powered by AI.[54] AI is a computer software designed to mimic intelligence to solve tasks.[55] AI comes in two forms, applied or general. Applied AI is a system designed to solve one task efficiently, i.e., drive cars or keep users on different websites such as YouTube or Facebook. General AI are computer systems which use intelligence in a general sense to solve any task it is asked to.[56] One of the differences between normal computer software, like Microsoft Office and AI is in how it is created. With normal computer software, the programmer writes all the code needed for the software to function. The programmer has full control over, and knowledge about how it works. With AI on the other hand, the programmer creates the initial conditions and testing parameters for how the software can teach itself how to do different tasks.[57,58] How AI programs teach themselves is not important for this analysis, other than the fact that it requires a lot of data, and that more data generally equals better AI.[59]

How FRT works specifically can be broken down to six steps.[60] Firstly, one must compile a set of images in a database (watchlist) the AI can use as a reference. Secondly, after the image-collection, the software analyses the picture of each person (there may be multiple pictures of one person), to create a biometric template of the face. The software "*reads the geometry of your face*", including features such as "*distance between your eyes and the distance from forehead to chin*". "*The software identifies facial landmarks — one system identifies 68 of them — that are key to distinguishing your face. The result: your facial signature*."[61] The software creates a mathematical model — a line of code — for each face. This line of code is the "*data*" in "*biometric data*" cfr. AIA Article 3.[62,63] The biometric template is stored in the system's

[54] Crumpler (2020)

[55] Brown (2021)

[56] Marr (2016)

[57] Domanska (2021)

[58] EPRS (2021) page 20

[59] Brown (2021)

[60] College of Policing (2022)

[61] Symanovich (2021)

[62] This will only be the case if the data allows for unique identification of an individual. This means that data stemming from FRT used only to assess whether two different pictures of a face belongs to the same person without any knowledge of their identity does not qualify as biometric data cfr. AIA Article 3(33), and GDPR Article 4(14).

[63] The creation of this line of code, and the question concerning its' classification as "*biometric data*" with regards to ECHR Art 8 influences the legality of the system. This will be discussed later on.

database for future scanning.[64] The third step is that the FRT-software detects individual faces in a video-feed. Fourthly, the FRT-software repeats step 2 on the images extracted from the video feed. The fifth step is to compare this newly created biometric template to the existing database. Lastly, the software assigns the similarity a numerical value, and based on a predetermined similarity score, the software either indicates a match or not.[65] After this, a human, e.g., police officer, might perform a quality control.[66]

2.2 Real-time facial recognition and its' use in publicly available places under Article 5(1)(d)(ii) of the proposed AI Act

2.2.1 Definition of AI

To fall within the scope of AIA, a system must use AI cfr. AIA Article 2. AI is defined as any

> "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."[67]

The Commission' proposed definition have received mixed reviews. There are multiple forms of techniques used to create AI. If all of them are covered in litra a-c of Annex 1 is not completely clear, but it seems so.[68,69] The NGO AlgorithmWatch has stated that the definition probably covers every technique used today, and in the foreseeable future,[70] but some academics and lawyers expressed concerned that the definition is too focused on techniques of creating AI, and therefore too broad, and in danger of being technologically outdated in the future.[71]

[64] Symanovich (2021)

[65] College of Policing (2022)

[66] I.c.

[67] Cfr. AIA Article 3(1)

[68] AIA Annex I litra a-c

[69] AlgorithmWatch (2021)

[70] I.c.

[71] Clarke (2021)

Their solution is to focus the definition on "*properties or possible results*" of AI instead of techniques.[72]

The Council has also pushed back against the definition. In a Czech presidency compromise text, AIA's definition of AI was significantly narrowed, to exclude "*more traditional software systems*."[73] The Council has received support from tech industry that the definition is too broad.[74] TechUK, a trade association for tech companies in the UK,[75] stated in their feedback submission to AIA, that "*the definition of 'AI system' is very broad and goes beyond what would normally be considered as 'intelligent.*"[76]

2.2.2 Prohibition on using law enforcement "*real-time' remote biometric identification systems*" in public

AIA Article 5(1) prohibits law enforcement from using "*real-time' remote biometric identification systems*" in public. To assess the scope of the prohibition, one must look to the definitions provided in Article 3.

In Article 3(37) "*real-time' remote biometric identification systems*" is defined as systems where "*the capturing of biometric data, the comparison and the identification all occur without a significant delay*". This covers instantaneous processing alongside "*limited short delays*" to avoid circumvention of the prohibition in Article 5(1). "*Remote biometric identification system*" is defined as a system capable of "*identifying natural persons at a distance*" using comparisons of captured and stored "*biometric data*", "*without prior knowledge…* [that the identified] *person will be present and can be identified*" cfr. Article 3(36). Lastly, "*biometric data*" is defined as "*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person*" cfr. Article 3(33).

[72] I.c.

[73] COD(2021) 14278/21 page 3

[74] Clarke (2021)

[75] https://www.techuk.org/

[76] Holden (2021) page 1

2.2.3 Differentiation between “real-time” and “post” facial recognition.

AIA Article 5(1)(d) only prohibits law enforcement from using “*real-time*” FRT in public, not “*post*”. An example of a “*post*” FRT system is Clearview AI. It works by uploading a picture of the person being identified to the system, which scans the image, much in the same way as “real-time” FRT, and provides an identity alongside other public photos of the person scanned and links to which websites they were found. Clearview AI allegedly has a database of more than three billion images scraped from Facebook, YouTube, Venmo and millions of other websites. The database is apparently far more detailed than anything ever constructed by the US government or other Silicon Valley giants.[77,78]

“*Post*” FRT is defined in Article 3(38) as anything not operating in “*real-time*” i.e., without “*significant”* or “*limited short delays*” to circumvent Article 5(1)(d).[79] This distinction has been criticized because what “*without significant delay*” means is completely unclear, and the intrusiveness of FRT does not necessarily depend on being “*real-time*”.[80]

Whether e.g., 24 hours qualifies as a “*significant delay*” is unclear.[81] The recitals in AIA are also unclear regarding the purpose of the distinction, other than stating that the two forms of FRT carries different risks to fundamental rights. Recital 8 mentions “*pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned*” in relation to what “*post*” FRT is. The mention of footage created by private devices and CCTV in Recital 8, indicates that the FRT system’s intended use, not necessarily just the time between creation and processing of the footage, should be part of the defining difference. This points to an FRT system disconnected from camera capturing the footage, intended to be used as a tool in a specific investigation, not general surveillance, alongside the time delay between creation of footage and processing. This is a better distinction. A distinction based only on the time difference is

[77] Hill (2020)

[78] The use of ClearviewAI, a program relying on scarping publicly accessible photos, by law enforcement has been deemed illegal in some European countries, e.g., Belgium. This will be discussed more later. Source: Brussels Times (2021)

[79] Cfr. AIA Article 3(37)

[80] EDPS/EDPB page 12 § 31.

[81] I.c.

problematic. These two examples, presuming 24 hours constitutes a "*significant delay*", illustrates why.

E.g., if police are chasing a suspect on the run, for which they already have created a biometric template for facial recognition, that escape the pursuit at a train station. If police can obtain the CCTV-camera footage at the train station, send it to the police precinct, run it through their FRT program, and find out which train the suspect escaped on in two hours, should the time delay prevent police from doing this and instead force them to wait 24 hours to not qualify as "*without significant delay*"? On the other hand, if only the time difference matters, could police create a camera-network covering every street corner in a city and link it to a central FRT system with a built-in 24-hour processing delay? That seems illogical at best.

This shows that it is not necessarily the "*real-time*" component of FRT which defines the intrusiveness of the technology. How the algorithm processing data for "*post*" and "*real-time*" FRT works, can be exactly the same. The only major difference for the purpose of AIA Article 3 seems to be the time-delay between creation of the footage being scanned and the scan itself. Real-time FRT can create the footage and scan it autonomously and instantaneously.[82] According to a literal interpretation of AIA's definition, "*post*" FRT also does not require a human to tell it to start processing images. There may of course be minor differences in how the algorithm/AI of each system works, but those differences are not an inherent difference between "*real-time*" and "*post*" FRT.

However, an FRT mass surveillance system on a e.g., 24-hour processing delay is to a degree less intrusive than one with instantaneous processing. With a time-delay on processing, law enforcement cannot physically intervene with someone/something using the FRT system, only watch it happen and intervene afterwards. In the most extreme circumstances, i.e., a totalitarian surveillance and police state, citizens would have a 24-hour head start on police tracking them. Furthermore, without real-time capability FRT cannot be used for "point defense".

[82] Recital 8 AIA.

3 Real-time facial recognition for counterterrorism under Article 8 of the European Convention on Human Rights

3.1 General overview of Article 8

ECHR Article 8 guarantees everyone "*the right to respect for his private and family life…*". The ECtHR has never defined what the right to privacy entails. It is a broad term not definable by an exhaustive list.[83] Like most fundamental freedoms in the ECHR, the right to private and family life is a dynamic concept, i.e., its' application changes with time and the evolution of society.[84] Data protection can serve as an example. When the Convention was conceived in the 1950's, data protection was not as central as it is today since modern computers did not exist.[85]

Instead of defining privacy, the Court assesses the criteria for interference on a case-by-case basis to determine if Article 8 has been breached.[86] Thus, one cannot as easily extrapolate a coherent legal principle from ECtHR caselaw as with some national jurisdictions and apply it to laws or actions which has not been already tried by the Court. Instead, one must look at similar cases as the one being assess and argue that they should be treated equally. The right to privacy is not absolute and the state can limit or interfere with it if the interference is "in accordance with the law", in pursuit of a legitimate aim and "necessary in a democratic society" cfr. Article 8(2).

3.2 Real-time facial recognition under the criteria for legal interference

3.2.1 Legitimate interest

The legitimate interests listed in ECHR Article 8(2) are *inter alia* "national security, public safety… [and] the prevention of disorder or crime".[87]

[83] *Gillan and Quinton v. the United Kingdom* § 61

[84] "*The European Convention on Human Rights — A Living Instrument*" page 7.

[85] "*Guide to the Case-Law - Data protection*" page 7

[86] Pool (2017) page 132

[87] The list in ECHR Article 8(2) is exhaustive

The Court normally does not spend much time assessing whether something is in pursuit of a legitimate interest.[88] This may especially be the case when assessing a law, rather than a specific action taken authorized by law. The difference could be illustrated by chapter 16 a in the Norwegian Criminal Procedure Act. Chapter 16a authorizes communications monitoring in serious criminal investigations. This is obviously in pursuit of the "*prevention of disorder and crime*". However, a legitimate interest must be demonstrated every time police monitors someone's communication, not just for the law itself. Police cannot use this authorization to monitor people's communications who clearly had nothing to do with a crime. Generally, counterterrorism is a legitimate interest, however, it is possible to think of exemptions, e.g., if a country would use the notion of terrorism to justify authoritarian measures outside the scope of legality of the ECHR. This will be touched on further in Chapter 3.2.3

3.2.2 Necessary in a democratic society

The ECtHR has clarified that the term "*necessary in a democratic society*" it does not means *""indispensable""*, nor does it have "*the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable*"."[89] The Court further noted that "*the interference must, inter alia, correspond to a "pressing social need"*."[90] However, the further meaning of the criterion and how it should be assessed is unclear, since the ECtHR has not provided a specific structure for it.[91,92] Because of this unclarity, a three-pronged approach has been proposed and adopted by scholars,[93,94] consisting of assessing the interfering measure's suitability (effectiveness), proportionality sensu strictu, and if less intrusive means can achieve the same result (subsidiarity). In this paper, the proportionality and subsidiarity will be assessed together.

[88] "*Guide to Article 8*" page 12.

[89] *Silver and Others v. the United Kingdom* § 97

[90] I.c.

[91] Gerards (2013) page 468-469

[92] Pool (2017) page 133

[93] Gerards (2013) page 468-469

[94] Pool (2017) page 133

3.2.2.1 General remarks regarding the necessity of secret surveillance and surveillance using new technologies specifically

In the case *S. and Marper v. the United Kingdom*, the ECtHR held that the development and employment of cutting-edge technologies for interfering with fundamental rights, makes the necessity requirement stricter. The case concerned the retention of DNA samples and fingerprints taken from two persons suspected and investigated for crimes for which they were not convicted. Since the DNA samples and fingerprints were taken in connection with an investigation for which they were suspected of having committed the crime, the law did not require the police to destroy the samples. The law allowed for indefinite retention to aid in future criminal investigations by building a national registry of biometric samples. The Court held that because of the rapid advances in genetic science, the possibilities for what data could be possible to extract from DNA and cellular samples in the future and how that could impact the privacy of the persons' whose samples were retained was violated. Regarding how this impacts the necessity-requirement, the Court stated that *"any State claiming a pioneer role in the development of new technologies bears* [a] *special responsibility for striking the right balance in this regard*."[95]

This "*special responsibility*" is relevant for the development and employment of real-time FRT as well. Real-time FRT is a brand-new technology, not fully developed. Just like with DNA and cellular samples, what data can be retrieved from the biometric templates, and how it can impact the privacy of the person to whom it belongs in the future is unknown. Some companies developing FRT, are also developing FRT linked with emotion recognition.[96] This means FRTs at one point in the future may be able to identify a person and "read" their emotions at the same time.[97] If this is actually possible is unknown,[98] but whether the actuality of the emotion scan is irrelevant as long as the entity performing the scan acts as if it is. Emotion detection is an extreme interference with the right to privacy, and given the possibility that the FRTs and their biometric templates of today could conceivably be used for emotion detection in a couple of

[95] *S. and Marper v. the United Kingdom* § 112

[96] EPRS (2021) page 4

[97] Ibid. page 1

[98] Stanley (2019)

years indicates that the same strict necessity requirement should be applied to real-time FRT as well.

The ECtHR has further held that secret surveillance is only allowed when "strictly necessary",[99] because such surveillance is a "*hallmark of police states*."[100] The Court specified that the notion of "strictly necessary" when it comes to secret surveillance, means the surveillance must generally be strictly necessary to protect a state's democratic institutions or for gathering "*vital intelligence*" in a given operation.[101,102] Thus, surveillance, especially secret surveillance, using real-time FRT to stop terror attacks must be "strictly necessary" mirroring the requirement in AIA Article 5(1)(d)(ii).

3.2.2.2 Effectiveness

The effectiveness of using real-time FRT for "point defense" or "preventative investigation" to "[prevent] *a specific, substantial and imminent threat of a terrorist attack*" cfr. AIA Article 5(1)(d)(ii) depends *inter alia* on the accuracy of the system used, its' processing capability and how easy it is to circumvent it. This is a two-pronged analysis, firstly, how effective would real-time FRT be for each of the purposes, and then how effective would the purposes be at preventing a terror attack?

3.2.2.2.1 General issues with the effectiveness of real-time facial recognition

Firstly, no modern FRT systems are 100% accurate. The accuracy is further influenced by differences in age of the person, their poses and facial expressions, and the distance, angles, lighting and backgrounds of the pictures, and the sex and skin color of the person.[103] Law enforcement and intelligence agencies would have to obtain a good image, (preferably multiple as it improves the accuracy of the system),[104] and keep them up to date as to avoid too many differences in the aforementioned factors. When it comes to foreign terrorists, this might be

[99] *Klass and Others v. Germany* § 42

[100] "*Guide to Article 8*" page 143

[101] *Szabó and Vissy v. Hungary*, §§ 72-73

[102] "*Guide to Article* 8" page 143

[103] EPRS (2021) page 6

[104] Lindsey (2021) page 7

incredibly hard. How much knowledge about foreign terror groups and its' members various western intelligence agencies have, is not public information, so how big of a problem this is, is impossible to say. Although, Interpol maintains a database with biometrics for terrorists[105] and their databases contains "*details*" concerning at least 135.000 foreign terrorist fighters. [106] If that means biometrics for the 135.00 terrorists is unclear, and how many they do not have "*details*" or biometrics for is unknown.

How accurate real-time FRT is on persons with known identities in general is hard to say. However, a report assessing the UK Metropolitan Police's trial of real-time FRT on six occasions can serve as an example. According to the report, the system flagged forty-two matches suitable for analysis. Of these forty-two matches, sixteen matches were discarded as wrong by a police officer right away, and twenty-six were deemed plausible enough to warrant a manual identity check. After the manual identity check, eight were correct, fourteen incorrect and the last four got lost.[107] The tests were done at specific events, analogous to "point defense", and cameras were placed either on a van or at fixed positions similar to normal CCTV-cameras. The entire location was always in view.[108] The report labeled this as an error rate of 81%[109] whilst the Metropolitan Police claimed the error rate was 1 in 1000, since they counted every wrong match per every face scanned.[110] However, seemingly none of these statistics account for potential false negatives, i.e., people on the watchlist not flagged.[111] Thus, the true accuracy of the system is hard to assess. This statistic will be used as a baseline for further analysis.

Secondly, FRT only works when there are pre-made biometric template to scan faces against. There is a rising trend in Europe of right-wing terrorism,[112] and lone-wolf attacks.[113] Identifying and tracking homegrown, lone-wolf terrorists radicalized over the internet is incredibly hard.[114]

[105] Interpol, "identifying terrorist suspects" (retrieved 12.11.2022)

[106] Interpol, "preventing terrorist travel" (retrieved 12.11.2022)

[107] University of Essex (2019) page 10

[108] Ibid. page 19

[109] Feldstein (2019)

[110] Manthorpe (2019)

[111] Feldstein (2019) and Manthorpe (2019)

[112] Institute for Economics & Peace (2019) page 82

[113] Lloyd (2021) page 4

[114] Bates (2016) page 9

Especially when it comes to lone-wolf right wing extremists. They are more likely to be identified by chance, and do not exhibit as big of a change in their personality as jihadists.[115] Real-time FRT would not be effective to combat this threat, but that is not detrimental.

Thirdly, there is the issue of the system's processing rate per second in relation to the number of targets for processing at any given time. How fast different FRT systems can process faces is hard to say, but the system used by the SWP could at least process fifty faces per second.[116] Many cities in the EU have average population densities above 2000 per square kilometer,[117] and in 2018 there were at least 14 cities in the EU with square kilometers areas surpassing 20.000 people.[118] With the real-time FRT employed by the SWP, one would need 40 cameras per square kilometer on average for cities with 2000 inhabitants per square kilometer, and 400 cameras for the most populated square kilometers to process everyone per second.[119] This could be doable, and one would not need to scan everyone each second, so the number required to cover everyone within a square kilometer is probably a lot lower.

Lastly, the issue of face covering. FRT requires a face to scan, so any form of total face covering when walking in public, or using of transportation obstructing the face might render the system ineffective.

3.2.2.2.2 "Preventative investigation"

"Preventative investigation" is the use of a city-wide real-time FRT network for secret surveillance to locate a suspect's, track their movement, identify contacts, and visually surveil the suspect in the planning phases before the attack.[120]

[115] Institute for Economics & Peace (2019) page 83

[116] R (on the application of Edward Bridges) v. the Chief Constable of South Wales Police [2020] § 11.

[117] Eurostat (2021)

[118] Rae (2018)

[119] Simplified assumption not accounting for tourists and commuters, which would increase the required amount of cameras

[120] See Chapter 1.2

The issue of real-time FRT's accuracy is not necessarily a problem. "Preventative investigation" is meant to investigate and prevent the attack in a timely manner before the attack. When the FRT-network is city-wide, with potentially cameras everywhere, it may not matter if the system gives a false positive or negative when a person enters line-of-sight of one camera (or sector of cameras, it would be multiple cameras per x square meters) if the system processes a person each time they enter line-of-sight, and not just one time. If enough cameras give one identity for a person, it could be presumed that the identity is correct, especially with the presumed accuracy of the real-time FRT system of the Metropolitan Police. FRT systems, especially "post", are usually programmed with lower accuracy thresholds when used for investigative purposes.[121] So even with the accuracy rate of the Metropolitan Police's FRT, it could probably reliably enough locate a suspect, track their movement, and identify contacts, especially if given multiple chances on the same person.

The same goes for the issue of processing power. Surveilling everyone in a city with millions of people at the same time with one central system might be impossible. Bringing down the required processing power, could potentially be solved by setting up local networks for e.g., each square kilometer, and these local networks could each communicate only the positive matches into one central computer. If this is feasible technically and/or financially is beyond the scope of this paper. For further analysis, it will be presumed to be possible.

Lastly, face covering might be an issue. The state's capability of using real-time FRT would have to be public knowledge cfr. the foreseeability-requirement.[122] Terrorists plotting an attack would most likely take active precautions to avoid being surveilled they know is a possibility.[123] However, face covering in public could be banned.[124,125] How to practically enforce it is another discussion, but using face covering when it is banned would attract attention. However, since real-time FRT can recognize faces using surgical facemasks, it could probably recognize that a face is fully covered as well. This could lead to police being dispatched to check it out.

[121] Crumpler (2020)

[122] See Chapter 3.2.3 for further analysis.

[123] Robbins (2021) page 96

[124] See *Dakir v. Belgium*

[125] This will be further discussed in point 3.2.2.4.2

In short, a real-time FRT network would be effective for "preventative investigation". Furthermore, to have a city-wide surveillance network able to locate a suspect, track their movement, identify contacts, and visually surveil the suspect in the planning phases before an attack would be an effective tool for counterterrorism. Police already use many different techniques to try and accomplish these goals today, e.g., monitoring locations of cellphones, interactions between cellphones to identify the other owner etc.

3.2.2.2.3 "Point defense"

"Point defense" is the use of real-time FRT as a tool for secretly identifying anyone entering a location identified as either the definite or likely target of the incoming attack, to either arrest or search and surveil them at the location.[126]

For this purpose, the aforementioned limitations of real-time FRT are less of an issue than for "preventative investigation". With regards to accuracy, the biggest problem for effectiveness is false negatives. An error rate of 81% might sound high, but the absolute number is the important factor.[127] If the error rate was 81% of thousands of matches, it would be ineffective, since it would be impossible to manually verify the results. However, only fourteen people were verified as incorrect matches after the identity check.[128] Use of real-time FRT would of course also be coupled with (undercover) police presence who could do an identity check, and either arrest or let the person go. Real-time FRT would be a tool to complement existing security, not replace it, and would not draw many resources away from this.

Processing power is probably not as big of a concern either. There are limits to have many people who can physically enter a limited area any given second, and the system also only has to identify them once, not all the time. Lastly, the aforementioned ban on face covering would be easy to enforce. Either uniformed or undercover police could intercept everyone with covered faces entry.

[126] See Chapter 1.2

[127] Presuming the error rate of the Metropolitan Police's real-time FRT.

[128] University of Essex (2019) page 10

To summarize, real-time FRT would be an effective tool for "point defense". A secret "point defense" system would also probably be an effective way to protect an identified or likely target from a known threat, if working perfectly. If police can identify everyone entering er getting close to a target, then they can stop the attack. The effectiveness also depends on underlying intelligence. If the target is known in advance, it could be very effective to stop the attack, but if law enforcement or intelligence agencies only know there might be an attack, without any more details, the effectiveness depends on how educated their guesses are as to what the targets could be. Furthermore, if the presence of the system is detected or suspected by the attacker(s) it could just force them to pick another unprotected target.

3.2.2.2.4 Summary

To summarize, there is evidence that real-time FRT, both used for "preventative investigation" and "point defense" would be beneficial in preventing terror attacks. Exactly how beneficial is hard to say without statistics concerning how many attacks have been stopped using real-time FRT and how many it failed to stop.

3.2.2.3 Proportionality

3.2.2.3.1 Who can be placed on a watchlist and surveilled using real-time facial recognition

Firstly, it is beneficial to assess who can be put on the watchlist of biometric templates necessary for a real-time FRT network to function. Case-law from the ECtHR regarding this question is very limited. The Court has previously excluded facial images from the category biometric data which is considered "sensitive data".[129] This, however, may be starting to change. The Court has stated it is aware of the rapid technological advances when it comes to facial recognition and the retention of facial images.[130] The Court further stated that the margin of appreciation for states when it comes to retention facial images and fingerprints is wider than with DNA and cellular samples, but only slightly.[131] The Court did stop short of classifying facial images as biometric data, but it did group it together with fingerprints which is considered biometric data. Whether a biometric template for facial recognition is considered "biometric data",

[129] ECtHR definition, not EU cfr. "*Guide to the Case-Law — Data protection*" page 1 and 19.

[130] *Gaughran v. the United Kingdom* § 80.

[131] Ibid. § 96

is therefore unclear. Because of this, the current case-law regarding the retention of facial images and fingerprints is the best indicator as to how the ECtHR would view creation of biometric templates for real-time FRT, i.e., how it can be done to and how long the template can be retained.

When it comes to people already convicted of terrorism-related offences, the retention of facial images and or other biometric data can probably be retained indefinitely, so long as the decision is individualized considering the likelihood of recidivism and if the retention is necessary, every 10 years.[132] It is more unclear with regards to people not convicted of any crimes. This probably also applies to known foreign terrorists even if they are not convicted in domestic courts. The most unclear issue is suspected, but not convicted homegrown terrorists and people not suspected of being terrorists, but with known connections. In case *S. and Marper v. the United Kingdom* the intended indefinite retention of fingerprints, DNA, and cellular samples of two people who were suspected but not convicted of any crimes was considered a violation of the right to privacy. However, in this case, one of the persons were acquitted of the crime in a trial and for the other the investigation was dropped. In that case, the presumption of innocence also played a huge role in determining whether Article 8 was violated.[133]

In the case of people not suspected of terrorism, but with connections, the case of *Catt v. the United Kingdom* may give some guidance. The case concerned an Applicant who had participated in demonstrations organized by the group Smash EDO. The group tried to close-down the operations of a factory in Brighton of a US based defense company with protests. Severe disorder and crime were frequent at these protests. The Applicant had been arrested, but not convicted, twice at such protests.[134] UK police had retained different files on the Applicant in a database called "Extremism database", which included information about political demonstrations he had participated in and a photograph of him. Under common law, the police could retain data for the prevention and detection of crime. With that competence, UK police retained data relating to "domestic extremism" which created the "Extremism database". "Domestic extremism" was defined as "*... the activity of individuals or groups who carry out criminal acts*

[132] *Peruzzo and Martens v. Germany* § 44

[133] *S. and Marper v. the United Kingdom* § 122

[134] *Catt v. the United Kingdom* § 7-8

of direct action to further their protest campaigns, outside the democratic process."[135] There was no maximum time limit for the retention of the data. Information about political leanings, i.e., "sensitive data" were also contained in the records which had a "chilling effect" according to the ECtHR.[136] Although retention of such data for preventative policing purposes was not by definition illegal, the Court found the Applicant had his right to privacy violated.

This is somewhat similar to affiliation with terrorism. The groups the Applicant was affiliated with were not prohibited, with the Court stating that the retention concerned "*the applicant's association with peaceful, political events: such events are a vital part of the democratic process.*"[137] However, terror groups are generally prohibited, and they are also not peaceful nor a vital part of democracy. Interpreting the Court's reasoning for saying the data retention antithetically indicates that such retention for terrorism affiliation could be legal.

When it comes to suspected terrorists in the case of an investigation it is not outside the legitimate scope of an investigation of terrorist crime for law enforcement to record and retain basic personal details concerning the arrested person or other people present at the time and place of arrest.[138]

3.2.2.3.2 Proportionality of preventative investigation

As mentioned above, "preventative investigation" requires cameras all across a city.[139] These cameras, regardless of who is eligible to be put on the watchlist for the system, processes the personal data of everyone scanned,[140,141] comparable to indiscriminate retention of location and/or communications data.

Locating and tracking the movements of a person of interest could be achieved with a GPS connected device. The device could either be the person's own electronic device (e.g., phone,

[135] Ibid. § 35

[136] I.c.

[137] Ibid. § 123

[138] *Murray v. the United Kingdom* § 93

[139] Robbins (2021) page 97

[140] I.c.

[141] See point 3.2.2.4.1

watch or tablet), or it could be a planted GPS-transmitter.[142] Both have their own problems. The former necessitates that the target is carrying the transmitting device when they move. If the target being tracked is suspicious, they might leave electronic devices when they move. The latter requires that the target brings the object the transmitter is attached to, e.g., if it is attached to a car, the target must use the car, which they do not necessarily do.[143]

Secondly, when it comes to planted devices, law enforcement must be able physically plant the device on the intended target. This requires them to know their location, and increases the risk of discovery. Using the suspect's own device requires that the device be identified and assigned to the owner. This might not be easy, as criminals have been known to buy burner phones or even create their own phone companies with custom made operating systems.[144]

Since GPS-transmitters only provide location data and not the identity of the moving subject without adding some other form of surveillance, e.g., visual, GPS-tracking alone could leave law enforcement agencies open to being tricked in a way real-time FRT does not. If the intended target discovers the planted or hacked device, the transmitter could be sent with someone else, leading law enforcement astray.

When compared to locating and tracking a suspect using GPS, real-time FRT is more intrusive. The ECtHR stated in *Uzun v. Germany* that data regarding geo-location obtained via a GPS-tracker is inherently less sensitive than (audio)visual data and states enjoy a greater margin of appreciation regarding when to employ it. [145] Real-time FRT used for the purpose of "preventative investigation" processes both (audio)visual and location data.[146] In that case, the German state prosecutor had ordered installation of a GPS-transmitter in the car of a suspected member of an offshoot cell of the Red Army Faction and perpetrator of several bombings and assassinations. This was however after other methods of surveillance already had proven ineffective and only on the condition that other less intrusive means had failed. It was also only tracking the location of two people, the owner and user of the car. In this context the GPS-tracking was

[142] See *C-511/18 - La Quadrature du Net and Others* and *Uzun v. Germany* respectively

[143] See *Uzun v. Germany*

[144] Cox (2019)

[145] *Uzun v. Germany* § 52.

[146] The processing of audio depends on the existence of a microphone in the camera and the ambient background noise being quiet enough to pick up conversations.

not considered a breach of the Applicant's right to privacy as it was seen as proportional to the need to arrest terrorists. However, in this case, the data collection was done every other day, not in real-time.[147]

Location data also does not only reveal a person's location, but it can infer information concerning other areas covered by the right to privacy, e.g., sexual preferences, life, and orientation,[148] gender identification,[149] religious views, personal relationships, and health data. This can be accomplished by looking at places a person visits. If a person frequents a place of worship, it the person faith can reasonably be inferred. Such information is considered a key element of the right to privacy.[150] Since real-time FRT relies on visual surveillance as well, it could reveal more detailed information about the aforementioned area of protection than just location data can. With regards to health data, visual surveillance can reveal information about e.g., diseases which leaves physical scars/markers on a person's face. Sexual preferences could be revealed by videotaping the gender of two people kissing as another example. This could have a deeply chilling effect.[151]

With regards to the examples of kissing in public or physical scars/marks on the body, one could argue that by stepping outside the privacy of one's own home, the right to privacy is forfeited in that instant. However, the ECtHR has taken another approach than this. It has in numerous cases stated that the right to privacy extends outside one's own home, and into the public sphere, e.g., in *López Ribalda and Others v. Spain*.[152] Even though this case concerned video surveillance inside a grocery store by a private company, it does have some interesting implications for the use of real-time FRT in public places. Firstly, it held that video surveillance in publicly accessible places do constitute an interference with the right to privacy. This means that CCTV cameras placed in view of a street or another logistical hub, does constitute an interference with the right to privacy, even though a person caught on tape might in layman's terms have been considered to have left their sphere of privacy by entering the public. If the

[147] § 12

[148] *Peck v. The United Kingdom* § 57

[149] I.c.

[150] "*Guide to Case-Law — Data Protection*" page 14

[151] Robbins (2021) page 97-98

[152] *López Ribalda and Others v. Spain* § 93

government could create biometric templates for everyone in a country, and place cameras all across cities, people would have no privacy outside their own homes.

The existence of the state's capability to use, and under which circumstances, such a system could be used would have to be public knowledge.[153] Under ECHR Article 8, such a law can itself be considered an interference. In the case *Klass and Others v. Germany* the ECtHR reasoned that legislation allowing wiretapping by law enforcement is considered an "*interference by a public authority*", because every citizen had to live with the knowledge that they potentially could be subject to such surveillance and that knowledge itself places a restriction on the freedom of communication. The case concerned a law authorizing secret surveillance of communications. The law did not require that the executive always notify the person whose communications were monitored after the surveillance seized, nor did it grant a way of challenging the approved surveillance request before a court. The applicants could therefore not prove that they had been subject to any secret surveillance measures authorized by the law in question, which the government also denied subjecting them to. Since the German security services could place any citizen under secret surveillance without mandatory notification post surveillance, nor any possibility to challenge the legality in a court pre-surveillance, they had to live with the knowledge of potentially being subjected to such surveillance and that knowledge itself had a "chilling effect" on the freedom of communication. Due to these facts, the ECtHR reasoned that the existence of such a law did constitute an "*interference*" in of itself, even if the measures it authorized were never implemented.[154]

The aforementioned issue of face-covering probably necessitates secret surveillance when used for "preventative investigation". If the public knows where cameras could be located and they are required to be marked, terrorists planning an attack could use the issue of face-covering to negate the effectiveness of the system. This means that it would be better to use normal CCTV-cameras and link them to a real-time FRT system. However, this would increase the chilling effect of the law authorizing the use of real-time FRT since the public would never know whether a CCTV-camera is a normal one or one linked with FRT.[155] The actuality of whether

[153] Further discussion in chapter 3.2.3

[154] *Klass and Others v. Germany* § 41

[155] Robbins (2021) page 96

a CCTV-camera is linked with real-time FRT or not, is irrelevant for the chilling effect. What matters is what the citizens believe or fear.[156]

This would create a chilling effect resulting from the knowledge of such a surveillance system, and the uncertainty of when it is turned on and who it tracks.[157,158] With the infrastructure allowing for such surveillance in place, the populous could never know when the government and law enforcement might be able to deduce all the above-mentioned information about them as they go about their day. Even with laws prohibiting the indiscriminate creation of biometric templates for people, people would not know if that prohibition were respected.

Furthermore, there are already CCTV cameras all across most major European cities. Six European cities are among the top 150 most surveilled cities in the world.[159] E.g., Berlin had 25.1 cameras per square kilometer and 6.24 per 1000 inhabitant in July 2022, [160] and a population density of 4322.9 per square kilometer in 2021.[161] Couple this with the AFR program used by the South Wales Police which could scan 50 faces per second,[162] 312 faces could be scanned per second per 1000 inhabitants, and 1255 faces per square kilometer, which equates to nearly a third of the population density, i.e., every four seconds the entire population could be scanned.[163]

Assuming GPS-tracking works perfectly, GPS-tracking could be coupled with using "post" FRT on the CCTV-cameras located along the itinerary taken by the tracker perhaps could accomplish mostly the same as a real-time FRT-network could in a city as surveilled as Berlin.[164] This use of "post" FRT would be the least intrusive way of using FRT for "preventative

[156] I.c.

[157] See *Klass and Others v. Germany* § 41

[158] Robbins (2021) page 96

[159] Bischoff (2022)

[160] I.c.

[161] Eurostat (2021)

[162] R (on the application of Edward Bridges) v. the Chief Constable of South Wales Police [2020] § 11.

[163] This is under a simplified assumption that the density of cameras follows the density of the population which obviously is different throughout the city.

[164] This would not be the case in every European city as Berlin is the second most surveilled city in Europe after London. How up to date with population changes these statistics are, is hard to say. Statista's stats show slightly different numbers for cameras per 1000 inhabitants in 2019. Source: Buchholz (2019)

investigation". A literal interpretation of "real-time" FRT in the prohibition in AIA Article 5(1) cfr. Article 3(37) would allow for using a "post" FRT network for nation-wide mass surveillance with cameras covering every street-corner. The only capability one would lose with this solution, is the capacity to surveil in real-time. How effective these methods for using "post" FRT would be depends on what constitutes a "*significant delay*" cfr. AIA Article 3(37) which is unclear.[165]

Real-time FRT surveillance would probably increase surveillance capability of law enforcement somewhat and be more effective that "post" FRT surveillance, especially if a "*significant delay*" cfr. AIA Article 3(37) must be interpreted to be 24 hours or perhaps even longer. However, it is unclear if the increase in surveillance capability offered by an extensive city-wide real-time FRT network is proportional to the interference it causes, especially when considering the strict necessity requirement for the use of new technology cfr. *S. and Marper v. the United Kingdom*.

Lastly, the placement and use of CCTV-cameras equipped with real-time FRT across a city could be rendered ineffective by using face covering. This could be prohibited to use in public,[166] but this interferes with the freedom of religion guaranteed by ECHR Article 9.[167] This means that to solve the biggest problem concerning real-time FRT for "preventative investigation", the state would also have to intrusively interfere with the freedom of religion.

However, the ECtHR has seemingly accepted mass surveillance somewhat comparable to real-time FRT for "preventative investigation" in *Big Brother Watch and Others v. the United Kingdom*. UK Intelligence could intercept all "*external communications data",*[168] but what data could be examined was subject to restrictions. The Court found that such bulk interception programs were not per se illegal.[169] However, as noted above, although all data flowing through the targeted bearers was intercepted, there were processes in place to discard a lot of data not deemed useful, although the process for reviewing the application of these selectors, particularly the ones who could identify an individual were not adequate.

[165] See Chapter 2.2.3

[166] See *Dakir v. Belgium.*

[167] Only with regards to religious face covering

[168] *Big Brother Watch and Others v. the United Kingdom* § 74

[169] Ibid. § 347

This could be compared to the mass surveillance using a city-wide real-time FRT network would entail. If it is possible to set up a city-wide real-time FRT network in the same way as the interception mechanisms in *Big Brother Watch and Others v. the United Kingdom*, such a system could perhaps be legal. How this potentially could be done is by sending the data, i.e., video feeds, directly from the cameras to a central processing network. Then the pre-made biometric templates could be applied to the video-feed and giving the operator either a location or a track to the next camera, before deleting the video-feed (comparable to the use of "strong selectors in *Big Brother Wacth and Others v. the United Kingdom)*. The technical feasibility of doing this is beyond the scope of this paper, the point is to show that one could think of a way could be used in a somewhat comparable way to a system the ECtHR has stated is legal in principle. This would, however, lose the added value of visual surveillance of the targeted person.

Mass surveillance using real-time FRT is different than the bulk interception of communications in *Big Brother Watch and Others v. the United Kingdom*, and it is hard to say which is more intrusive. Real-time FRT also processes biometric and visual data alongside location data (which is the most striking similarity between the two), whilst the bulk interception in *Big Brother Watch and Others v. the United Kingdom* also included the content of communications. In the case *Uzun v. Germany*, the Court stated that audio and/or visual surveillance is more intrusive than location data because "*they disclose more information on a person's conduct, opinions or feelings*."[170] The communications monitoring in *Big Brother Watch v. the United Kingdom* could also reveal a great deal about this.

The information gathered by bulk interception of communications might be more useful in a counterterrorism sense than what can be obtained with real-time FRT. E.g., with regards to the lone wolf problem of terrorism mentioned above, real-time FRT might not necessarily provide any useful intel in identifying them as a threat, locating, and arresting them. Communications and data traffic monitoring on the other hand might accomplish this by tracking their internet traffic if they are posting things on websites such as 8Chan,[171] even though this is highly debatable.

[170] *Uzun v. Germany* § 52

[171] Anti-Defamation League (2019)

A review of 225 terrorist investigations ending with charges in the US concluded that NSA's bulk interception of phone metadata[172] "*had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group*" and bulk interception of actual contents of communications "*played a role*" in only 4.4 percent of the cases examined.[173] How significant that role was is hard to say, but the report did state that traditional investigative and intelligence tools were far more effective.[174]

The CJEU has dealt with a question similar to using real-time FRT for "preventative investigation". In case *C-511/18 - La Quadrature du Net and Others*, the CJEU stated that the retention of real-time location data could be done "*only in respect of persons with respect to whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities*".[175] Retention of data originating from people outside this category could only be done when "*objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating terrorism*" exists, and the data retained cannot be in real time.[176] However, if a Member State faced a foreseeable, legitimate and serious national security threat, general and indiscriminate retention of location and traffic data could be retained.[177] Using real-time FRT for "preventative investigation" would process biometric, (audio)visual and location data from everyone within line-of-sight, regardless of who is one the watchlist.

This is a CJEU case so the importance of it with regards to the ECHR is limited, however the ECtHR did assess multiple CJEU cases labeled "*relevant case-law*" [178] in *Brother Watch and Others v. the United Kingdom*. The ECtHR did not state which weight, if any, it attached to CJEU case-law other than stating it is relevant. However, ultimately, the ECtHR did conclude

[172] Metadata is data regarding the length and time of phone calls, and the numbers the phone communication originated from. Source: Cahall (2014)

[173] Cahall (2014)

[174] I.c.

[175] *C-511/18 - La Quadrature du Net and Others* § 188.

[176] I.c.

[177] *Big Brother Watch and Others v. the United Kingdom* § 240

[178] Ibid. § 209

that bulk interception of location and communications data is in principle legal under ECHR Article 8, which would seem to be in line with what the CJEU concluded in *C-511/18 - La Quadrature du Net and Others*. CJEU case-law would likely never be decisive for the ECtHR, however, it could be a supporting argument for a conclusion the ECtHR already has decided upon.

To summarize, it is very hard to say if using real-time FRT for "preventative investigation" could in principle be legal under ECHR Article 8. It would be deeply intrusive both to the people on the watchlist and to the rest of the public. Furthermore, there are other less intrusive options, such as using GPS-tracking or even "post" FRT cfr. AIA Article 3(38), although they might not be as effective as real-time FRT.

However, the somewhat comparable bulk interception regime of the content of communications and its' metadata, was deemed in principle legal in *Big Brother Watch and Others v. the United Kingdom,* and it was the scheme's lack of important safeguards in some areas which violated Article 8 because it was not in accordance with the law. If a real-time FRT used for "preventative investigation" implements the safeguards lacking in *Big Brother Watch and Others v. the United Kingdom*, it could very well be legal under Article 8 especially considering the wide margin of appreciation in matters concerning "national security".[179]

3.2.2.3.3 Point defense

The question then becomes if it real-time FRT can be used for "point defense", and if so, where. The case *Colon v. the Netherlands* shows that designating zones where the police can stop and search, and require ID from anyone inside the zone is legal. In that case, the mayor of Amsterdam had designated most of the city center as a special security zone for six months where a public prosecutor could order that anyone within the zone could be stopped and searched for weapons, and be required to provide an ID. This order could last for a period of twelve hours,

[179] Cfr. *Beghal v. the United Kingdom* § 95

and the time of day could be randomly selected, but the order could not be renewed.[180] A similar renewable order for Greater London was deemed illegal in *Gillian and Quinto v. the United Kingdom*.

Using real-time FRT for "point defense" is both less and more intrusive than these cases. It is more intrusive because the FRT network process the biometric data of everyone entering a particular location. However, only the people on the watchlist could identified. In *Colon v. the Netherlands* the authorization for stop and search and requiring identification was indiscriminate, so everyone could be subjected to it. Even though the zone was quite large, encompassing almost all of the "*old city center*",[181] so police might not have been able to identify and search everyone within the zone during the twelve hours the authorization was in effect, real-time FRT for "point defense" would be much more targeted. It would also be geographically more limited, only deployed in select locations.

A real-time FRT network would still indiscriminately process the personal data from everyone entering line-of-sight, but the ECtHR has previously stated that such indiscriminate processing is not per se illegal.

In *Beghal v. the United Kingdom*, the Court also accepted in principle zones where police enjoy wider powers to stop and search individuals are legal under Article 8, even though the Applicant in that case had her right to privacy cfr. Article 8 violated. Concerning the power TACT Schedule 7 gave police officers at ports or border controls to stop, search or detain people without reasonable suspicion to determine whether they were terrorists or not, the Court said:

> "intelligence gathered during the examinations… contributed to a rich picture of the terrorist threat to the United Kingdom and its interests abroad, and could assist in the disruption or deterrence of terrorists' plans….Were "reasonable suspicion" to be required, terrorists could avoid the deterrent threat of Schedule 7 by using people who had not previously attracted the attention of the police ("clean skins"); and the mere fact of a stop could alert a person to the existence of surveillance….."[182]

[180] *Colon v. the Netherlands* § 3 and § 93

[181] Ibid. § 3

[182] Ibid. § 95

This means that stop and search police powers for counterterrorism do not necessarily require reasonable suspicion. It is an important, but not required, safeguard to protect against arbitrary interference which is the decisive factor. The Court also noted that:

> "ports and border controls will inevitably provide a crucial focal point for detecting and preventing the movement of terrorists and/or foiling terrorist attacks. Indeed, all States operate systems of immigration and customs control at their ports and borders, and while these controls are different in nature to the Schedule 7 powers, it is nevertheless the case that all persons crossing international borders can expect to be subject to a certain level of scrutiny".[183]

Thus, it seems like establishing of zones with increased protection, and wider powers for police to stop and search individuals without reasonable suspicion, and require their ID is in principle legal under ECHR Article 8. However, as shown by Chapter 3.2.2.3.1, inclusion on the watch-list for real-time FRT would be based on somewhat reasonable suspicion.

As to the use of surveillance cameras and visual surveillance in these zones, the ECtHR stated in *Perry v. the United Kingdom*, that "*the normal use of security cameras per se… in the public street or on premises, such as shopping centres or police stations where they serve a legitimate and foreseeable purpose, do not raise issues under Article 8 § 1 of the Convention*."[184] This means visual surveillance in these zones is legal even though real-time FRT equipped CCTV-cameras is not "*normal use of security cameras*".

Real-time FRT has the risk of false positives in a way these cases do not. False positives, i.e., when a misidentified as being on the watchlist, are not necessarily a big problem. If a person is misidentified, and stopped by police, they could either show and ID, and prove their identity, thus granted access, perhaps also without being searched. Searching them could probably also be done.[185] If they do not have an identity with them, and police are convinced they are a person eligible for detainment, they would be detained. However, they cannot be detained for long before police must ask a court for further extension, in which case the misidentification most likely would be resolved, and they would be let go. The real identity of the detained person

[183] Ibid. § 92

[184] *Perry v. the United Kingdom* § 40

[185] See *Beghal v. the United Kingdom*

could probably be ascertained before this too. Such detainment would obviously be an intrusive interference with both Article 8 and Article 2 Protocol 4, but that would be the price required to use such a system.

How the "fear" that a real-time FRT system might be deployed impacts the right to freedom of movement cfr. ECHR Article 2 Protocol 4, the Court stated in *Colon v. the Netherlands* that a fear of being stopped and searched, without being prevented from entry cannot be considered an interference with the freedom of movement.[186] The case of *Colon v. the Netherlands* is different because the special security zone was announced to the public, whilst the use of real-time FRT for "point defense" and the protected locations would be secret.[187] This secrecy would also have a "chilling effect", however if the law states that real-time only can be used for "point defense", the chilling effect would probably be less severe because citizens would know that the surveillance at least was limited geographically.[188]

This geographical limitation would also have an effect on how much other information could be inferred using real-time FRT. When used for "point defense", real-time FRT would only track when someone enters the protected location, and not the movement of people or which places they frequent etc. Used for this purpose, the visual surveillance aspect of real-time FRT would also reveal "sensitive information", i.e., health data or sexual preferences, about fewer people than when used for "preventative investigation" since it would only do so in the protected locations, not across a city.

When it comes to other, less intrusive options, there are no viable alternatives to real-time FRT for "point defense". FRT is intrinsically a tool for both surveillance and identification at the same time and a real-time FRT can regulate who and block people from entering a location/event and also do surveillance to gather intelligence from the protected location/event simultaneously without being noticed.

The only other solution which could accomplish both these tasks less intrusively, although not secretly, would be the set up manual identification checkpoints for every entrance into the place

[186] *Colon v. the Netherlands* § 97-100

[187] See Chapter 1.2

[188] See previous chapter for "chilling effect"

intended to be protected by the FRT system, and keep the normal CCTV surveillance. This is probably not a practical solution for protecting locations thousands of people enter every day, but is used at events. There might not be enough police and/ security guards in a city for manual checkpoints at every high-value target, and regular police work/security. Manual checkpoints would also create a huge logistical bottleneck, akin to passport controls in airports, which probably could not work in everyday life. "Post" FRT would not work either because practically, people entering the protected locations cannot wait for a "*significant delay*" cfr. AIA Article 3(37).

These cases, lack of alternatives, and how geographical constraints limits the intrusiveness of real-time FRT by geographical constraints seems to indicate that setting up a real-time FRT network for "point defense" is in principle legal. The legality will depend on if it is "in accordance with the law".

Where could real-time FRT for "point defense" be set up? For a location confirmed by law enforcement and/or intelligence as the target for the terror attack the question is unproblematic. Real-time FRT could be deployed there. In cases without a confirmed target, the question is less clear.

In the case *Colon v. the Netherlands* the designation of most of the old city center of Amsterdam as a special security zone was based on the need to combat the rise of violent crime, and amounts of illegal weapons present.[189] This zone was specifically designated because statistics showed that these places were overrepresented with regards to where violent crime happened. Applied to the use of real-time FRT for the purpose of "point defense", this could mean places where law enforcement and/or intelligence agencies could designate places to be protected either based on previous statistics as to where terror attacks are likely to happen, and/or where they have specific intelligence indicating something to be a possible target.

Alongside this, there are probably some places which could be protected by default. The case *Beghal v. the United Kingdom* mentions travel points, e.g., airports and train stations etc. specifically. Travel points could perhaps be protected by default. They could either be a target of

[189] *Colon v. the Netherlands* § 3-4

an attack due to the amount of people present or a good way of catching the perpetrators when they are accessing the country.

Other places, such as governmental headquarters and critical infrastructure where the public normally either do not have access or very limited access, e.g., power plants, water supplies and communications stations, may be protected by default as well. If the public generally either do not have or very limited access, the interference with their rights would not be very intrusive since they cannot be there in the first place, and the consequences of a successful attack against such places might be much more devastating than a successful attack against a town square.

3.2.2.4 Summary

The use of real-time FRT for the prevention of a terror attack proposed exempt under AIA Article 5(1)(d)(ii) is probably in principle legal under ECHR Article 8. What purpose it can be used for is difficult to say. If the purpose of "preventative investigation" would be legal is very unclear, but the purpose of "point defense" is more likely to be legal since it is less intrusive by being limited in scope to only select locations. If the use is legal depends on the clarity of the law and safeguards to protect against abuse in the legislation authorizing the use of real-time FRT to prevent a terror attack. In case only the purpose of "point defense", and not "preventative investigation", is legal, the law authorizing the use of real-time FRT must also have adequate safeguards to prevent the use of real-time FRT for "point defense" from gliding over into "preventative investigation".

In any case, the use of real-time FRT in publicly accessible places would have to be subjected to very strict safeguards to prevent abuse. The vagueness of terrorism, and terror attack is problematic in this regard, and influences how strong the aforementioned legal safeguards required must be. These safeguards should include adequate safeguards in the criteria for when it can be used,[190] sufficient judicial review,[191] clear delimitations concerning which, and the number of, places which can be protected using such a system, equally clear limitations concerning who can be added to the database necessary for the FRT system to function, and adequate safeguards

[190] See discussion in Chapter 3.2.3

[191] See discussion in point 3.2.3.2

preventing unnecessary retention of biometric templates. Lastly, the law must clearly state and limit the powers of what law enforcement can do in case of a match. These safeguards, and how they are envisioned in AIA Article 5 will be discussed in the next chapter.

3.2.3 In accordance with the law

Even though AIA Article 5 is not a legal basis for the use of real-time FRT in public places, it does have some requirements in Article 5(1)(d)(ii), 5(2) and 5(4) that must be fulfilled for a domestic law authorizing the use of real-time FRT in public by law enforcement to not violate AIA. This section will analyze these legislative requirements and see if they are "in accordance with the law" under ECHR Article 8 if implemented "verbatim" in the domestic law of Member States.

The requirement of "*in accordance with the law"* has two aspects. Firstly, the foreseeability-requirement i.e., any law authorizing an interference with a fundamental right must be sufficiently clear. The law must be written in a way as to allow the citizens to reasonably know when the state may use its' discretionary powers and when they might be subjected to it.[192] Laws authorizing an interference with a fundamental right must also be adequately accessible to the public.[193] The level of precision required of the domestic law authorizing the interference depends on the intrusiveness of the interference.[194] Laws authorizing very intrusive measures, e.g., secret surveillance, has a stricter foreseeability-requirement than laws authorizing less intrusive measures.

Secondly, the law must have sufficient legal safeguards, to prevent against abuse.[195] The level of protection and safeguards required for a law to be "in accordance with the law" correlates with the intrusiveness of the interference. Such protections can be e.g., measures for excluding illegally obtained evidence or requirements for judicial review.[196]

[192] Pool (2017) page 132 and *Malone v. the United Kingdom* § 67

[193] This will be discussed in greater detail in chapter 3.2.3.2.2

[194] *Gillan and Quinton v. the United Kingdom* § 77

[195] "Guide to Article 8" page 11

[196] See *Uzun v. Germany* § 72

3.2.3.1 Foreseeability-requirement with regards to AIA Article 5(1)(d)(ii)

The foreseeability-requirement for secret surveillance is a bit different. In the case *Roman Zakharov v. Russia*, the ECtHR stated that "*foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly*".[197] If the suspect could foresee this, the surveillance would be pointless. However, the foreseeability-requirement does demand the domestic law have "*clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated.*"[198] This is true for other forms of secret surveillance as well.

In *Big Brother Watch and Others v. the United Kingdom* the Court established criteria for laws concerning secret surveillance and bulk interception of data to be in accordance with the law. The Court stated it needed to update the criteria for foreseeability with regards to bulk interception from the safeguards for targeted interception of communications which followed from the case *Weber and Saravia v. Germany*.[199] The criteria established by the Court were if the law defined with sufficient clarity *inter alia*:

> "the grounds on which bulk interception may be authorised;
> the procedure to be followed for granting authorisation;
> the procedures to be followed for selecting,
> examining and using intercept material;
> the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
> the procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance".[200]

The details concerning exactly what kind of data was intercepted is not as important when analyzing how this case can guide the assessment of real-time FRT with regards to "in accordance

[197] *Roman Zakharov v. Russia* § 229

[198] I.c.

[199] *Big Brother Watch v. the United Kingdom* § 361

[200] Ibid. § 361

with the law". The most interesting thing is what grounds the Court considered sufficiently well-defined to allow for bulk interception, and which safeguards was required.

3.2.3.1.1 The notion of "terror attack" in AIA Article 5(1)(d)(ii)

AIA Article 5(1)(d)(ii) exempts the use of real-time FRT in public places by law enforcement than to prevent a "terror attack" from the general prohibition.[201] Terrorism, and by extension terror attack, is a concept without a universally agreed upon definition. The question is if terrorism is a sufficiently clear legal constraint to protect against arbitrary (ab)use and allow citizens to reasonably know when the state may use its real-time FRT in publicly accessible places?

Because of how intrusive real-time FRT is, the legal restraint regulating its' use should be proportionally strong. Terrorism is hard to define and often as much of a political issue as a legal issue.[202] Legal experts have expressed skepticism about the possibility of reaching an international consensus regarding what defines terrorism.[203] Despite this, the cases of *Beghal v. the United Kingdom* and *Big Brother Watch and Others v. the United Kingdom* can provide some guidance on the notion of "terrorism" with regards to the foreseeability-requirement.

In the case *Beghal v. the United Kingdom* UK police officers' at ports or border controls[204] powers to stop, search and "detain"[205] to "*question a person to whom this paragraph applies for the purpose of determining whether he appears to be a person falling within section 40(1)(b)*" cfr. the Terrorism Act of 2000 (TACT) Schedule 7. Terrorism was defined in subsection 40 (1) b as anyone who "*is or has been concerned in the commission, preparation or instigation….*" of:

> 1) "In this Act "terrorism" means the use or threat of action where—
> (a) the action falls within subsection (2),

[201] And of course, the other two exempted uses.

[202] Di Filippo (2020) page 4

[203] I.c.

[204] Ibid. § 40

[205] Not formally detain, but prevent from leaving cfr. *Beghal v. the United Kingdom* § 96

(b) the use or threat is designed to influence the government or to intimidate the public or a section of the public, and
(c) the use or threat is made for the purpose of advancing a political, religious or ideological cause.

(2) Action falls within this subsection if it—
(a) involves serious violence against a person,
(b) involves serious damage to property,
(c) endangers a person's life, other than that of the person committing the action,
(d) creates a serious risk to the health or safety of the public or a section of the public, or
(e) is designed seriously to interfere with or seriously to disrupt an electronic system."[206]

Both a UK court and the ECtHR noted that the wide definition of "terrorism" gave police broad discretionary powers, which was problematic.[207] The broad discretionary powers this definition gave rise to was not decisive on its own, however, coupled with a lack of judicial review or other oversight and the already broad discretionary powers the stop and search without reasonable suspicion practice entailed, it was considered a violation of ECHR Article 8. This means that the ground for interference could be wider with adequate safeguards to protect against abuse.

In *Big Brother Watch and Others v. the United Kingdom* the ECtHR took the same position.[208] In this case, a warrant for bulk interception of communications data could be issued by the executive if they deemed it necessary "*in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well-being of the United Kingdom so far as those interests were also relevant to the interests of national security*."[209]

"national security" allowed surveillance of activities which threatened the safety or well-being of the State and activities which were intended to undermine or overthrow parliamentary democracy by political, industrial or violent means

[206] Ibid. § 39

[207] Ibid. § 93 and § 72.

[208] *Big Brother Watch and Others v. the United Kingdom* § 371

[209] Ibid. § 368

> serious crime was defined in section 81(2)(b) of RIPA as a crime for which the perpetrator (assuming he or she was over the age of twenty-one and had no previous convictions) could reasonably be expected to be sentenced to imprisonment for a term of three years or more; or where the conduct involved the use of violence, resulted in substantial financial gain or was conducted by a large number of persons in pursuit of a common purpose."[210]

With regards to the clarity of the grounds the Court noted that they were considered to be wide, and that wider grounds offered greater potential for abuse, although the Court accepted these grounds for interception of data, if the safeguards to prevent abuse ware adequate.[211] What is decisive was again how the safeguards designed to prevent the potential abuse wide grounds for an interference provides.

The EU's definition of "terrorism", in a directive aimed at combating terrorism, is equally wide as the UK's and can be liable for authoritarian interpretation. Terrorism is defined as an exhaustively defined list of criminal offences, e.g., kidnapping or hostage-taking, attacks against the life of a person and hijacking an aircraft or other means of transportation, done for the purpose of;

> "seriously intimidating a population
> unduly compelling a government or international organisation to perform or abstain from performing any act
> seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organization".[212]

All these grounds are vague and open to expansive interpretation. E.g., an organized criminal enterprise murdering witnesses during an investigation and/or trial to keep others from testifying could be argued to be "*seriously intimidating a population*", i.e., making the criminal enterprise a terrorist organization. Perhaps especially if the criminal enterprise occupies a dominant position in a geographical region of a country, with influence and power rivalling a local or national government,[213] making them able to commit crimes with impunity because no one

[210] Ibid. § 369

[211] Ibid. § 370-371

[212] Cfr. Directive 2017/541/EU Article 3(2)

[213] Like some drug cartels in Latin-America do. Source: Felbab-Brown (2022)

wants to testify. This shows how quickly a law permitting deeply intrusive surveillance on the grounds of counterterrorism over time could be expansively interpreted. In the same way the Trump administration contemplated designating Mexican drug cartels as terrorist organizations,[214] the government of an EU Member State could invoke the notion of terrorism to justify the use of real-time FRT in a crackdown against narcotics.

However, there is no indication in AIA that the EU definition must be guiding in the domestic law of member states, but it illustrates the problem well. These uncertainties opens up for really pushing the boundaries by opening up the definition of "terrorism" and keeping the system on for extended periods of time due to the lack of clarity on the temporal restrictions for "terror attack". This could lead to a situation where a government couples the ambiguity of terrorism, with the tactic of using terrorism as a pretext for authoritarian policies, to justify widespread surveillance of a large portion of the population. Also considering how intrusive surveillance real-time FRT makes possible, allowing their use for counterterrorism comes with a credible risk of massive violations of the right to privacy. There is no guarantee that will happen, yet it seems like a possibility given how different European intelligence agencies and Europol have conducted mass surveillance in the past,[215,216] and perhaps still do.

The definition of terrorism in TACT largely mirrors the EU definition. As another example, the Norwegian definition of "terrorism" is mostly identical to the EU's definition, and even perhaps a little wider since it explicitly adds critical infrastructure to the criterion mirroring the thirds criterion in the EU definition.[217] How these three definitions compare to that of the various member states is beyond the scope of this paper, but what can be extrapolated from this is that terrorism is hard to define in a way which do not leave wiggle-room for wide interpretations. With regards to real-time FRT this uncertainty is important when assessing the necessity of "point defense" and "preventative investigation".

Thus, it seems like the ECtHR has accepted "terrorism" as an adequately foreseeable ground for authorizing intrusive interferences with the right to privacy in Article 8. This is important

[214] Reuters (2019)

[215] Bigo (2013) page 39, 45, 49, 52-53 and 57.

[216] Fotiadis (2022)

[217] Penal Code § 131

with regards to AIA Article 5(1)(d)(ii) because it has a stricter and clearer ground for authorizing the use of real-time FRT than thee aforementioned cases.

3.2.3.1.2 "Specific and imminent attack" as a legal restraint in AIA Article 5(1)(d)(ii)

The prohibition against authorizing the use of real-time FRT except for a "*specific and imminent attack"* in public for counterterrorism in AIA Article 5(1)(d)(ii) is an important safeguard to protect against arbitrary interference and abuse. This narrows the scenarios Member States are allowed to authorize the use of real-time FRT in public more than just the notion of "terrorism" or counterterrorism the which it seems like ECtHR has accepted.

The grounds for the bulk interception scheme in *Big Brother Watch v. the United Kingdoms* did not require that the surveillance be in response to an "*imminent*" nor a "*specific*" threat, something the Court did not discuss.[218] However, the Court noted that a requirement of "reasonable suspicion" was "*less germane in the bulk interception context, the purpose of which is in principle preventive when surveillance is done for preventative purposes*."[219] Since bulk interception does not require reasonable suspicion, it could be argued that the Court's logic also could be applied to the use of real-time FRT, meaning requirements of a "*specific*" and "*imminent*" threat might not be required under ECHR Article 8, perhaps especially for "preventative investigation". The Court seems to accept looser safeguards when it comes to preventative surveillance, rather than targeted surveillance.[220] The use of real-time FRT for "preventative investigation" would be more preventative in nature than "point defense". It is supposed to discover, investigate, and foil the plot as early as possible. Thus, it would seem like requiring the threat to be "*specific*" and "*imminent*" in AIA Article 5(1)(d)(ii) is stricter than what the ECtHR deems necessary, especially for "preventative investigation". The Council removed the requirement that the threat must be "*imminent*" in their latest version of AIA Article 5(1)(d)(ii).[221] This may perhaps be legal under ECHR Article 8, but it should remain in the final version, as a safeguard to prevent abuse and to ensure compliance with ECHR Article 8.

[218] *Big Brother Watch v. the United Kingdom* § 368-371

[219] Ibid. § 348

[220] Ibid. § 348

[221] COD(2021) 14278/21 page 57

The notion of "*attack*" in AIA Article 5(1)(d)(ii) also seems to further ensure compliance with ECHR Article 8. As mentioned above, the Court has accepted intrusive measures and surveillance on the grounds of "general counterterrorism" in the cases of *Beghal v. the United Kingdom* and *Big Brother Watch and Others v. the United Kingdom*. Specifying that real-time FRT may only be used by law enforcement in public in response to an "*attack*" could prevent abuse, both in the form of using it when there is no indication that an attack might happen and for other criminal offences. It might be easier both legally and politically to designate organized criminal enterprises as terror organizations as mentioned above, than to state that their crimes constitute a "*terror attack*". Furthermore, AIA Article 5(1)(d)(ii) in its' current form, requires that the threat of an attack be "*specific*". This requirement is well suited to stop law enforcement and/or intelligence agencies from raising the threat level in a country, hinting vaguely at a possibility of an attack happening.

All these requirements and how effective they are or would be in preventing abuse must be assessed in conjunction with the requirement of prior judicial authorization by an independent organ cfr. AIA Article 5(3) cfr. Article 5(2).

3.2.3.2 Judicial review in AIA Article 5(3)

AIA Article 5(3) requires that Member States authorizing the use of real-time FRT under the proposed exemption, include a mechanism to subject the use to judicial review by a court or another independent administrative organ, except in a "*duly justified situation of urgency*".

In *Big Brother Watch and Others v. the United Kingdom,* the bulk interception regime operated by the UK intelligence community worked like this: the intelligence community could intercept all traffic flowing through data bearers with regards to external communications. All the intercepted data was retained. Then there were two forms of selection processes for what data to be further examined: either a software ranked the data after probability of intelligence value using "complex queries",[222] or the software used "selectors"[223] to search the data for matches against the "selectors". After this, the data not singled out by the two processes was discarded without

[222] This was not defined in the judgement

[223] Search words for the software going through the intercepted data

being searched by humans.[224] The warrants for such interception was made by the directors of the intelligence agencies to the executive. That the warrant was granted by the executive, not an independent organ was criticized by the Court.[225] The biggest problem the Court had with the process of granting the warrant was that the selectors, and particularly the strong selectors,[226] only were subjected to an independent review after the warrants were granted.[227] This meant that "*section 8(4) did not meet the "quality of law" requirement and was therefore incapable of keeping the "interference" to what was "necessary in a democratic society*"[228] and a violation of ECHR Article 8.

Based on this, the requirement of prior independent judicial review for the use of real-time FRT in AIA Article 5(3), is probably necessary for any legislation under ECHR Article 8. AIA Article 5(3) also requires that the independent organ reviewing requests for the use of real-time FRT consider "*personal limitations*" when assessing the necessity cfr. Article 5(2). As shown by *Big Brother Watch and Others v. the United Kingdom,* this is also probably necessary for a law authorizing the use of real-time FRT to be "in accordance with the law".

However, since intelligence agencies neither inform the public about their knowledge of a planned attack, nor should be required to, since that would make their job impossible, the mechanisms for judicial review proposed in AIA Article 5(3) would probably have to be secret hearings.

Generally, such secret hearings can be problematic, by evolving into a sham process over time. The system of secret courts reviewing surveillance requests under the Foreign Intelligence Surveillance Act in the US is an example of this. The FISA-courts were established for "[assessing] *applications submitted by the United States Government for approval of electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes*".[229] Proceedings are classified with limited oversight. This has proven prone to abuse and lackluster

[224] *Big Brother Watch and Others v. the United Kingdom* § 17,18 and 325.

[225] Ibid. § 377

[226] These are selectors which can identify an individual cfr. *Big Brother Watch and Others v. the United Kingdom* § 346.

[227] Ibid. § 383

[228] Ibid. § 426

[229] Foreign Intelligence Surveillance Court

judicial control. In the period between 1973, the US Government delivered 35 333 requests for electronic surveillance to the FISA Court. Of these 35 333 requests, only 12 were denied, and only 532 modified to get approved.[230] Since these proceedings are classified, it is impossible to comment on the merit of each individual request, but the general trend is worrying. It does not seem to be hard to get a request for such electronic surveillance approved by the FISA Court.

Such hearings could evolve into a blank cheque for law enforcement and intelligence agencies to keep it turned on continuously when they raise the threat level in a nation, similar to what happened with the FISA-courts. This would erode any confidence the public has in them, and that confidence from the public is crucial for mitigating the "chilling effect" discussed in Chapter 3.2.2.

When assessing the adequacy of safeguards against arbitrary interference and abuse, the existence or lack of evidence of arbitrary interference or abuse is an important factor.[231] Because this paper analyses whether the situation proposed exempted in AIA Article 5(1)(d)(ii) and the requirements to the domestic laws of Member States in AIA Article 5 paragraph (2) and (3) are permissible in general, and not any one specific case in a member state, this is not applicable.

However, requiring the exempted situation to authorize the use of real-time FRT for counter-terrorism in AIA Article 5(1)(d)(ii) to be an "*imminent and specific attack*" could perhaps stop judicial hearings evolving into such a sham process. If the threat must be "*specific*", law enforcement would have to go to a court with evidence of a specific threat, instead of vague threats a terror group has issued against a country. If the threat must be "*imminent*", law enforcement/intelligence agencies would also have to present evidence to the court with regards to the temporal aspect. These two requirements would mean that law enforcement would have to present more evidence for more additional criteria when requesting authorization to use real-time FRT from the court, than was the case in e.g., *Big Brother Watch and Others v. the United Kingdom*.

3.2.3.2.1 Geographical and personal limitations

[230] Epic.org (2015)

[231] See *Big Brother Watch v. the United Kingdom* § 360

Furthermore, the requirement of "*specific*" in AIA Article 5(1)(d)(ii) might also help prevent against abuse with regards to "*geographic and personal limitations*" cfr. AIA Article 5(2)(2). The court granting an authorization for using real-time FRT shall only do so when it is satisfied by "*objective evidence or clear indications presented to it*"[232] that the use of real-time FRT is necessary and proportionate to achieve the stated goal, and the court shall consider the "*elements referred to in paragraph 2*"[233] i.e., "*geographic and personal limitations*". This means that law enforcement must present evidence to the court regarding which group made the threat and where it might materialize if they possess such evidence. This means that if a Member State's law enforcement and intelligence agencies discover a threat from ISIS against a target in the capital, it might not be necessary to surveil people affiliated with right-wing extremism in the opposite part of the country. The court could then perhaps more easily stop unnecessary surveillance if it were attempted.

4 Conclusion

As the *Roman Zakharov v. Russia case* shows, a law does not need to explicitl state exactly when a government may use its' capability for secret surveillance. It only needs to give an adequate indication for when they might employ it. If real-time FRT is used for "preventative investigation" it does seem like thee legal safeguards envisioned in AIA Article 5 are adequate, and the grounds which can authorize its' use are sufficiently clear. If real-time FRT only can be used for "point defense", laws in Member States should state that it cannot be used city or country wide. The passage that the independent judicial authority reviewing and authorizing the use of real-time FRT only shall consider the "*geographical limitations*" in AIA Article 5(2(2) cfr. Article 5(3) with regards to necessity and proportionality might be a bit vague.

If the safeguards proposed in AIA Article 5 actually are adequate in protecting against arbitrary interference and preventing abuse remains to be seen. IF the safeguards actually are good enough when implemented in the individual member states will largely depend on the existence or lack evidence of arbitrary interference or abuse.[234] What can be said is that based

[232] AIA Article 5(3)(2)

[233] AIA Article 5(3)(2)

[234] *Big Brother Watch v. the United Kingdom* § 360

on ECtHR case-law, the required safeguards and exemption for a "*specific and imminent terror attack*" seems adequate in theory.

Thus, it seems like the use of real-time FRT under the proposed exemption in AIA Article 5(1)(d)(ii) could legally be used according to ECHR Article 8. If it can be used for mass surveillance in a way like or similar to "preventative investigation" is unclear, but it seems like it probably at least could be used for "point defense". However, the ECtHR has never assessed any use of real-time FRT before, so what the Court would say if a case ever were tried is hard to say. In that case, evidence showing either abuse or compliance with the safeguards would probably be an important factor in assessing the legality of that specific case, but that might not necessarily mean that it cannot in principle be used under the proposed exemption in AIA Article 5(1)(d)(ii).

5 Final remarks

The purposes of "point defense" and "preventative investigation" are not mentioned in AIA, but are something defined for the purpose of this paper. The reason for this was to illustrate two different ways real-time FRT could be used for counterterrorism under the exemption proposed in Article 5(1)(d)(ii) with regards to ECHR Article 8.

One of the purposes of AIA is to introduce "*harmonized rules*"[235] for placement, sale, use and prohibition on certain use of AI systems in the single market,[236] and to provide a common European approach to the regulation of AI and ""*real-time" remote biometric identification systems*." Leaving the details of regulating the use of real-time FRT under the proposed exemption to the Member States could run contrary to this idea if regulation could vary by this much. The proposed exemptions in AIA should be more detailed and specify which of the two purposes could be allowed to extend equal protection against the risks the use of real-time FRT poses to the fundamental rights of European citizens.

[235] Cfr. AIA Art 1(a)

[236] Cfr. AIA Art 1(a)

6 Bibliography

6.1 Literature

AlgorithmWatch, “EU policy makers: Protect people’s rights, don’t narrow down the scope of the AI Act!” 23.11.21, https://algorithmwatch.org/en/statement-scope-of-eu-ai-act/, retrieved 16.10.22

Anti-Defamation League, “Gab and 8chan: Home to Terrorist Plots Hiding in Plain Sight”, 04.05.19, https://www.adl.org/resources/reports/gab-and-8chan-home-to-terrorist-plots-hiding-in-plain-sight, retrieved 25.10.22

Bates, Rodger A. “Tracking Lone Wolf Terrorists”, *The Journal of Public and Professional Sociology*, Volume 8, Issue 1, Article 6, March 2016, https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1111&context=jpps

Big Brother Watch, “Stop facial recognition”, NTA, https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/#facial-recognition-uk, retrieved 25.10.22

Bigo, Didier, Nicholas Hernanz and Sergio Carrera et al. “Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law.” *Liberty and Security in Europe*, No. 62 (2013)

Borshoff, Isabella, “UK court backs police in facial recognition lawsuit.” *Politico*, 04.09.2019, https://www.politico.eu/article/uk-court-backs-police-in-facial-recognition-lawsuit/, retrieved 26.09.22

Brown, Sara. “Machine learning, explained.” 21.04.21, https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained, retrieved 16.10.22

Brussels Times, “Belgian police illegally used facial recognition software.” *Brussels Times*, 11.10.21, https://www.brusselstimes.com/188743/belgian-police-illegally-used-facial-recognition-software, retrieved 14.09.22

Buchholz, Katharina. “The Most Surveilled Cities in Europe”, 06.09.2019, https://www.statista.com/chart/19268/most-surveilled-cities-in-europe/, retrieved 15.10.22

Bischoff, Paul. “Surveillance camera statistics: which cities have the most CCTV cameras?” 11.07.22, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/, , retrieved 15.10.22

Cahall, Bailey, Peter Bergen, David Sterman and Emily Schneider, “Do NSA's Bulk Surveillance Programs Stop Terrorists?”, 13.01.2014, https://www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/, retrieved 25.10.22

Captain William A. Perkins, “Component Integration Challenges presented by Advanced Layered Defence Systems (A2/AD).” *The Three Swords Magazine*, nr. 33/ March 2018, p. 52-64, https://www.jwc.nato.int/images/stories/threeswords/A2AD_2018.pdf

Clarke, Laurie. “MEPs are preparing to debate Europe’s AI Act. These are the most contentious issues”, *Techmonitor*, 20.04.21, https://techmonitor.ai/policy/eu-ai-regulation-machine-learning-european-union, retrieved 27.10.22

College of Policing, “Live facial recognition”, 22.04.22, https://www.college.police.uk/app/live-facial-recognition/live-facial-recognition, retrieved 15.09.22

Council of the European Union and the European Council, “The ordinary legislative procedure”, 07.04.22
https://www.consilium.europa.eu/en/council-eu/decision-making/ordinary-legislative-procedure/, retrieved 10.10.22

Council of Europe. “Guide to Article 8 of the European Convention on Human Rights — Right to respect for private and family life, home and correspondence”, 31.08.22, https://www.echr.coe.int/documents/guide_art_8_eng.pdf, retrieved 25.10.22

Council of Europe, “Guide to the Case-Law of the of the European Court of Human Rights — Data Protection”, 31.08.22, https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf

Council of Europe, "Guide on Article 2 of Protocol No. 4 to the European Convention on Human Rights — Freedom of movement", 31.08.22, https://www.echr.coe.int/Documents/Guide_Art_2_Protocol_4_ENG.pdf

Council of Europe, "The European Convention on Human Rights — A Living Instrument", September 2022, https://www.echr.coe.int/Documents/Convention_Instrument_ENG.pdf

Crumpler, William. "How Accurate are Facial Recognition Systems – and Why Does It Matter?" 14.04.2020, https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter, retrieved 16.10.22

Cox, Joseph. "Inside the Phone Company Secretly Run by Drug Traffickers." *Vice News,* October 22, 2019. https://www.vice.com/en/article/wjwbmm/inside-the-phone- company-secretly-run-by-drug-traffickers, retrieved 16.10.22

Di Fillipo, Marcello. "The Definition(s) of Terrorism in International Law" in *Research Handbook on International Law and Terrorism*, Ben Saul (eds), 2. Edition, Cheltenham: Edward Elgar Publishing, 2020, pp. 2-15, https://doi-org.ezproxy.uio.no/10.4337/9781788972222, E-Book

Domanska, Olena. "machine learning vs traditional programming", 17.12.21, https://www.avenga.com/magazine/machine-learning-programming/, retrieved 20.10.22

Epic.org, "Foreign Intelligence Surveillance Act Court Orders 1979-2014", 23.07.15, https://web.archive.org/web/20150723190947/https:/epic.org/privacy/wiretap/stats/fisa_stats.html, retrieved 16.10.22

European Commission, "Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence." 21.04.21, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682, retrieved 20.10.22

European Commission. "What is the European Data Protection Board (EDPB)?" https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-

organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_en, retrieved 16.10.22

European Commission by Monica Lloyd and Annelies Pauwels, *Lone Actors as a Challenge for P/CVE* Luxembourg: Publications Office of the European Union, 2021, https://home-affairs.ec.europa.eu/system/files/2021-10/ran_lone_actors_as_challenge_for_pcve_july_2021_en.pdf, retrieved 16.10.22.

European Parliament Resolution, 2020/2016(INI), 06.10.21 "Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters." https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

European Parliament, "Use of artificial intelligence by the police: MEPs oppose mass surveillance." 06.10.21, https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance, retrieved 20.10.22

European Parliament Research Service by Tambiama Madiega and Hendrik Mildebrath, *Regulating Facial Recognition in Europe*, PE 698.021. Brussels:2021. DOI: 10.2861/140928

European Data Protection Board. "Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement Version 1.0." 12.05.22, https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf

European Data Protection Board and European Data Protection Supervisor, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)* 18.06.21, https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps_joint_opinion_ai_regulation_en.pdf

Eurostat, Population density by NUTS 3 region", 20.08.21, https://ec.europa.eu/eurostat/databrowser/view/DEMO_R_D3DENS__custom_2790211/bookmark/table?lang=en&bookmarkId=d1a9a590-0543-45b0-ab08-805a3fea0b5e, retrieved 15.10.22

Feldstein, Stevens. “The Global Expansion of AI Surveillance”, *Carniege Endowment*, 17.09.2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847, retrieved 08.11.22

Felbab-Brown, Vanda, “How Mexico’s Cartel Jalisco Nueva Generación rules”, *Brookings*, 29.05.22, https://www.brookings.edu/opinions/how-mexicos-cartel-jalisco-nueva-generacion-rules/, retrieved 25.10.22

Fotiadis, Apostolis, Ludek Stavinoha, Giacomo Zandonini, Daniel Howden, “A data ‘black hole’: Europol ordered to delete vast store of personal data”, *The Guardian*, 10.01.22, https://www.theguardian.com/world/2022/jan/10/a-data-black-hole-europol-ordered-to-delete-vast-store-of-personal-data, retrieved 25.10.22

Gall, Lydia. “Dispatches: The End of Liberal Democracy in Hungary?”, 29.07.2014, https://www.hrw.org/news/2014/07/29/dispatches-end-liberal-democracy-hungary, retrieved 25.10.22

Gerards, Janneke “How to improve the necessity test of the European Court of Human Rights”, *International Journal of Constitutional Law*, Volume 11, Issue 2, April 2013, pp. 466–490, https://doi.org/10.1093/icon/mot004

Goujard, Clothilde. “Europe edges closer to a ban on facial recognition.” *Politico*, 20.09.22, https://www.politico.eu/article/europe-edges-closer-to-a-ban-on-facial-recognition/, retrieved 26.09.22

Greenwald, Glenn and Ewen MacAskill, “NSA Prism program taps in to user data of Apple, Google and others”, *The Guardian*, 07.06.2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, retrieved 16.10.22,

Hill, Kashmir. “The Secretive Company That Might End Privacy as We Know It.” *The New York Times*, 02.11.21, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html, retrieved 20.09.22

Holden, Katherine on behalf of TechUK, "TechUK response to the Commission's proposed Artificial Intelligence Act", 06.08.21, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665579_en, retrieved 27.10.22

Human Rights Watch, *Silencing Turkey's Media The Government's Deepening Assault on Critical Journalism*, ISBN: 978-1-6231-3427. United States of America: 15.12.16, https://www.refworld.org/docid/5852a8a54.html

Institute for Economics & Peace. *Global Terrorism Index 2019: Measuring the Impact of Terrorism*, Sydney: November 2019. https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2019-web.pdf, retrieved 16.10.22.

Interpol, "Preventing Terrorist Travel", (NTA), https://www.interpol.int/en/Crimes/Terrorism/Preventing-terrorist-travel, retrieved 12.11.22

Interpol, "Identifying Terrorist Suspects", (NTA), https://www.interpol.int/en/Crimes/Terrorism/Identifying-terrorist-suspects, retrieved 12.11.22

Khan, Mehreen. "EU plans sweeping regulation of facial recognition." *Financial Times*, 22.08.2019, https://www.ft.com/content/90ce2dce-c413-11e9-a8e9-296ca66511c9, retrieved, 26.09.22.

Kayali, Laura. "How facial recognition is taking over a French city." *Politico*, 26.09.19, https://www.politico.eu/article/how-facial-recognition-is-taking-over-a-french-riviera-city/, retrieved 26.09.22

Lindsey Jacques, "Facial Recognition Technology and Privacy: Race and Gender - How to Ensure the Right to Privacy Is Protected," *San Diego International Law Journal 23*, no. 1 (2021): 111-156, https://heinonline-org.ezproxy.uio.no/HOL/Page?public=true&handle=hein.journals/sdintl23&div=8&start_page=111&collection=usjournals&set_as_cursor=0&men_tab=srchresults

Li, Eileen. “Europe’s Next Steps in Regulating Facial Recognition Technology.” https://www.jtl.columbia.edu/bulletin-blog/europes-next-steps-in-regulating-facial-recognition-technology, retrieved 26.09.22

Li, Stan Z. Ben Schouten, and Massimo Tistarelli, “Biometrics at a Distance: Issues, Challenges, and Prospects” in *Handbook of Remote Biometrics*, Massimo Tistarelli, Rama Chellappa and Stan Z. Li (eds), London: Springer, 2009, pp. 3-21, https://doi.org/10.1007/978-1-84882-385-3_1

Lomas, Natasha, “MEPs call for European AI rules to ban biometric surveillance in public.” *TechCrunch*, 15.04.21, https://techcrunch.com/2021/04/15/meps-call-for-european-ai-rules-to-ban-biometric-surveillance-in-public/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuanRsLmNvbHVtYmlhLmVkdS8&guce_referrer_sig=AQAAAAleXGP0Unr_dRwZrWPFOnm8p09r6vxwooDTNZdwbSMEx41WbKEjvV07KadFgDcVnWmsnlC2QDSuKFbrpN95J6m2GWdBmpsFPy0b_KPheSNmfo0vMLGpRf0GuCJJOQG78SQmQGzngKK9oShzDeHfPhkse9Zw6LW1_9jQ71S3u1, retrieved 26.09.22

Manthorpe, Rowland, and Alexander J Martin, 81% of 'suspects' flagged by Met's police facial recognition technology innocent, independent report says” *Sky News*, 04.07.19, https://news.sky.com/story/met-polices-facial-recognition-tech-has-81-error-rate-independent-report-says-11755941, retrieved 08.11.22

Marr, Bernard. “What Is The Difference Between Artificial Intelligence And Machine Learning?” *Forbes*, 06.12.16, https://www.forbes.com/sites/bernardmarr/2016/12/06/what-is-the-difference-between-artificial-intelligence-and-machine-learning/?sh=6589e2aa2742, retrieved 20.10.22

Norwegian Government, “Forslag til forordning om kunstig intelligens (KI-forordningen).” 12.11.21, https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/juni/forslag-til-forordning-om-kunstig-intelligens-ki-forordningen/id2884935/, retrieved 10.10.22

Pool, R.L.D., and B.H.M. Custers. “The Police Hack Back: Legitimacy, Necessity and Privacy Implications of the next Step in Fighting Cybercrime.” *European Journal of Crime, Criminal Law and Criminal Justice* 25, no. 2 (2017): 123–44. https://doi.org/10.1163/15718174-25022109

Rae, Alasdair, “Europe's most densely populated square kilometres – mapped”, *The Guardian,* 22.04.18, https://www.theguardian.com/cities/gallery/2018/mar/22/most-densely-populated-square-kilometres-europe-mapped, retrieved 10.10.22

Reuters, “Trump Says U.S. to Designate Mexican Drug Cartels as Terrorists.” *Reuters*, 26.11.19. https://www.reuters.com/article/us-usa-mexico-cartels- idUSKBN1Y02NJ, retrieved 16.10.22

Robbins, Scott. “Facial Recognition for Counter-Terrorism: Neither a Ban Nor a Free-for-All” in *Counter-Terrorism, Ethics and Technology — Emerging Challenges at the Frontiers of Counter-Terrorism*, Adam Henschke, Alastair Reed, Scott Robbins and Seumas Miller (eds), 1. Edition, Berlin: Springer, 2021, pp. 89-104, https://doi.org/10.1007/978-3-030-90221-6_6, E-Book

Singh, Neema Guliani and Clare Garvie, “Lawmakers Need to Curb Face Recognition Searches by Police”, 25.10.16, https://www.aclu.org/news/privacy-technology/lawmakers-need-curb-face-recognition-searches, retrieved 20.10.22

Stanley, Jay. “Experts say “emotion detection” lacks scientific foundation.” 18.07.19, https://www.aclufl.org/en/news/experts-say-emotion-recognition-lacks-scientific-foundation#:~:text=Nevertheless%2C%20in%20the%20end%2C%20after,his%20or%20her%20facial%20movements.%E2%80%9D, retrieved 16.10.22.

Symanovich, Steve. “What is facial recognition? How facial recognition works.” 20.08.21, https://us.norton.com/blog/iot/how-facial-recognition-software-works, retrieved 15.09.22

United States Foreign Intelligence Court, “About the Foreign Intelligence Surveillance Court”, NTA, https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court, retrieved 29.09.22

University of Essex by Pete Fussey and Daragh Murray, "*Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition"* Colchester: 2019. https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf

Zenner, Kai. "Documents." https://artificialintelligenceact.eu/documents/, retrieved 24.10.22, Future of Life Institute

6.2 Case-law/Table of Cases

6.2.1 European Court of Human Rights

Beghal v. the United Kingdom (Application no. 4755/16) 28 February 2019

Big Brother Watch and Others v. the United Kingdom (GC) (Applications nos. 58170/13, 62322/14 and 24960/15) 25 May 2021

Catt v. the United Kingdom (Application no. 43514/15) 24 April 2019

Colon v. the Netherlands Application no. 49458/06 15 May 2015

Dakir v. Belgium (Application no. 4619/12) 11 July 2017

Gaughran v. the United Kingdom (Application no. 45245/15) 13 July 2020

Gillan and Quinton v. the United Kingdom (Application no. 4158/05) 28 June 2010

Klass and Others v. Germany, Application no. 5029/71, 6 September 1978,

López Ribalda and Others v. Spain [GC] (Applications nos. 1874/13 and 8567/13) 17 October 2019

Malone v. The United Kingdom, Application no. 8691/79, 2 August 1984,

Murray v. the United Kingdom (GC) (Application no. 14310/88) 28 October 1994

Oliviera v. the Netherlands, (Application no. 33129/96) 06 November 2002

Peck v. The United Kingdom, Application no. 44647/98, 28 April 2003,

Perry v. the United Kingdom (Application no. 63737/00) 17 October 2003

Peruzzo and Martens v. Germany (Applications nos. 7841/08 and 57900/12) 4 June 2013

Roman Zakharov v. Russia (GC) (Application no. 47143/06) 04 December 2015

S. and Marper v. the United Kingdom (GC) (Applications nos. 30562/04 and 30566/04) 04 December 2008

Silver and Others v. the United Kingdom (Application nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75) 24 March 1983

Szabó and Vissy v. Hungary (Application no. 37138/14) 06 June 2016

Uzun v.Germany (Application no. 35623/05) 02 December 2010

Weber and Saravia v. Germany (Application no. 54934/00) 26 June 2006

6.2.2 European Court of Justice

Case C-26/62 *Van Gend en Loos v. Nederlandse Administratie der Belastingen,* 5 February 1963,

Case C-6-64 *Costa v E.N.E.L.* 15 July 1964

Case C-511/18 *La Quadrature du Net and others*, 6 October 2020

6.2.3 Domestic cases

R (on the application of Edward Bridges) v. the Chief Constable of South Wales Police [2020] EWCA Civ 1058, https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

Rt-2005-846 (Uskyldspresumpsjon)

6.3 Table of Treaties

ECHR — Convention for the Protection of Human Rights and Fundamental Freedoms, Rome 4 November 1950.

EU Charter of Fundamental Rights — Charter of Fundamental Rights of the European Union, Lisbon 13 December 2007.

TFEU *Treaty on the Functioning of the European Union*. Consolidated version 2016 (EUT 2016/C 202/01)

TEU *Treaty on European Union.* Consolidated version 2016(EUT 2016/C 202/01)

6.3.1 European Union legislation

6.3.1.1 AI Act

COM(2021) 206 final *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules of Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts* (AI Act — AIA)

2021/0106(COD) ****I DRAFT REPORT on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM2021/0206 – C9-0146/2021 – 2021/0106(COD))*

COD(2022) 13102/22 *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Fourth Presidency compromise text*

2020/2016(INI) *European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*

ANNEXES to the Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts

COD(2021) 8115/20 *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Presidency compromise text*

6.3.1.2 Other EU legislation

Directive 2002/58/EC *of European Parliament and the Council of the European Union Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector* (Directive on privacy and electronic communications)

Directive (EU) 2016/680 *of European Parliament and the Council of the European Union Directive 2016/680/EU of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA* (Law Enforcement Directive — LED)

Regulation (EU) 2016/679 *of European Parliament and of the Council of the European Union of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)* (General Data Protection Regulation — GDPR)

Directive (EU) 2017/541 *of European Parliament and of the Council of the European Union of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA*

6.4 Domestic legislation

Terrorism Act (2000) https://www.legislation.gov.uk/ukpga/2000/11/contents

2005 LOV-2005-05-20-28 The Penal Code (Penal Code)

1995 LOV-1995-08-04-53 The Police Act (The Police Act)

1986 LOV-2022-06-17-59 "Act on the Procedure in Criminal Cases" (Act on the Procedure in Criminal Cases)