Abstract

As facial recognition technology (FRT) proliferates worldwide, a critical question emerges: can surveillance methods designed to maintain public order and safety inadvertently undermine the very fundamental freedoms they seek to safeguard? This psycho-legal analysis investigates how the use of FRT by the Dutch police interacts with the exercise of the core freedoms of expression and peaceful assembly in the context of public protests. Through mixed-method research, the study first conducts doctrinal analyses of normative legal conditions and their evolving judicial interpretations across different levels of governance, ranging from international to national. The legal reviews reveal a troubling reality: there are currently no legally binding, event-specific restrictions imposed on retrospective identification of protesters, creating a regulatory grey zone where accountability remains diffuse. Complementing the legal component, an online vignette-based survey among young adults reveals psychological dimensions and implications of such surveillance used in the Netherlands. After becoming aware of FRT deployment, respondents consistently reported significant deterrence on specific variables relating to both expression and assembly, demonstrating a manifestation of the classic "chilling effect". Against the somewhat dystopian socio-philosophical backdrop of Foucault's disciplinary notion of the Panopticon, the perceived visibility through FRT surveillance potentially constraining behaviour is particularly concerning. The findings illuminate a paradox at the heart of modern democracy: technologies utilised by law enforcement authorities may erode crucial participatory foundations. This thesis offers policy recommendations, such as harmonised statutory safeguards, ex-ante rights impact assessments, and independent oversight, aiming to protect the right to protest in the digital age.

Key words: facial recognition technology, freedom of expression, freedom of assembly, protest surveillance, chilling effect, law enforcement, regulation, biometric data, privacy

"Visibility is a trap."

— Michel Foucault, *Discipline & Punish* (1977)

Table of Contents

List of Abbreviations

AIA	Artificial Intelligence Act (2025)
AP	Autoriteit Persoonsgegevens (the Dutch Data Protection Authority)
BIS	Biometric Identification System
CATCH	Centrale Automatische TeChnologie voor Herkenning (the Dutch FRT)
CCTV	Closed-Circuit Television
CJEU	Court of Justice of the European Union
CFREU	Charter of Fundamental Rights of the European Union (2000)
CoE	Council of Europe
DCtTH	District Court of The Hague
DPIA	Data Protection Impact Assessment
ECHR	European Convention on Human Rights (1950)
ECtHR	European Court of Human Rights
FRT	Facial Recognition Technology
FRIA	Fundamental Rights Impact Assessment
GDPR	General Data Protection Regulation (2016)
GEB	Gegevensbeschermingseffectbeoordeling (the Dutch DPIA)
Gw	Grondwet (the Dutch Constitution, 2023)
ICCPR	International Covenant on Civil and Political Rights (1966)
IRAC	Issue-Rule-Application-Conclusion
LED	Law Enforcement Directive (2016)
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming (the Dutch implementation act of the GDPR, 2021)
UDHR	Universal Declaration of Human Rights (1948)
Wpg	Wet politiegegevens (the Dutch Police Data Act, 2024)

The Right to Protest in the Panoptic Reality

In March 2025, Extinction Rebellion initiated summary proceedings against the Dutch police after an activist affiliated with the climate action group was questioned at her doorstep about her involvement in specific demonstrations (NOS, 2025). It was a direct consequence of the collection and processing of her personal data without any prior notice or formal suspicion. This occurrence was not a one-off incident; it reflects an ongoing trend of unannounced home visits to peaceful protesters, who have repeatedly reported feeling intentionally intimidated and watched (Amnesty International, 2023). While policies governing such practices are lacking, leaving their rationale and justification opaque, the regional chief of police asserted that their purpose is not to deter anyone from participating in anything. According to the presiding judge, this case raises a fundamental issue: the friction between the constitutional right to demonstrate and the core duty of the police to maintain public order (Huisman, 2025).

This tension becomes more pronounced in light of the rapid technological advancement of mass surveillance methods, which are increasingly utilised during demonstrations worldwide (Privacy International, 2025). Closed-Circuit Television (CCTV) footage, often supplemented by body cameras and drones, can nowadays be linked to artificial intelligence (AI) systems capable of identifying individuals by analysing biometric data, meaning the unique physical, physiological, or behavioural characteristics of a person, such as fingerprints or DNA (Smith & Mann, 2024, pp. 87-88). When such biometric identification systems (BIS) involve facial image processing algorithms, it is referred to as facial recognition technology (FRT).

Within the field of biometric surveillance, FRT represents the latest and the greatest. In the Netherlands, it is increasingly deployed through a database called ‘Centrale Automatische TeChnologie voor Herkenning’ (CATCH), due to evident growing effectiveness in identifying unknown suspects during criminal investigations (Politie, 2024). To illustrate, its usage rose by 54% from 2022 to 2023, and the success rate of identifications surged from approximately 11%

to around 41% (Politie, 2023). Furthermore, Dutch law enforcement authorities have access to a database containing over 338,000 surveillance cameras across nearly 75,000 locations in the Netherlands (Aanhangsel Handelingen I, 2024/2025, nr. 748). Against the socio-psychological backdrop of Foucault's (1977) Panopticon and Orwell's (1949) Big Brother, one might question whether this results in an enhanced feeling and perhaps fear of being watched.

When used in protest settings, where anonymity may be essential for the full realisation of the right to demonstrate, the use of FRT raises serious concerns about its potential chilling effect on civic participation (Matulionyte, 2024, p. 61). The Dutch police can deploy various identification methods in the context of protests. In addition to ID checks *during* assemblies, videos and online activities may also be investigated *after* events. Such data-driven policing has previously been scrutinised for risks related to privacy violations, discriminatory outcomes, and lack of transparency (De Hert & Lammerant, 2016, p. 167; Lágana, 2022). Out of fear of being identified and potential repercussions, protesters have expressed feelings of deterrence from exercising their protest-related rights (Amnesty International, 2024, p. 27).

These issues are exacerbated by the absence of regulations governing the use of FRT (Gabrielli, 2025, p. 22). The EU's newly adopted AI Act (2025) constitutes the first piece of legislation to include specific provisions on BIS. While it prohibits *real-time* (i.e., live) usage, *post-remote* (i.e., retroactive) application is still relatively unregulated. National legislative acts also remain absent, and existing frameworks are considered to provide insufficient protection (Galič & Stevens, 2023, p. 477; Hu & Kouwenberg, 2023, p. 3). This legislative gap is particularly concerning when taking the psychological effects of biometric surveillance into account. Therefore, this thesis aims to critically examine the conditions and consequences of the Dutch police using FRT in the context of protests. An extensive legal and psychological analysis will reveal that current frameworks remain ambiguous and inadequate, resulting in a regulatory grey area and a lack of legal safeguards that require urgent attention.

Societal Relevance

The anarchist 'Provo' happenings in the mid-1960s and the anti-nuclear marches during the Cold War illustrate how deeply embedded public protest is in Dutch socio-political culture (Van Diepen, 2004, pp. 215-218; Hietland, 2016, p. 433). Recently, farmer tractor blockades, climate-justice actions, and university encampments have demonstrated that collective dissent remains a mainstream channel for renegotiating the social contract (Verloo, 2020, pp. 84-85). In the context of this long-standing tradition of demonstrations in the Netherlands, it is therefore paramount that this social practice remains free, safe, and accessible for everyone.

Recent civil surveys indicate that nearly 60% of the Dutch population feels politics does not protect people like them (SCP, 2024, p. 37), reinforcing the importance of public dissent. Furthermore, the Digital Decade Eurobarometer revealed that 85% of Dutch respondents want public authorities to ensure AI systems respect their rights and values (EC, 2024, p. 44).

When protesting is associated with surveillance and intimidation, it risks normalising the suppression of dissent and fostering a climate of fear and self-censorship, raising serious concerns about rule of law backsliding (Pech, 2021, p. 19). Therefore, this thesis seeks to raise public awareness and inform societal debates on data-driven policing, biometric surveillance, and legal safeguards necessary to protect the true Dutch democratic identity.

Academic Relevance

Despite its increasing deployment and broad public concern, the use of FRT by Dutch law enforcement remains not only underregulated but also relatively underexplored. Amnesty International (2024) provided the first detailed report on FRT in the context of Dutch protests; Galič and Stevens (2023) have underscored the fragmentation of existing Dutch frameworks while emphasising regulatory gaps and a lack of coherent oversight; and Storbeck et al. (2025) have examined the psychological effects of surveillance on activists in the Netherlands.

However, in the literature review, no studies were found that assessed the interaction between the use of FRT by Dutch law enforcement and public protest participation. In addition to analysing the regulatory grey zone, this thesis addresses this academic gap by exploring the socio-psychological effects of FRT on the exercise of the rights to freedom of expression and assembly. It adds to emerging research at the intersection of law, technology, and psychology, contributing to scholarly debates on protest governance, democratic resilience, and biometric surveillance. Findings are relevant for scholars, policymakers, organisations, and authorities seeking to develop comprehensive frameworks for regulating FRT deployment.

Interdisciplinarity

While doctrinal research may elucidate existing black-letter standards and normative frameworks, it cannot capture behavioural or psychological consequences. This limitation is addressed by integrating socio-psychological theory and a quantitative empirical survey, which will reveal how FRT may affect individual attitudes toward protest-related rights and freedoms. However, while social science may help explain public perceptions and decision-making, it cannot provide concrete suggestions on how to address the regulatory gap precisely.

Therefore, this thesis employs a psycho-legal mixed-methods research design, allowing for a normative-empirical inquiry into the interaction between FRT and fundamental freedoms. It aims to yield a comprehensive understanding and evaluation of the complex issues and their implications at hand. Doctrinal analyses clarify the legal conditions and judicial interpretations of FRT; socio-psychological theory aids in explaining behavioural intentions and institutional trust; empirical findings offer a systematic examination of how it may affect individual attitudes towards exercising freedom of expression and assembly. This combination of interdisciplinary insights is believed to not only enhance the analysis of the impact of FRT but also guide the development of more effective, responsive, and rights-oriented regulation.

Research Questions

Considering the gaps and issues outlined, this thesis will explore the research question: *How does the use of facial recognition technology (FRT) by the Dutch police interact with the fundamental rights to freedom of expression and assembly in the context of protests?*

To formulate a substantive answer, the following sub-questions will be investigated:

(I) *Under what legal conditions is the use of FRT by the Dutch police permitted?*

(II) *How have judicial interpretations of these legal conditions evolved?*

(III) *How does awareness of the use of FRT by the Dutch police affect individual attitudes towards exercising freedom of expression and assembly?*

Hypotheses

To answer the third sub-question, and drawing on the socio-psychological concepts outlined in the Theoretical Framework, the following hypotheses will be tested:

Table 1

Hypotheses Sub-Question III

Code	Null hypothesis H_0	Alternative hypothesis H_a
H1	$\mu_\Delta = 0$ Awareness of the use of FRT **does not affect** attitudes towards exercising freedom of **expression**.	$\mu_\Delta \neq 0$ Awareness of the use of FRT **does affect** attitudes towards exercising freedom of **expression**.
H2	$\mu_\Delta = 0$ Awareness of the use of FRT **does not affect** attitudes towards exercising freedom of **assembly**.	$\mu_\Delta \neq 0$ Awareness of the use of FRT **does affect** attitudes towards exercising freedom of **assembly**.

Note. μ_Δ = mean change in self-reported attitudes before and after reading survey vignettes.

Theoretical Framework

This section will outline the relevant legal and socio-psychological concepts, which will serve as the analytical lenses through which the case study will be interpreted. Drawing on vast literature, it presents multiple perspectives on the main concepts of this thesis.

Legal Concepts

The following legal concepts are elucidated through a doctrinal analysis of relevant legal instruments and scholarship. These vary in scope, covering international, regional, and national contexts, and binding nature, distinguishing between hard and soft law. Tables 4 and 5 provide comparative overviews of the legal instruments and frameworks discussed in this section.

Noteworthy, the Netherlands adheres to a monist legal tradition as stipulated by Articles 93 and 94 of the Constitution (Besselink, 2022, p. 406). This means that ratified international treaties automatically gain binding force in the domestic legal order and may take precedence over conflicting national legislation (Bovend'Eert, 2021, p. 408).

Fundamental Rights

In the history of human rights, the Universal Declaration of Human Rights (UNGA, 1948) is the most prominent document (Hunt, 2007, p. 205). Articles 12, 19, and 20(1) outline the rights to privacy, freedom of expression, and freedom of assembly, respectively. Although not classed as a legally binding document, the UDHR has served as a key source of inspiration for many other treaties (Charlesworth, 2008, para. 13). The International Convention on Civil and Political Rights (ICCPR, 1966), for instance, which protects the rights to privacy, freedom of expression, and assembly in Articles 17, 19, and 21, respectively. The UN Guiding Principles (UNGPs) have established the duty of states to safeguard human rights (UN, 2011, p. 1), which has been deemed crucial for adequate AI regulation (Beduschi & Ebert, 2021, p. 15).

Furthermore, the European Convention on Human Rights (ECHR, 1950), established by the Council of Europe (CoE), offers an advanced regional framework for the protection of fundamental rights and freedoms (Frowein, 2009, para. 17). Articles 8, 10, and 11 delineate the rights to privacy, freedom of expression, and freedom of assembly, respectively. Additionally, the European Union (EU) developed its own Charter of Fundamental Rights (CFREU, 2000). Its provisions on privacy, expression, and assembly in Articles 7, 11, and 12, respectively, are clearly equivalent to the ECHR (Lynskey, 2015, p. 47). However, unlike the ECHR, the CFREU establishes the protection of personal data as a robust and distinct right under Article 8, directly underpinning highly important data protection principles (Hijmans, 2016, p. 17).

The Dutch Constitution (Grondwet, Gw, 2023) enshrines rights to privacy, expression, and assembly under Articles 10, 9, and 7(3), respectively. Similar to the CFREU, it explicitly mentions rules regarding the "recording and dissemination of personal data" (Article 10 Gw). The Dutch Public Assemblies Act (Wet openbare manifestaties, 2010) regulates the exercise of assembly, translating it into a liberal notification-rather-than-authorisation regime (Swart & Roorda, 2023, p. 36). Under Article 1(1) of the Act, 'public' refers to "a place open to the public by virtue of destination or fixed use". Although 'assembly' is not defined, it can be contextually interpreted as equivalent to 'protest' or 'demonstration', defined in Dutch as "expressions of resistance" (Van Dale, 2025). These terms will be used interchangeably throughout this thesis.

Data Protection

The first internationally agreed-upon set of principles regarding privacy was developed by the Organisation for Economic Co-operation and Development (OECD) in 1980. Another relevant international instrument is Convention 108 (1981), providing the first legally binding conditions in the field of the individual protection of privacy and personal data (CoE, 2022). Its modernised version, Convention 108+ (2018), reinforces rights concerning personal data by

offering a human rights-based framework for assessing the legitimacy and proportionality of deploying technologies in data processing settings (De Terwangne, 2021, p. 3).

Regional frameworks further shape the relevant regulatory landscape. The General Data Protection Regulation (GDPR, 2016) is the world's strictest privacy and security legislation, encompassing requirements for data collection from individuals within the EU (Wolford, 2025). Its adoption provided a comprehensive replacement for the 1995 Data Protection Directive and marked a transition from harmonisation to uniformity in data protection (Bygrave, 2014, p. 20). It implements a risk-based approach, using risk as a tool to prioritise and target enforcement actions in a manner proportionate to the actual hazard caused (Quelle, 2018, p. 512).

In Article 5, the GDPR enumerates the core data protection principles paramount to any type of data processing (De Hert & Papakonstantinou, 2016, p. 185). It further establishes the Data Protection Impact Assessment (DPIA) in Article 35, discussed in the Doctrinal Analysis. The 'Uitvoeringswet Algemene verordening gegevensbescherming' (UAVG, 2021) is the Dutch implementation act of the GDPR. Compliance is monitored by the Dutch Data Protection Authority (Autoriteit Persoonsgegevens, AP, 2024), which recently reinforced its firm stance regarding facial recognition by imposing a fine of 30.5 million euros on the American company Clearview AI following its illegal data collection of facial images from Dutch citizens.

Article 4(14) GDPR defines 'biometric data' as "personal data resulting from specific technical processing relating to physical, physiological or behavioural characteristics" allowing or confirming one's "unique identification". Articles 9(1) GDPR and 22(1) UAVG prohibit the processing of special personal data categories, including biometric data. The GDPR stipulates derogations if "necessary for reasons of substantial public interest, on the basis of […] law […] proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard […] fundamental rights" (Article 9(2)(g)). In the UAVG: only when "necessary for authentication or security purposes" (Article 29).

According to Article 2(2)(d) and Recital 19 GDPR, data processing by law enforcement generally falls outside its scope. However, it remains relevant in contexts where the processing purposes are unclear. The Law Enforcement Directive (LED, 2016) is adopted in parallel with the GDPR and concerns law enforcement data processing. Unlike the GDPR, it is a Directive, not a Regulation, necessitating transposition into national legislation to take effect (Best, 2022, p. 237). In the Netherlands, this is the Police Data Act (Wet politiegegevens, Wpg, 2024) and the Judicial Data and Criminal Records Act (Wet justitiële en strafvordelijke gegevens, 2024). The former is discussed in the Doctrinal Analysis; the latter is not relevant to this study as it pertains to the judiciary, whose data processing falls outside this research scope.

Biometric Identification

The AI Act (AIA, 2025) is the first comprehensive framework regulating AI (Gabrielli, 2025, p. 3). The EU sought to regulate this innovative technology to enhance the conditions for its advancement and application (Directorate General for Communication of the EP, 2025). This is achieved through three main pillars: a solid reliance on the GDPR, an ethical dimension, and a renewed focus on fundamental rights (Mantelero, 2024, p. 3). The latter is, for instance, shown by the introduction of the Fundamental Rights Impact Assessment (FRIA) requirement under Article 27 AIA, a variation of and addition to the aforementioned DPIA.

Similar to the GDPR, the AIA ‘calibrates’ concrete risk scores, aiming for compliance that respects fundamental rights. It establishes distinct rules for varying risk levels, classified as unacceptable, high, limited, and minimal (Future of Life Institute, 2025). The first two are particularly relevant to this study. AI systems that fall under the highest category are regarded as direct violations of fundamental rights and are therefore considered ‘unacceptable’ and, in principle, prohibited (Article 5). AI systems impacting health, safety, or fundamental rights are categorised in the second tier, ‘high risk’, and are subject to strict scrutiny (Article 6).

Article 3(35) defines 'biometric identification' as "automated recognition" of specific human features to establish one's identity "by comparing biometric data to […] biometric data […] stored in a database". This is often achieved through remote BIS, "typically at a distance" and "without [the person's] active involvement" (Article 3(41)). It distinguishes '*real-time* remote', with all steps occurring "without significant delay", resulting in "instant identification" and "limited short delays in order to avoid circumvention" (Article 3(42)), from '*post*-remote', encompassing all other remote BIS (Article 3(43)). In FRT, the latter refers to the retrospective identification by matching facial images to reference databases (Christakis et al., 2022, p. 6). The former are prohibited "in publicly accessible spaces for the purposes of law enforcement" (Article 5(1)(h)), the latter are classified as high-risk (Article 6 & Annex III).

While the AIA is the only binding instrument in the Netherlands that explicitly mentions it, several soft laws address FRT. As mandated by a Human Rights Council Resolution (2023), the UN (2024) recently published a 'toolkit for law enforcement officials to promote and protect human rights in the context of peaceful protests'. At the regional level, the CoE (2021) adopted guidelines drafted by the Committee of Convention 108, and, following an EU Resolution (2021), the European Data Protection Board (EDPB, 2022) established guidelines for its use by law enforcement authorities. Nationally, the AP (2024) established a legal framework, and the police formulated a deployment framework, providing guidance for assessing FRT use cases, requiring police units to conduct their own evaluations regarding its proportionality and necessity (Politie, 2024). However, as will be elaborated in the Doctrinal Analysis, this internal decision-making has been scrutinised by scholars (Galič & Stevens, 2023, p. 467).

Regulatory Gap

Alarming messages regarding the use of FRT, particularly in more authoritarian regimes such as China, Russia, and Iran, and especially during demonstrations, have been raised for

years (Rest of World, 2024; Privacy International, 2025). In Europe, similar concerns have been raised, illustrated by the discourse surrounding Hungary's anti-Pride law, permitting FRT usage during Pride marches (Amnesty International, 2025). Recently, in the Netherlands, FRT was employed by law enforcement authorities to arrest climate protesters at Schiphol Airport. The Dutch Public Prosecution Service scrutinised this practice due to its carelessness and lack of verifiability, leading to data deletion and procedural revisions (OM, 2024).

European research reports have indicated that biometric surveillance tools, such as FRT, have advanced more rapidly than their corresponding regulatory frameworks have evolved (FRA, 2019; EDRi, 2021; EPRS, 2021; WEF, 2022; ALI, 2025). Furthermore, the issued guidelines addressing FRT lack legally binding authority and are often not considered to impose the meaningful constraints needed (Canova & Simmler, 2024, p. 10). Existing regulations are further consistently criticised for adopting a fragmented and reactive approach that overlooks long-term sociotechnical impacts (Urquhart & Miranda, 2021, pp. 217), for failing to ensure or establish effective oversight and accountability mechanisms (Gabrielli, 2025, p. 18), and for insufficiently safeguarding the fundamental rights and freedoms impacted by FRT deployment (Lynch, 2024, p. 4), culminating in urgent concerns regarding the erosion of civil liberties and democratic values caused by unchecked FRT use (Smith & Miller, 2021, p. 171).

Individual citizens and non-profit organisations in the Netherlands have also highlighted this lack of regulation and transparency. In early 2024, following concerns raised by Dutch investigative journalists, the Minister of Justice and Security, Dilan Yesilgöz, was questioned for the first time about the legislative gap concerning the use of FRT by Dutch law enforcement authorities (Aanhangsel Handelingen I, 2023/2024, nr. 982; Schrader et al., 2024). Other alarm bells regarding the far-reaching consequences of this mass surveillance technology have been sounded by Bits of Freedom (2019), a Dutch organisation advocating for citizens' digital rights, resulting in the AP formulating its general legal framework (Houwing, 2024).

Socio-Psychological Concepts

The following socio-psychological concepts are explained through a literature review of corresponding theories, empirical studies, and other scholarship. The first two sub-sections describe classic constructs; the other two concern more recent FRT-related research.

The Panopticon

Foucault's (1977) perspective on the Panopticon provides a foundational metaphor for understanding surveillance as a disciplinary mechanism: power operates through internalisation of visibility; individuals regulate behaviour under the assumption of being watched (p. 201). It may be questioned whether identification through FRT use could have a similar deterrent effect. While originating in closed institutions such as prisons, scholars have since extended this logic to open, everyday settings, where this notion has been theorised to be salient too.

Mitchell (1995, p. 116), for instance, contends public space is not inherently democratic or inclusive but produced through political contestation over who is permitted to appear, speak, and dissent. In this light, surveillance is considered to erode democratic participation, especially among marginalised communities (p. 117). FRT use in protest contexts may then perhaps also undermine the ability of individuals to express their views freely in public.

Contemporary surveillance arguably exceeds the logic of the Panopticon. In this regard, Haggerty and Ericson (2000, p. 608) introduced the "surveillance assemblage", which refers to fragmented data collection systems that converge to create fluid, decentralised networks of observation. People thus not only risk being constantly monitored in real life but also flagged across interconnected databases online, enhancing a sense of imminent traceability.

Rather than treating surveillance as a neutral tool of governance, these theories consider how it might actively condition behaviour and the democratic function of the public space. This sociological lens forms a critical backdrop for examining potential chilling effects.

The Chilling Effect

In his legal scholarship, Schauer (1978, p. 689) conceptualised the "chilling effect" as refraining from lawful expression or association due to fear of potential consequences, such as sanctions, scrutiny or retaliation, even when these are uncertain or unlikely. He claimed vague legislation can create a climate in which people voluntarily censor themselves, "chilling" their exercise of constitutional freedoms (p. 699). Nowadays, this notion is often tied to the deterring effects of surveillance technologies: When protesters believe they might be identified and penalised, the prospect of visibility alone may be enough to inhibit action.

The Theory of Planned Behaviour provides a useful lens for analysing this behavioural change. According to Ajzen (1991, p. 182), behaviour is shaped by intention, which in turn is influenced by attitudes, norms, and perceived behavioural control. FRT might negatively affect all components: it may foster negative attitudes by increasing perceived risks, shift norms by creating social pressure to abstain, and lower perceived behavioural control by reducing sense of safety and agency; potentially leading to less intention to participate in protests.

Slovic's (1987, p. 285) Risk Perception Theory further states that risk assessments may shape individual decision-making processes, suggesting that behaviour results from rational cost-benefit analyses and emotional responses. These appraisals converge in Dinev and Hart's (2006, p. 15) version of the "privacy calculus", framing behaviour as a subjective evaluation of perceived risks and benefits. Interestingly, institutional trust is not only a well-established factor in these perceptions but has also been found to be crucial in explaining why individuals comply with the law in general (Tyler, 2006, p. 172). Building on this logic, one might question how awareness of FRT affects decisions to participate in peaceful assemblies.

Rather than presuming surveillance inevitably chills protest participation, these theories highlight the conditional nature of its potential effects. This psychological lens underscores the importance of understanding how FRT impacts individual behavioural processes.

General Perceptions

Empirical research has demonstrated that public acceptance of FRT depends on context and significant psychological drivers. Concerns regarding crime, trust in procedural fairness, and perceived normative alignment collectively enhance support for police use of live FRT, with legitimacy acting as a mediating factor (Bradford et al., 2020, p. 14). Scenario experiments indicate that familiarity and trust in FRT are highest for private authentication and routine public surveillance but lowest for medical applications (Lai & Rau, 2021, p. 7).

Cross-national surveys suggest that FRT acceptance reflects confidence in government and prevalent privacy and security norms; however, preference falsification may obscure opposition in authoritarian settings (Kostka et al., 2023, p. 4). Perceptions are also context-dependent regarding venues: people tend to trust FRT more in schools and hospitals than in open public spaces policed by law enforcement agencies (Choung et al., 2024, p. 6).

Overall attitudes embody a trade-off in which familiarity with technology enhances expected benefits, while concerns about privacy intensify perceived harms (Mesch & Lam, 2024, p. 9). Large-scale polling continues to reveal substantial support for policing applications, moderated by concerns regarding privacy and safety (Miethe et al., 2025, p. 1033).

Taken together, these findings suggest that public endorsement of FRT is conditional, depending on a dynamic interplay of contextual benefits, perceived legitimacy, and privacy trade-offs, rather than indicating uniform or unconditional approval.

Protest Surveillance

Numerous studies have consistently shown that surveillance technologies shape civic behaviour and attitudes in complex, often restrictive ways. Interviews with activists reveal that camera surveillance and protest policing are perceived through various ideological lenses; nonetheless, they are generally regarded as instruments that reshape repertoires of collective

action (Ullrich & Knopp, 2019, p. 188). Rights-based scholarship highlights that surveillance chills expression and assembly, eroding conditions for participatory democracy (Murray et al., 2024, p. 405). Recent Dutch research identified two new manifestations of the chilling effect restraining activists: hyper-transparency and hyper-alertness (Storbeck et al., 2025, p. 4).

The psychological consequences of protest surveillance in the Netherlands are further well-documented by two reports from Amnesty International (2023, 2024). They specifically investigated the use of surveillance tools, such as ID scans and live cameras, by the Dutch police during peaceful assemblies. Their research demonstrates that this not only directly interferes with protest-related rights and freedoms but may also discourage citizens from exercising them (2023, p. 5). Notably, FRT deployment was found to exacerbate this chilling effect; individuals expressed fear about the potential repercussions of being identified (2024, pp. 26-27).

Taken together, these findings illustrate that ever-expanding surveillance infrastructures may generate chilling effects that reshape both individual behaviour and collective action, conditioning risk perceptions on civic participation and legitimacy notions.

Methodology

Legal

The first two sub-questions are addressed through qualitative doctrinal legal research, entailing systematic analysis of legal standards, normative frameworks, and case law. It enables legal scholars to construct coherent interpretations of the law from within the legal system itself (Smits, 2017, p. 210). Its strength lies in its capacity to produce precise and transparent legal doctrine that promotes justice and to provide a solid, dependable structure for legal principles, particularly where law remains silent or ambiguous (Bhat, 2020, pp. 167). Given the regulatory gap surrounding FRT use by Dutch law enforcement in protest settings, this method is deemed appropriate to substantiate the legal dimension of the main research question.

First, the legal conditions under which Dutch law enforcement may use FRT in protest contexts will be examined through a comparative analysis of human rights and data protection frameworks across different levels. Findings are organised on three themes (rights interference, biometric data processing, and post-remote biometric identification) and mainly based on seven primary legal sources (the ICCPR, ECHR, CFREU, Gw, LED, Wpg, and AIA).

Second, the judicial interpretations of these requirements will be assessed by exploring case law from three different bodies: the European Court of Human Rights (ECtHR), the Court of Justice of the EU (CJEU), and the District Court of The Hague (DCtTH). This jurisprudence serves as important legal precedents and as an interpretative layer in normatively assessing whether current legal safeguards provide sufficient and adequate protection against FRT. The Issue-Rule-Application-Conclusion (IRAC) method was used (Holland & Webb, 2019, p. 114). Legal scholarship and soft law supplement and contextualise these analyses. All sources were selected on legal authority and relevance to data protection and human rights.

Psychological

The third sub-question is investigated through quantitative empirical survey research complemented by an interpretation of the concepts outlined in the Theoretical Framework. This approach is appropriate for studying attitudinal shifts and is widely used to analyse individual perceptions and self-reported behavioural intentions (Schutt, 2020, p. 388).

Findings will help explain how awareness of the use of FRT by the Dutch police affects general perceptions of FRT usage, attitudes toward exercising freedom of expression and assembly, and institutional trust in general. The socio-psychological concepts outlined in the Theoretical Framework will serve as guidance in interpreting the results in the Discussion. This combined analytical approach will substantiate the psychological dimension of this thesis. The following paragraphs provide a detailed description of the methods used.

Participants

The survey was conducted between May 12 and June 1, 2025, and distributed to Dutch citizens through online social media platforms. It used voluntary and anonymous participation with informed consent. The sampling aimed to capture a heterogeneous sample reflecting varied protest experiences. Prior to the recruitment, approval was obtained from the Ethics Review Board of the University of Amsterdam. No identifiable data was collected, no compensation was provided to participants, and storage protocols align with GDPR standards.

The participants included 85 young adults between the ages of 20 and 27 (M = 21.49, SD = 2.67). The sample was predominantly female (66, 77.6%), with eighteen males (21.2%) and one participant (1.2%) preferring not to disclose their gender. A slight majority was born in the Netherlands (48/85, 56.5%), with most living there for over ten years (49/85, 57.6%). Table 6 provides an overview of the Survey Cohort Descriptives. Of the 110 individuals who provided informed consent to participate, 86 (78.2%) completed all items. One respondent was removed as he was not born, did not reside at the time of the survey, and had not participated in a protest in the Netherlands. An a priori power analysis in *G*power 3.1 (two-tailed, d = .35, α = .05) indicated N = 80 for 80% power; the sample (N = 85) satisfied this criterion.

Materials

The following four variables were used to measure attitude changes toward exercising freedoms of expression and assembly before and after reading a vignette about the use of FRT based on Likert-scale items: willingness, likelihood, perceived safety, and perceived capability. The vignette consisted of two informational passages about the number of surveillance cameras and the potential for biometric identification, as well as the use of such FRT by the Dutch police. Furthermore, other Likert-scale questions captured general perceptions toward FRT use and institutional trust. Additionally, a slider-scale item was used to state political orientation, and

one open-ended question allowed for elaboration of specific thoughts and concerns regarding the use of FRT in the Netherlands. The full survey can be found in Appendix A.

Given the brief survey length and to minimise fatigue, the attitude constructs were assessed with single items (Wanous et al., 1997, p. 247). All five-point Likert items were recoded to numeric values from –2 (“strongly disagree”) to +2 (“strongly agree”), the attitude-change items from –2 (“extremely negative”) to +2 (“extremely positive”), and the political orientation item from 0 (left-wing) to 100 (right-wing).

Procedure

All participants were told the survey concerned general public perceptions of protest participation in the Netherlands and would take a maximum of ten minutes. The self-designed survey was administered using Qualtrics (https://www.qualtrics.com). Its design entailed both experimental, i.e., confirmatory, and descriptive, i.e., exploratory, features. All participants were presented with the same custom fixed-item ordered questions and vignettes.

Analysis

All analyses were conducted in *R* 4.4.0 (R Core Team, 2025) using the tidyverse 2.0.0 and effect size 0.8.6 packages. Two-tailed one-sample *t*-tests ($\alpha = .05$, $df = 84$) compared the mean change in the attitude variables per fundamental freedom to zero. Effect sizes are reported as Cohen’s *d* with 95 % CIs. All difference scores were screened for univariate normality and assessed via Shapiro-Wilk tests (all $p > .06$). Results were robust in Wilcoxon signed-rank tests. To control family-wise error, the Bonferroni-adjusted significance ($\alpha = .00625$) was applied. Descriptive statistics summarised responses, and thematic coding revealed recurring patterns in open-ended responses (Braun & Clarke, 2006, p. 16). Various tables and figures presenting the results of the analyses will be referenced throughout the Empirical Analysis.

Doctrinal Analysis

This section will provide the doctrinal analyses conducted to answer the first two sub-questions of this research. First, the legal conditions for three relevant topics will be explained. Second, their judicial interpretation by various types of courts will be explored.

Legal Conditions

Based on the concepts outlined in the Theoretical Framework, the following subsections expound on the specific legal conditions regarding fundamental rights interference, biometric data processing in general, and post-remote biometric identification. The organisation is based on governance level, progressing from international to regional to national.

Fundamental Rights Interference

Although certain rights may be fundamental, they are not necessarily absolute, resulting in subjection to certain restrictions only allowed under narrowly defined legal conditions. The legally binding instruments on fundamental rights outlined in the Theoretical Framework (i.e., ICCPR, ECHR, CFREU, and Gw) will be comparatively analysed on such interferences.

While the ICCPR does not state any specific derogation from the right to privacy, Article 17(2) does provide "the right to the protection […] against […] interference or attacks" on it. Furthermore, Article 19(3) ICCPR stipulates freedom of expression implies "special duties and responsibilities" and thus may be "subject to certain restrictions" if "provided by law and […] necessary: (a) for respect of the rights or reputations of others; (b) for the protection of national security or of public order, or of public health or morals". This derogation provision has been found particularly important for state obligations in the field of digital surveillance (Chubb & Lyer, 2024, pp. 779). Article 21 ICCPR imposes the same exceptions for peaceful assembly, notably adding the words "in a democratic society" in the necessity requirement.

In the ECHR, the following is found in all three limitation clauses: “prescribed by” or “in accordance with” law and “necessary in a democratic society”. Furthermore, each one refers to certain general interests, similar to the ICCPR, with some articles specifying additional ones. Any interference must thus comply with principles of legality, necessity, and proportionality. These three doctrines have been deemed a true testament to the ECtHR’s indirect utilitarianist approach to the interference of fundamental ECHR rights (Letwin, 2023, p. 22).

Article 52 CFREU stipulates a limitation triplet similar to the ECHR regarding “general interest recognised by the Union or the need to protect the rights and freedoms of others”, while recognising other EU treaties, the ECHR, and national constitutional traditions. This provision is found pivotal in introducing a methodology for the CJEU, though it is considered evolving due to a lack of sufficient coherence (Petursson, 2025, p. 251). Thus, the CFREU imposes no specific derogations on privacy, expression, or assembly. Regarding personal data processing, Article 8(2) CFREU mentions that “must be [….] fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law” and that individuals have both a right of access and rectification to data collected on them.

The limitation clauses for the fundamental freedoms found in the Gw are formulated as “without prejudice to” either “responsibility […] under the law” or “restrictions laid down by or pursuant to Act of Parliament”. No specific derogation is formulated for the right to privacy. However, in addition to its provision on the protection of personal data, Article 10(3) Gw states that “the law lays down rules on the rights of persons to access data recorded about them and the use made of such data, as well as to correct such data”. The rise of tech, big data, and AI raises the imminent question of whether the current Gw still provides sufficient safeguards to protect Dutch constitutional rights. Recently, at the request of the Ministry of Home Affairs and Kingdom Relations, twelve legal scholars wrote pleas on possible amendments for the Gw in the digital age, based on their vision of the future legal landscape (BZK, 2024).

Biometric Data Processing

Law Enforcement Directive (LED)

Article 8(1) LED stipulates that the processing of personal data is only lawful "if […] necessary for the performance of a task carried out by a competent authority" for purposes of "prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding [of] public security" (Article 1(1)). However, this provision is not deemed to address the strict 'legitimacy' requirement as set out in Article 8(2) CFREU (Brewczyńska, 2023, p. 122).

The 'special categories of personal data' are equivalent to those in the GDPR until the point where Article 9(1) GDPR states "shall be prohibited" and LED Article 10 states "shall be allowed only where". It further stipulates that such processing must be: "strictly necessary, subject to appropriate safeguards […], and only: (a) where authorised by […] law; (b) to protect […] vital interests […]; or (c) where [it] relates to data […] manifestly made public". An EU Working Party (2017, p. 10) stressed the need for a narrow interpretation of the last one, which has also previously been scrutinised in terms of investigative genetic genealogy purposes (Kuru, 2025, p. 1).

Moreover, Article 27 LED requires a prior 'Data Protection Impact Assessment' (DPIA) when "in particular, using new technologies, and taking into account the nature, scope, context, and purposes" of such processing is likely to pose high risks to individual rights and freedoms. Building on this, Article 28 specifies further conditions regarding prior consultation with supervisory data protection authorities if a high risk is indeed established. A case study of a Dutch big-data forensic platform has shown not only the importance of conducting DPIAs before deploying such technologies, but also common pitfalls in light of the specific nature of privacy risks in law enforcement and the need to create specific DPIA methodologies (Seyyar & Geradts, 2020, p. 7).

Wet politiegegevens (Wpg)

As stated in the Theoretical Framework, the Wpg is the Dutch transposition of the LED; both have been scrutinised for various conceptual issues (Custers & Leiser, 2019, p. 10). For instance, the Wpg provides a legal basis for automated data analysis, deemed problematic when used for investigative purposes (Brinkhoff, 2017, p. 68) and lacking transparent regulation in this regard (Te Molder et al., 2023, p. 116).

The Dutch DPIA (gegevensbeschermingseffectbeoordeling, GEB) obligations in Article 4(c) Wpg are identical to those in the LED. However, the Wpg limits these to police data and does not state other regulations or detailed implementation guidelines, leaving their practical operationalisation to internal police and AP oversight.

Although the special data categories are the same as in the GDPR and the LED, the requirements regarding their processing differ slightly. Article 5 Wpg stipulates that processing of such data "shall take place only where […] unavoidable […], in addition to the processing of other police data […] and the data are adequately secured".

The legal conditions in the Wpg are subtly but significantly stricter than those in the LED. First, the threshold of unavoidability in Article 5 Wpg is stricter than that of necessity in Article 10 LED, as the former requires that no viable alternative exists to achieve the same objective, whereas the latter allows some discretion. Second, the Wpg only permits this specific processing if an individual is already the subject of other police data, prohibiting processing in isolation. Third, Articles 5 and 6 Wpg state more concrete requirements and detailed rules regarding adequate data security and protection.

While the Wpg implements the obligations from the LED with added strictness, it still considered to fall short in meeting the 'end-to-end' safeguards (Schermer & Galič, 2022, p. 176) and having proactive review of an independent authoritative body highly needed in case of biometric data processing (Hu & Kouwenberg, 2023, p. 3).

Post-Remote Biometric Identification

Artificial Intelligence Act (AIA)

As noted in the Theoretical Framework, the AIA prohibits the use of real-time remote BIS under Article 5(1)(h). However, post-remote BIS fall under the 'high-risk' assessment level, to which different rules apply. Article 26(10) outlines five substantive and procedural safeguards for the use of post-remote BIS in law enforcement, explicitly stating these are "without prejudice to" the LED. The AIA thus functions as the lex specialis to the LED (Veale & Zuiderveen Borgesius, 2021, p. 101).

In summary, law enforcement authorities must comply with the requirements of (I) authorisation, (II) use limitations, (III) data deletion, (IV) no automated decision-making, and (V) documentation and reporting when deploying post-remote BIS, such as FRT. Additionally, deployers of such AI systems must adhere to FRIA obligations; yet, concrete methodological criteria still remain absent (Mantelero, 2024, p. 18).

Furthermore, the AIA regulation of post-remote BIS is considered insufficient in light of necessity tests articulated by both the ECtHR and the CJEU (Jasserand, 2023, p. 17). This may result in implementation fragmentation among member states (Giannini & Tas, 2024, p. 5) and unjustified usage expansion (Murray, 2024, p. 146).

Soft Law Guidelines

At the international level, the UN has taken a firm stance against the use of FRT in the context of peaceful protests. Both the Model Protocol (paras. 61-62, 71) and the technical component (paras. 35-37) of the new UN toolkit (Voule, 2024) explicitly prohibit FRT to categorise, profile, or remotely identify protesters before, during, and after demonstrations, emphasising the individual right to anonymity and warning against the alarming potential for chilling effects on the freedom of assembly.

At the regional level, a more nuanced approach emerges. The CoE Guidelines allow for limited FRT usage while emphasising strong rights protections, requiring strict necessity and proportionality tests, and supervisory authority oversight (2021, p. 29). The EDPB provides further guidance for law enforcement authorities, highlighting the serious interference of FRT with fundamental rights and requiring mandatory impact assessments and prior consultation with supervisory authorities (2022, paras. 39-41). Both emphasise the need for clear legal parameters and accountability measures.

At the national level, Dutch frameworks focus on practical implementation while maintaining strict usage controls. The AP (2024, p. 3) emphasises that, based on existing legislation, the utilisation of FRT by law enforcement authorities requires either explicit consent or substantial public interest justification. The police's (2024, p. 7) framework provides guidance for operational deployment, considering ethical, legal, and technical aspects. However, both merely outline already existing legislation, deemed inadequate for failing to impose substantive constraints on predictive police profiling (De Hert & Lammerant, 2016, p. 145), construct independent oversight (Hu & Kouwenberg, 2023, p. 3), guarantee 'end-to-end' safeguards (Schermer & Galič, 2022, p. 177), and address gaps in the checks and balances system (Galič & Stevens, 2023, p. 461).

Judicial Interpretations

Based on the legal conditions outlined in the previous section, the following subsections explore jurisprudence to assess how courts have applied the interaction between fundamental rights and data protection in practice. In addition to several general legal precedents relevant to this field from both the ECtHR and the CJEU, two cases will be analysed in detail: a case before the DCtTH on camera surveillance in public spaces (*Politie v. AP*, 2024) and a landmark ECtHR case on the use of real-time FRT in the context of protests (*Gluhkin v. RU*, 2023).

General Legal Precedents

Since the early 21st century, the ECtHR has established crucial precedents regarding biometric data and Article 8 ECHR (privacy). The landmark case *S. & Marper v. UK* (2008) addressed indefinite retention of DNA profiles and fingerprints by UK authorities, even after acquittals (para. 119). The ECtHR ruled this policy disproportionate and violative of Article 8 (para. 125), reinforcing the proportionality principle for biometric data retention by requiring it to be held only as long as necessary under specific circumstances (para. 107).

Catt v. UK (2019) reinforced these principles, finding indefinite personal data retention from a peaceful protester disproportionate, constituting an Article 8 infringement (para. 128). This ruling demonstrates that data retention in peaceful assembly contexts without clear legal safeguards may breach the ECHR, highlighting surveillance risks in protest environments (para. 123). This strict approach was upheld in *Gaughran v. UK* (2020), finding data retention in case of minor offences disproportionate due to a lack of review possibilities (para. 94). The privacy infringement reinforced proportionality and judicial oversight requirements (para. 96).

Another well-known case before the ECtHR, *Big Brother Watch & Others v. UK* (2021), found UK mass surveillance and bulk interception a direct violation of both Articles 8 and 10 due to insufficient independent oversight, judicial authorisation, and abuse of safeguards (paras. 426-427). It also stated such practices may create chilling effects on expression, emphasising the need for transparent, accountable surveillance for the first time (paras. 448, 350).

The CJEU delivered a landmark preliminary ruling, *RL v. Landeshauptstadt Wiesbaden* (2024), in which fingerprint ID card requirements were found to interfere with Articles 7 and 8 CFREU (para. 73). It reaffirms that biometrics call for sufficient safeguards and proportionality assessments (paras. 84, 110-118). Other legal controversies, such as the decade-long proceeding by the Dutch civil rights group Vrijbit (2020) over facial scans for passport purposes, similarly underscore the conflicting interests between security measures and civic freedoms.

DCtTH in Politie v. AP

During the COVID-19 pandemic, the Dutch police had deployed Mobile Camera Cars (MCAs) equipped with 360-degree cameras to monitor public spaces (para. 2). These vehicles captured real-time panoramic, street-level footage, including images of individuals and license plates. The AP (2022) subsequently imposed a fine for processing data without conducting a prior GEB. The legal issue at stake was whether the police had indeed violated their obligations under Article 4(c) Wpg (the GEB requirement) with their MCA deployment.

First, the ECtHR confirmed that the footage constituted personal data, even if no actual identification had taken place (para. 9). Second, this was thought to involve high-risk processing due to the scale, novelty, and lack of control of monitoring individuals without their awareness of the data collection and usage. Moreover, it was stressed that the surveillance may have been "impossible for individuals to avoid" (para. 11). Third, the GEB obligation was breached as it was completed days after the processing initiation (para. 14). Fourth, the appeal to emergency circumstances was dismissed as there was no "force majeure situation" (para. 18). However, the fine was reduced based on the offence duration and recurrence risk (para. 24).

In conclusion, the DCtTH confirmed that the police violated Article 4(c) Wpg by failing to conduct a GEB before deploying the MCAs. This case affirms that public video surveillance, even without identification, qualifies as high-risk processing. It further clarifies that procedural safeguards, such as conducting a GEB, are not optional, even in crisis situations.

ECtHR in Gluhkin v. RU

In August 2019, Mr Gluhkin held a peaceful solo protest in the Moscow underground (para. 7). After images were shared online, police used CCTV footage and FRT to identify and locate Gluhkin (paras. 8-12). He was subsequently arrested, charged with holding a public event without prior notification, with authorities arguing the cardboard figure constituted a "quickly

(de)assembled object" (para. 13). Despite the peaceful nature of his protest, he was convicted and fined (para. 15, 17), leading Gluhkin to bring the case in front of the ECtHR. The relevant provisions from the ECHR are Articles 8 (right to privacy) regarding biometrics and images in public spaces, and 10 (freedom of expression) in terms of nonverbal expressions.

The ECtHR examined the case under both articles and established several key principles regarding FRT use in protest contexts. Under Article 10, the Court found that Gluhkin's protest constituted protected expression on matters of public interest (para. 51). The utilisation of FRT for identification and monitoring created a significant interference with his rights, operating "as a tool of suppression" (para. 52), which was unjustified, as authorities failed to demonstrate the requisite tolerance for peaceful protest (para. 56). Furthermore, the use of FRT was considered to infringe on Article 8 (para. 73), classifying the biometric data collected as sensitive political information needing "heightened protection" (para. 76). The domestic legal order was criticised for lacking sufficient safeguards, limitations, and supervisory mechanisms (para. 83).

In conclusion, the ECtHR stressed that FRT is "highly intrusive" (para. 88) and requires "the highest level of justification" due to its potential chilling effect on freedom of expression and assembly, directly linking biometric surveillance to deterring the exercise of these rights (para. 86, 88). This unanimous ruling establishes a clear legal precedent that using FRT in the context of protests and in the absence of adequate legal safeguards, proportionality assessments, and transparency violates the ECHR, expanding the chilling effect doctrine.

However, scholars have scrutinised this judgement for failing to establish authoritative, rights-informed standards by not clarifying conditions for FRT deployment (Gabrielli, 2025, p. 27) and implementing a "laid-back approach" that avoided addressing whether it is intrinsically ECHR-compatible (Cocito, 2024, p. 3). While this case may have been straightforward due to its administrative nature, more complex challenges in the balancing of privacy rights with law enforcement aims will likely arise in the future (Palmiotto & González, 2023, p. 6).

Empirical Analysis

This section will provide the analyses performed with the empirical data obtained from the conducted survey to answer the third sub-question. The sub-sections are divided based on the different types of components in the survey, both exploratory and confirmatory.

Exploratory Questions

Just over half of the sample had firsthand protest experience: 45 respondents (52.9%) reported ever joining a demonstration in the Netherlands, most having done so once or twice in the past five years (32.9% of the full sample), while 20% had taken to the streets three or more times. Familiarity with FRT was mixed: although 50.6% indicated they had heard about FRT, only one out of five respondents (18.8%) knew the Dutch police can deploy it. Three-quarters (75.3%) were unaware of the number of surveillance cameras on the streets in the Netherlands and the potential for biometric identification through that footage; respondents tended to feel uneasy with that fact: one-third (34.2%) disagreed that the number of cameras made them feel safe, whereas 37.6% “somewhat agreed” and 12.9% “strongly agreed”.

Attitudes toward the use of FRT by Dutch law enforcement authorities were ambivalent. While a clear majority (35.3%) “somewhat agreed” with such use and 18.8% “strongly agreed”, a sizable minority (35.3% combined) expressed some level of disagreement. Mirroring this, 44.7% acknowledged personal concern about FRT, yet only 7.1% were “strongly” worried, and one quarter were neutral. When asked about its primary purpose, two-thirds (69.4%) believed FRT should be employed “mostly for safety”, with just 4.7% selecting “mostly for control” and 8.2% opting for “both equally”, 17.7% rejected either rationale or were unsure.

Perceptions of institutional trust showed mild erosion: about one-third of respondents “somewhat agreed” that FRT undermines trust in the government (34.1%) and law enforcement (27.1%); however, strong distrust was voiced by fewer than one in ten. Finally, political self-

placement on a left-right slider scale averaged 28.56 (*SD* = 2.67), indicating a modest lean toward the left side of the political spectrum. These descriptive patterns, though exploratory, suggest that previous protest activity and limited prior knowledge shape a cautiously mixed public stance toward FRT use by the Dutch police (see Table 7).

Finally, the baseline attitudes, visualised in Figure 1, revealed that respondents entered the study relatively confident about exercising their freedom of expression but more cautious regarding assembly. Roughly three-quarters already "somewhat" or "strongly" agreed in terms of expression *willingness* and *capability*, and just one in ten openly disagreed. Perceived *safety*, however, drew a mixed response, with neutrality and mild scepticism accounting for nearly half the sample. The pattern sharpened for assembly: *willingness* to join a protest was still more positive than negative, but the neutral share is markedly larger, with disagreement dominating the *likelihood* item: almost half of the participants signalled they were unlikely to take to the streets in the Netherlands on matters that are important to them. In short, before any mention of FRT, the sample felt able and inclined to voice opinions, but their resolve to truly partake in protests was already tempered by safety and motivational reservations.

Attitude Change

After participants read the vignette explaining when and how the Dutch police can use FRT, each respondent indicated "how this knowledge affects my…" *willingness*, *likelihood*, perceived *safety*, and *perceived* capability to exercise the freedoms. Responses were recorded with five-point Likert scale items ranging from extremely negative to extremely positive, with the middle marking neither positive nor negative. Tables 2 and 3, as well as Figure 2, display the results for the eight two-tailed one-sample *t*-tests conducted to evaluate H1 (freedom of expression) and H2 (freedom of assembly). Negative mean-change scores indicate participants reported lower agreement than initially, relative to the neutral midpoint (0).

Table 2

One-Sample t-Test Results for Freedom of Expression (N = 85, df = 84)

Attitude	M_Δ	*SD*	*t*(84)	*p*	Cohen's *d*	95 % CI for *d*
Willingness	-0.08	0.93	-0.82	.416	-0.09	[-0.30, 0.13]
Likelihood	-0.33	0.97	-3.14	.002	-0.34	[-0.56, -0.12]
Safety	0.11	1.13	0.86	.392	0.09	[-0.12, 0.31]
Capability	-0.09	0.80	-1.09	.279	-0.12	[-0.33, 0.10]

Note. M_Δ = mean change (post-pre-exposure to vignettes with information on FRT). Negative values indicate attitudes below the neutral midpoint (0). Bonferroni-adjusted $\alpha = .00625$.

For freedom of expression, the only significant shift found concerned the *likelihood* of its exercise: knowing about FRT use by Dutch law enforcement authorities produced a modest, negative effect on expressing oneself (e.g., thoughts and opinions) in the Netherlands on matters important to them (M_Δ = -0.33, *SD* = 0.97), *t*(84) = -3.14, *p* = .002, *d* = -0.34, 95 % CI [-0.56, -0.12]. By contrast, the same knowledge left participants' *willingness* (M_Δ = -0.08), perceived *safety* (M_Δ = +0.11), and perceived *capability* (M_Δ = -0.09) remained essentially unchanged; each confidence interval spanned the neutral point, and all *p* values exceeded .27.

The pattern was slightly stronger for freedom of assembly. Learning about FRT use by Dutch law enforcement authorities exerted a small, negative effect on *willingness* to assemble (e.g., participate in protests) in the Netherlands in support of matters important to them (M_Δ = -0.31, *SD* = 0.91), *t*(84) = -3.09, *p* = .003, *d* = -0.33, 95 % CI [-0.55, -0.12] and *likelihood* of doing so (M_Δ = -0.39, *SD* = 0.96), *t*(84) = -3.71, *p* = <.001, *d* = -0.40, 95 % CI [-0.62, -0.19]. Perceptions of *safety* (M_Δ = -0.02) and *capability* (M_Δ = -0.13) did not significantly differ from neutrality ($|t| \leq 1.59$, $p \leq .117$). The Bonferroni-adjusted criterion ($\alpha = .00625$) confirms that only the three effects just described in detail remain statistically significant.

To conclude, these analyses yield only partial confirmation of both hypotheses.

Table 3

One-Sample t-Test Results for Freedom of Assembly (N = 85, df = 84)

Attitude	M_Δ	*SD*	*t*(84)	*p*	Cohen's *d*	95 % CI for *d*
Willingness	-0.31	0.91	-3.09	.003	-0.33	[-0.55, -0.12]
Likelihood	-0.39	0.96	-3.71	< .001	-0.40	[-0.62, -0.19]
Safety	-0.02	1.14	-0.19	.850	-0.02	[-0.24, 0.20]
Capability	-0.13	0.75	-1.59	.117	-0.17	[-0.39, 0.04]

Note. See Table 2 note.

Thoughts and Concerns

Twenty-seven respondents replied to the open-ended question at the end of the survey, which inquired about specific thoughts or concerns regarding FRT in the Netherlands. Three broad themes and nine sub-themes were identified. Table 8 provides this framework, while Table 9 contains the complete responses with their corresponding code(s).

Political and civil liberties concerns dominated: one-third of all segments warned that FRT could be repurposed for protest surveillance (9/27). In contrast, others feared wider regime risks such as an authoritarian drift (5/27) or unspecified future misuse (1/27).

A second cluster focused on implementation concerns. Here, respondents most often questioned responsibility and accountability for errors or abuse (8/27) and highlighted potential bias and discrimination inherent in algorithms or enforcement practices (5/27), with additional anxiety reported about data privacy protection and storage principles (3/27).

Finally, a minority expressed supportive views: several saw FRT as acceptable under conditional use with strict safeguards (5/27) or placed institutional trust in Dutch authorities to use FRT carefully and in accordance with the law (6/27). A few cited possible technological benefits, such as quicker suspect identification in criminal investigations (2/27).

Overall, this suggests that while many participants acknowledge situational advantages of FRT, reservations about political surveillance and equitable implementation remain salient.

Discussion

Reflections

The doctrinal analyses facilitated an intriguing comparison between law in theory and in practice. The legal landscape surrounding FRT is not only multilayered across governance levels but also among legal doctrines, serving as a true testament to the potential and intrinsic complexities of its regulation. While hard law delineates the conditions for the processing of biometric data (GDPR, UAVG, LED, Wpg) and the use of live biometric identification (AIA), soft law (UN, CoE, EDPB, AP, the Dutch Police) provides FRT guidance while emphasising its dangers in the context of protests and the need for more robust regulation. To date, no legally binding rules govern the retrospective use of FRT by the Dutch police.

Nevertheless, Dutch citizens have access to strong fundamental rights frameworks and safeguards (ICCPR, ECHR, CFREU, Gw). Judicial interpretations from various courts (ECtHR, CJEU, and DCtHR) have proven to be strict in cases of biometric surveillance and post-remote identification due to the capability of undermining the very conditions for exercising freedom of expression and assembly. Such rights interferences may be legitimate only where all tests of legality, legitimate aim, necessity, and proportionality are sufficiently satisfied.

The empirical results reveal a nuanced manifestation of Foucault's (1977) Panopticon operating through Schauer's (1978) chilling effect notion: FRT awareness revealed a significant deterrent effect on the likelihood of expression and both willingness and likelihood to assemble. Surveillance-induced self-regulation may therefore target specific intentions, challenging the traditional panoptic prediction of behavioural modification. The stronger effects on assembly further demonstrate how FRT deployment may reduce collective protest participation. Despite the relatively high rate of FRT acceptance, measurable chilling effects occurred, revealing that panoptic power may operate through psychological mechanisms below conscious approval, activated by knowledge of potential visibility rather than actual surveillance.

Evaluations

This study addresses a Dutch-specific gap in FRT literature by integrating black-letter analysis with empirical data on attitudes towards the exercise of protest-related rights, which previous Dutch studies and scholarship had examined solely legally (Galič & Stevens, 2023), qualitatively (Amnesty, 2023, 2024), or behaviourally (Storbeck et al., 2025).

Peaceful assembly is protected as a cornerstone of Dutch democracy (Swart & Roorda, 2023, p. 49). The safe exercise of freedom of expression and assembly is, therefore, of utmost importance for society as a whole. If FRT use by the police in the context of protests results in increasing identification, profiling, or reprisal, it risks reshaping not only the number but also the scope, meaning, and inclusivity of public events (OHCHR, 2020; EPRS, 2021).

Furthermore, the legal 'ought' has truly complemented the socio-psychological 'is'. While the former tried to clarify when and how FRT may be deployed, the latter contributed to understanding how individuals might respond to it in practice. This interdisciplinary integration resulted in a fruitful combination of interpretivist and post-positivist epistemologies.

Limitations

The regulatory gap encountered has posed a significant obstacle in and of itself. Further, it is acknowledged that due to the new and evolving nature of this field, Dutch-focused legal scholarship and FRT-specific judicial interpretations were relatively scarce. Future (use) cases will undoubtedly provide more nuance to the tests of the legal principles in practice.

This study may lack population representativeness because of convenience sampling, online recruitment, and the number of respondents. Given the relatively young, female, and left-wing cohort, findings may also lack certain generalisability to older or more politically diverse populations. Additionally, the results depended on self-reported attitudes and intentions rather than actual observed behaviour. Finally, the Likert items sacrificed reliability: the vignette only measured immediate attitudinal change, not sustained behaviour over time.

Recommendations

Comparative analysis might reveal insights into how other jurisdictions legislate FRT. Given the often-discriminatory nature of algorithms, it is interesting, if not necessary, to explore the interplay between FRT deployment and the prohibition of discrimination. Technical audits may also be conducted to couple legal analysis with training data and false-positive rates to link proportionality principles to empirical accuracy. Other research designs, such as panel studies or field experiments, could track individuals before and after FRT deployment during protests. This might clarify if and how the chilling effect manifests in real-life settings. Furthermore, holistic remedy and oversight studies could be conducted through qualitative interviews with activists, police units, and supervisory bodies to reveal accountability gaps.

The complex relationship between Dutch administrative, criminal procedural, and data protection law has long been highlighted (De Hert & Lammerant, 2016, pp. 161-167). Clear, harmonised legal standards are needed across the EU to address the legislative gap and avoid both potential abuses and fragmentation in biometric surveillance laws (Raposo, 2022, p. 517). There is no need to start from scratch: existing policies and regulations provide a stepping stone (Galič & Stevens, 2023, p. 477). This thesis contends that this not only requires looking beyond the boundaries of legal doctrines but also beyond the discipline of law itself.

Conclusion

In today's digitalised world, maintaining privacy can be so challenging that it is nearly forgotten as a fundamental right to which everyone is entitled. Intrusive surveillance methods such as FRT are as difficult to detect as they are to avoid. When used in protest settings, these can have a deterrent effect on protest-related rights and freedoms. FRT deployment poses a dystopian slippery slope towards an obligation to be identifiable without the possibility to object (Weijts, 2025). The visibility trap has evidently expanded to the public space. It is, therefore, paramount citizens are not only aware of being watched but also of being protected.

References

Primary legal authoritative sources are cited in accordance with The Bluebook 22nd edition; all other authoritative sources are cited in line with APA 7th edition.

Primary Authority

Treaties and Other International Agreements

Charter of Fundamental Rights of the European Union (CFREU), Dec. 7, 2000, 2000 O.J. (C 364) 1

Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Nov. 4, 1950, 213 U.N.T.S. 221

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), Jan. 28, 1981, E.T.S. No. 108

International Covenant on Civil and Political Rights (ICCPR), Dec. 16, 1966, 999 U.N.T.S. 171

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), Oct. 10, 2018, C.E.T.S. No. 223

Constitutions

Grondwet (Gw) [Constitution], Stb. 2023, 62 (Neth.)

Statutes

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 Apr. 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 (Law Enforcement Directive) (LED), 2016 O.J. (L 119) 89

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (GDPR), 2016 O.J. (L 119) 1

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (AIA), 2024 O.J. (L 144) 1

Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) [Implementation Act General Data Protection Regulation], Stb. 2021, 135 (Neth.)

Wet justitiële en strafvorderlijke gegevens (Wjsg) [Judicial Data and Criminal Records Act], Stb. 2024, 198 (Neth.)

Wet openbare manifestaties (Wom) [Public Assemblies Act], Stb. 2010, 350 (Neth.)

Wet politiegegevens (Wpg) [Police Data Act], Stb. 2024, 377 (Neth.)

Cases

Big Brother Watch & Others v. U.K., App. Nos. 58170/13, 62322/14 & 24960/15, Eur. Ct. H.R. (May 25, 2021)

Catt v. U.K., App. No. 43514/15, Eur. Ct. H.R. (Jan. 24, 2019)

Gaughran v. U.K., App. No. 45245/15, Eur. Ct. H.R. (Feb. 13, 2020)

Gluhkin v. Russ., App. No. 11519/20, Eur. Ct. H.R. (July 4, 2023)

Korpschef van Politie v. Autoriteit Persoonsgegevens (*Politie v. AP*), Rb. Den Haag, 8 Oct. 2024, ECLI:NL:RBDHA:2024:16324 (Neth.)

RL v. Landeshauptstadt Wiesbaden, Case C-61/22, ECLI:EU:C:2024:251 (CJEU 2024)

S. & Marper v. U.K., App. Nos. 30562/04 & 30566/04, Eur. Ct. H.R. (Dec. 4, 2008)

Other Authorities

Aanhangsel Handelingen I, 2023/2024, nr. 982

Aanhangsel Handelingen I, 2024/2025, nr. 748

Ada Lovelace Institute (ALI). (2025). An eye on the future: A legal framework for the governance of biometric technologies in the UK. In *Nuffield Foundation*. Ada Lovelace Institute. https://www.adalovelaceinstitute.org/report/an-eye-on-the-future/

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-t

Amnesty International. (2023). Unchecked Power: ID Checks and Collection of Data from Peaceful Protesters in the Netherlands. In *Amnesty International* (EUR 35/6650/2023). https://www.amnesty.org/en/documents/eur35/6650/2023/en/

Amnesty International. (2024). Recording dissent: Camera surveillance at peaceful protests in the Netherlands. In *Amnesty International* (EUR 35/8469/2024). https://www.amnesty.org/en/documents/eur35/8469/2024/en/

Amnesty International. (2025, March 21). *Hungary: Pride ban is full-frontal attack on LGBTI people and must not be signed into law*. https://www.amnesty.org/en/latest/news/2025/03/hungary-pride-ban-is-full-frontal-attack-on-lgbti-people-and-must-not-be-signed-into-law/

Article 29 Data Protection Working Party. (2017). Opinion on some key issues of the Law Enforcement Directive (EU 2016/680). In *European Commission*. European Commission. https://ec.europa.eu/newsroom/article29/items/610178/en

Autoriteit Persoonsgegevens (AP). (2024a). *Juridisch kader gezichtsherkenning*. Autoriteit Persoonsgegevens. https://www.autoriteitpersoonsgegevens.nl/documenten/juridisch-kader-gezichtsherkenning

Autoriteit Persoonsgegevens (AP). (2024b, September 3). *Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition*. Autoriteit Persoonsgegevens. https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition

Beduschi, D., & Ebert, D. I. (2021). *The relevance of the Smart Mix of Measures for Artificial Intelligence - Assessing the Role of Regulation and the Need for Stronger Policy Coherence*. The Geneva Academy of International Humanitarian Law and Human Rights. https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/The%20relevance%20of%20the%20Smart%20Mix%20of%20Measures%20for%20Artificial%20Intelligence.pdf

Ben-Shachar, M., Lüdecke, D., & Makowski, D. (2020). effectsize: Estimation of Effect Size Indices and Standardized Parameters. *The Journal of Open Source Software*, *5*(56), 2815. https://doi.org/10.21105/joss.02815

Besselink, L. (2022). Artikelen 93 en 94: Doorwerking en voorrang van internationaal recht. In *Een nieuw commentaar op de Grondwet* (pp. 406–420). Boom. https://pure.uva.nl/ws/files/146201055/Besselink_-_Artikelen_93_en_94_GW_met_noten.pdf

Best, E. (2022). Policy-making in the European Union. In *European Union Politics* (7th ed., pp. 235–290). Oxford University Press.

Bhat, P. I. (2020). Doctrinal legal research as a means of synthesizing facts, thoughts, and legal principles. In *Oxford University Press eBooks* (pp. 143–168). https://doi.org/10.1093/oso/9780199493098.003.0005

Bits of Freedom. (2019). Het ware gezicht van gezichtsherkenningstechnologie. In *Bits of Freedom*. https://www.bitsoffreedom.nl/wp-content/uploads/2019/11/het-ware-gezicht-van-gezichtsherkenningstechnologie.pdf

Bovend'Eert, P. (2021). Het toetsingsverbod van art. 120 Grondwet en het toetsingsgebod van art. 94 Grondwet. In *Constitutioneel Recht* (pp. 408–417). Wolters Kluwer.

Bradford, B., Yesberg, J., Jackson, J., & Dawson, P. (2020). Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology. *SocArXiv*. https://doi.org/10.31235/osf.io/n3pwa

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brewczyńska, M. (2023). Between legitimacy and lawfulness: in search of rationality and consistency in EU data protection. *European Data Protection Law Review*, *9*(2), 112–122. https://doi.org/10.21552/edpl/2023/2/6

Brinkhoff, S. (2017). Big data data mining by the Dutch Police: Criteria for a future method of investigation. *European Journal for Security Research*, *2*(1), 57–69. https://doi.org/10.1007/s41125-017-0012-x

Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press.

Canova, G., & Simmler, M. (2024). Facial recognition technology in law enforcement: Regulating data analysis of another kind. *Computer Law & Security Review*, *56*, 106092. https://doi.org/10.1016/j.clsr.2024.106092

Charlesworth, H. (2008). Universal Declaration of Human Rights (1948). In *A. Peters & R. Wolfrum (Eds.), Max Planck Encyclopedia of Public International Law [MPEPIL]. Oxford University Press.* https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1479

Choung, H., David, P., & Ling, T. (2024). Acceptance of AI-Powered Facial Recognition Technology in Surveillance scenarios: Role of trust, security, and privacy perceptions. *Technology in Society*, 102721. https://doi.org/10.1016/j.techsoc.2024.102721

Christakis, T., Bannelier, K., Castelluccia, C., & Métayer, D. L. (2022). Mapping the use of facial recognition in public spaces in Europe – Part 1: A quest for clarity: Unpicking the "Catch-All" term. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4110512

Chubb, A., & Lyer, K. R. (2024). Transnational Human Rights Violations: Addressing the Evolution of Globalized Repression through National Human Rights Institutions. *Journal of Human Rights Practice*, *16*(3), 770–793. https://doi.org/10.1093/jhuman/huae017

Cocito, C. (2024, January 9). *Glukhin v. Russia: facial recognition considered highly intrusive but not inconsistent with fundamental rights - Strasbourg Observers*. Strasbourg Observers. https://strasbourgobservers.com/2024/01/09/glukhin-v-russia-facial-recognition-is-a-highly-intrusive-technology-but-the-court-abstains-from-considering-a-potential-inconsistency-with-fundamental-rights/

Council of Europe (CoE). (2022). *Convention 108 and Protocols*. Council of Europe Portal. https://www.coe.int/en/web/data-protection/convention108-and-protocol

De Hert, P., & Lammerant, H. (2016). Predictive profiling and its legal limits: Effectiveness gone forever. In *Exploring the boundaries of big data* (pp. 145–168). Amsterdam University Press.

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, *32*(2), 179–194. https://doi.org/10.1016/j.clsr.2016.02.006

De Terwangne, C. (2021). Council of Europe convention 108+: A modernised international treaty for the protection of personal data. *Computer Law & Security Review*, *40*, 105497. https://doi.org/10.1016/j.clsr.2020.105497

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-Commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Directorate General for Communication of the European Parliament. (2025, February 19). *EU AI Act: first regulation on artificial intelligence*. European Parliament. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

Ericson, R. V., & Haggerty, K. D. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605–622. https://doi.org/10.1080/00071310020015280

European Commission (EC). (2024). *The Digital Decade*. European Union. https://doi.org/10.2759/927260

European Data Protection Board (EDPB). (2023). Adopted Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. In *European Data Protection Board*. https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

European Digital Rights (EDRi). (2021). *The rise and rise of biometric mass surveillance in the EU*. https://edri.org/wp-content/uploads/2021/07/The-Rise-and-Rise-of-Biometric-Mass-Surveillance-in-the-EU_Dutch-Summary.pdf

European Parliament. (2021). *European Parliament Resolution on Artificial Intelligence in Criminal Law and its use by the police and judicial Authorities in criminal matters (2020/2016(INI))* (P9_TA(2021)0405). https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html

European Parliamentary Research Service (EPRS). (2021). Regulating facial recognition in the EU. In *PE 698.021* (pp. 1-) [Report]. European Union. https://doi.org/10.2861/140928

European Union Agency for Fundamental Rights (FRA). (2019). Facial recognition technology: fundamental rights considerations in the context of law enforcement. In *European Union Agency for Fundamental Rights*. https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

Foucault, M. (1977). *Discipline and punish: The birth of the prison*. Pantheon Books. (Original work published 1975)

Frohwein, J. A. (2009). European Convention for the Protection of Human Rights and Fundamental Freedoms (1950). In *A. Peters & R. Wolfrum (Eds.), Max Planck*

Encyclopedia of Public International Law [MPEPIL]. Oxford University Press. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e790

Future of Life Institute. (2025). *High-level summary of the AI Act | EU Artificial Intelligence Act*. EU Artificial Intelligence Act. https://artificialintelligenceact.eu/high-level-summary/

Gabrielli, G. (2025). The use of facial recognition technologies in the context of peaceful protest: the risk of mass surveillance practices and the implications for the protection of human rights. *European Journal of Risk Regulation*, 1–28. https://doi.org/10.1017/err.2025.26

Galič, M., & Stevens, L. (2023). Regulating police use of facial recognition technology in the Netherlands: The complex interplay between criminal procedural law and data protection law. *New Journal of European Criminal Law*, *14*(4), 459–478. https://doi.org/10.1177/20322844231212834

Giannini, A., & Tas, S. (2024, December 10). AI Act and the prohibition of Real-Time Biometric Identification. *Verfassungsblog*. https://doi.org/10.59704/a15aa6e58151c853

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605–622. https://doi.org/10.1080/00071310020015280

Hietland, C. (2016). Het imaazje van Provo. *Tijdschrift Voor Geschiedenis*, *129*(3), 433–446. https://doi.org/10.5117/tvgesch2016.3.hiet

Hijmans, H. (2016). Privacy and Data Protection as Values of the EU That Matter, Also in the Information Society. In *The European Union as guardian of internet privacy: The Story of Art 16 TFEU* (pp. 17–75). Springer. https://doi.org/10.1007/978-3-319-34090-6_2

Holland, J., & Webb, J. (2019). *Learning legal rules: A Students' Guide to Legal Method and Reasoning*. Oxford University Press.

Houwing, L. (2024, March 26). *De politie trekt zich van niemand wat aan bij de inzet van gezichtsherkenning*. Bits of Freedom. https://www.bitsoffreedom.nl/2024/03/27/de-politie-trekt-zich-van-niemand-wat-aan-bij-de-inzet-van-gezichtsherkenning/

Hu, Y. Y., & Kouwenberg, M. (2023). Gezichtsherkenningstechnologie in de opsporing. Tijd voor onafhankelijk toezicht? In *Ars Aequi*. https://repository.ubn.ru.nl/bitstream/handle/2066/287257/287257.pdf?sequence=1&isAllowed=y

Huisman, C. (2025, May 14). DPG Media Privacy Gate. *De Volkskrant*. https://www.volkskrant.nl/binnenland/politie-belooft-nieuwe-aanpak-voor-huisbezoeken-aan-demonstranten~bf946019/?referrer=https%3A%2F%2Fwww.google.com%2F

Hunt, L. (2007). The Soft Power of Humanity. In *Inventing Human Rights* (pp. 176–214). W.W. Norton & Company.

Jasserand, C. (2023). The future AI Act and facial recognition technologies in public spaces: *European Data Protection Law Review*, *9*(4), 430–443. https://doi.org/10.21552/edpl/2023/4/9

Kostka, G., Steinacker, L., & Meckel, M. (2022). Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly*, *40*(1), 101761. https://doi.org/10.1016/j.giq.2022.101761

Kuru, T. (2025). Investigative genetic genealogy in Europe: Why the "manifestly made public by the data subject" legal basis should be avoided. *Computer Law & Security Review*, *56*, 106106. https://doi.org/10.1016/j.clsr.2025.106106

Laganà, M. (2022, April 1). *Facial recognition and human rights in Europe — Human Rights Pulse*. Human Rights Pulse. https://www.humanrightspulse.com/mastercontentblog/facial-recognition-and-human-rights-in-europe

Lai, X., & Rau, P. P. (2021). Has facial recognition technology been misused? A public perception model of facial recognition scenarios. *Computers in Human Behavior*, *124*, 106894. https://doi.org/10.1016/j.chb.2021.106894

Letwin, J. (2023). Proportionality, stringency and utility in the jurisprudence of the European Court of Human Rights. *Human Rights Law Review*, *23*(3). https://doi.org/10.1093/hrlr/ngad014

Lynch, N. (2024). Facial Recognition Technology in Policing and Security—Case Studies in Regulation. *Laws*, *13*(3), 35. https://doi.org/10.3390/laws13030035

Lynskey, O. (2015). *The foundations of EU Data Protection Law*. Oxford University Press.

Mantelero, A. (2024). The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template. *Computer Law & Security Review*, *54*, 106020. https://doi.org/10.1016/j.clsr.2024.106020

Matulionyte, R. (2024). Transparency of Facial Recognition Technology and Trade Secrets. In *The Cambridge Handbook of Facial Recognition in the Modern State* (pp. 60–73). Cambridge University Press. https://doi.org/10.1017/9781009321211

Mesch, G., & Lam, I. (2024). Public perceptions about the police's use of facial recognition technologies. *AI & Society*. https://doi.org/10.1007/s00146-024-02158-w

Miethe, T. D., Dudinskaya, T., Forepaugh, C., & Sousa, W. H. (2023). Facial Recognition Technology in Policing: A National Survey of Public support for this technology and Privacy/Safety Concerns. *Crime & Delinquency*, 001112872211501. https://doi.org/10.1177/00111287221150172

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). (2024, September 30). *Essaybundel De Grondwet en nieuwe technologie klaar voor de toekomst*. Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/rapporten/2024/08/01/essaybundel-de-grondwet-en-nieuwe-technologie-klaar-voor-de-toekomst

Miranda, D., & Urquhart, L. (2021). Policing faces: the present and future of intelligent facial surveillance. *Information & Communications Technology Law*, *31*(2), 194–219. https://doi.org/10.1080/13600834.2021.1994220

Mitchell, D. (1995). The End of Public Space? People's Park, Definitions of the Public, and Democracy. *Annals of the Association of American Geographer*, 108–133. https://bpb-us-e2.wpmucdn.com/sites.middlebury.edu/dist/c/2991/files/2014/01/Mitchell-End-of-Public-Space.pdf

Molder, R. T., Dubelaar, M., Fedorova, M., Lestrade, S., & Walree, T. (2023). *Naar een duidelijker juridisch kader voor geautomatiseerde data-analyse in de opsporing*. https://hdl.handle.net/2066/293066

Murray, D., Fussey, P., Hove, K., Wakabi, W., Kimumwe, P., Saki, O., & Stevens, A. (2023). The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe. *Journal of Human Rights Practice*, *16*(1), 397–412. https://doi.org/10.1093/jhuman/huad020

NOS. (2025, March 25). *Kort geding Extinction Rebellion om huisbezoeken agenten aan demonstranten*. https://nos.nl/artikel/2561077-kort-geding-extinction-rebellion-om-huisbezoeken-agenten-aan-demonstranten

Office of the United Nations High Commissioner for Human Rights (OHCHR). (2020). *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests* (A/HRC/44/24). United Nations Human Rights Council. https://undocs.org/en/A/HRC/44/24

Openbaar Ministerie (OM). (2024, January 12). *Uitkomst nader onderzoek identificatie klimaatdemonstranten Schiphol*. Ministerie Van Justitie En Veiligheid. https://www.om.nl/actueel/nieuws/2024/01/12/uitkomst-nader-onderzoek-identificatie-klimaatdemonstranten-schiphol

Organisation for Economic Co-operation and Development (OECD). (1980). *Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data*. OECD. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Orwell, G. (1949). *Nineteen Eighty-Four*. Secker & Warburg.

Palmiotto, F., & González, N. M. (2023). Facial recognition technology, democracy and human rights. *Computer Law & Security Review*, *50*, 105857. https://doi.org/10.1016/j.clsr.2023.105857

Pech, L. (2021). The concept of chilling effect: Its untapped potential to better protect democracy, the rule of law, and fundamental rights in the EU. In *Open Society Foundations*. https://www.opensocietyfoundations.org/uploads/c8c58ad3-fd6e-4b2d-99fa-d8864355b638/the-concept-of-chilling-effect-20210322.pdf

Petursson, G. T. (2024). A new framework for limitation of fundamental rights in EU law? In *European Union and its neighbours in a globalized world* (pp. 239–252). https://doi.org/10.1007/978-3-031-65381-0_12

Politie. (2023). *Centrale Automatische TeChnologie voor Herkenning (CATCH) Jaarcijfers 2023*. https://www.politie.nl/binaries/content/assets/politie/nieuws/2024/november/494e7e76-a31d-4085-a97c-d654c52ba1a6.pdf

Politie. (2024, November 19). *Fors meer gezichtsvergelijkingen voor opsporing in 2023*. politie.nl. https://www.politie.nl/nieuws/2024/november/19/fors-meer-succesvolle-gezichtsvergelijkingen-voor-opsporing-in-2023.html

Privacy International. (2025). *Tracking protest surveillance*. https://privacyinternational.org/examples/tracking-protest-surveillance

Quelle, C. (2018). Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach. *European Journal of Risk Regulation*, *9*(3), 502–526. https://doi.org/10.1017/err.2018.47

R Core Team. (2025). *R: A language and environment for statistical computing (Version 4.4.0) [Computer software].* R Foundation for Statistical Computing. https://www.r-project.org/

Raposo, V. L. (2022). The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal. *European Journal on Criminal Policy and Research*, *29*(4), 515–533. https://doi.org/10.1007/s10610-022-09512-y

Rest of World. (2025, February 27). The changing face of protest. *Rest of World*. https://restofworld.org/2024/facial-recognition-government-protest-surveillance/

Schauer, F. (1978). *Fear, risk and the First Amendment: Unraveling the chilling effect*. William & Mary Law School Scholarship Repository. https://scholarship.law.wm.edu/facpubs/879

Schermer, B., & Galič, M. (2022). Biedt de Wet politiegegevens een stelsel van 'end-to-end' privacywaarborgen? *Nederlands Tijdschrift Voor Strafrecht*, *3*(3), 167–177. https://doi.org/10.5553/nts/266665532022003003006

Schrader, M., Vugts, Y., & Van Tilburg, A. M. (2024, January 5). *Politie experimenteert met gezichtsherkenning, maar wetgeving ontbreekt*. NOS. https://nos.nl/nieuwsuur/artikel/2503831-politie-experimenteert-met-gezichtsherkenning-maar-wetgeving-ontbreekt?utm_source=chatgpt.com

Schutt, R. K. (2020). *Understanding the social world: Research methods for the 21st century* (2nd ed.). SAGE Publications.

Seyyar, M. B., & Geradts, Z. (2020). Privacy impact assessment in large-scale digital forensic investigations. *Forensic Science International Digital Investigation*, *33*, 200906. https://doi.org/10.1016/j.fsidi.2020.200906

Slovic, P. (1987). Perception of risk. *Science*, *236*(4799), 280–285. https://doi.org/10.1126/science.3563507

Smith, M., & Mann, M. (2024). Facial Recognition Technology and Potential for Bias and Discrimination. In *The Cambridge Handbook of Facial Recognition in the Modern State* (pp. 87–95). Cambridge University Press. https://doi.org/10.1017/9781009321211

Smith, M., & Miller, S. (2021). The ethical application of biometric facial recognition technology. *AI & Society*, *37*(1), 167–175. https://doi.org/10.1007/s00146-021-01199-9

Smits, J. M. (2017). What is legal doctrine? In *Cambridge University Press eBooks* (pp. 207–228). https://doi.org/10.1017/9781316442906.006

Sociaal en Cultureel Planbureau (SCP). (2024, September 2). *Burgerperspectieven 2024 Bericht 2*. Ministerie Van Volksgezondheid, Welzijn En Sport. https://www.scp.nl/publicaties/publicaties/2024/09/03/burgerperspectieven-2024-bericht-2

Storbeck, M., Jacobs, G., Schuilenburg, M., & Van Den Akker, R. (2025). Surveillance experiences of extinction rebellion activists and police: Unpacking the technologization of Dutch protest policing. *Big Data & Society*, *12*(1). https://doi.org/10.1177/20539517241307892

Stoycheff, E., Liu, J., Xu, K., & Wibowo, K. (2018). Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects. *New Media & Society*, *21*(3), 602–619. https://doi.org/10.1177/1461444818801317

Swart, N., & Roorda, B. (2023). De reikwijdte van het bijkans heilige demonstratierecht. *Het Nederlands Juristen Comité Voor De Mensenrechten*, 28. https://njcm.nl/wp-content/uploads/2023/03/NTM-48-1_SwartRoorda.pdf

Tyler, T. R. (2006). *Why people obey the law*. Princeton University Press. https://doi.org/10.2307/j.ctv1j66769

Ullrich, P., & Knopp, P. (2018). Protesters' reactions to video surveillance of demonstrations: Counter-Moves, security cultures, and the spiral of Surveillance and Counter-Surveillance. *Surveillance & Society*, *16*(2), 183–202. https://doi.org/10.24908/ss.v16i2.6823

United Nations General Assembly (UNGA). (1948). *Universal declaration of human rights* (217 (III) A). https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf

United Nations Human Rights Council (HRC). (2023). *Right to privacy in the digital age* (A/HRC/RES/54/21). https://undocs.org/en/A/HRC/RES/54/21

United Nations (UN). (2011). *Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" framework*. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

Van Diepen, R. (2004). *Hollanditis: Nederland en het kernwapendebat, 1977-1987*. Bakker.

Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, *22*(4), 97–112. https://doi.org/10.9785/cri-2021-220402

Verloo, N. (2020). Voorbij het stigma van de populistische demonstrant: protest heeft een centrale functie in onze democratie! *Beleid En Maatschappij*, *47*(1), 84–86. https://doi.org/10.5553/benm/138900692020047001010

Voule, C. N. (2024). *Model protocol for law enforcement officials to promote and protect human rights in the context of peaceful protests: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*(A/HRC/55/60). United Nations Human Rights Council. https://undocs.org/en/A/HRC/55/60

Vrijbit. (2020, June 28). *Zaak Wijnberg*. Burgenrechtenbeweging Vrijbit. https://www.vrijbit.nl/rechtszaken-paspoortwet/zaak-wijnberg

Weijts, C. (2025, May 7). Column: Gewoon geen gelul meer. *Den Haag Centraal*. https://www.denhaagcentraal.net/nieuws/opinie/column-gewoon-geen-gelul-meer/

Wickham, H., Averick, M., Bryan, J., Chang, W., McGowan, L., François, R., Grolemund, G., Hayes, A., Henry, L., Hester, J., Kuhn, M., Pedersen, T., Miller, E., Bache, S., Müller, K., Ooms, J., Robinson, D., Seidel, D., Spinu, V., . . . Yutani, H. (2019). Welcome to the Tidyverse. *The Journal of Open Source Software*, *4*(43), 1686. https://doi.org/10.21105/joss.01686

Wolford, B. (2024, August 29). *What is GDPR, the EU's new data protection law?* GDPR.eu. https://gdpr.eu/what-is-gdpr/

World Economic Forum (WEF), UNICRI, INTERPOL, & Netherlands Police. (2022). A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations. In *World Economic Forum*. World Economic Forum. https://unicri.org/sites/default/files/2022-11/A%20Policy%20Framework%20for%20Responsible%20Limits%20on%20Facial%20Recognition.pdf

Tables

Table 4

Comparative Overview of Legal Instruments

Domain	**Fundamental Rights**			**Data Protection**			**Biometric Identification**		
Scope	**Int.**	**Reg.**	**Nat.**	**Int.**	**Reg.**	**Nat.**	**Int.**	**Reg.**	**Nat.**
Hard	ICCPR	ECHR, CFREU	Gw, Wom	Convention 108(+)	GDPR, LED	UAVG, Wpg	N/A	AIA	N/A
Soft	UDHR, UNGPs	N/A	N/A	OECD Guidelines	N/A	N/A	UN Toolkit	CoE & EDPB Guidelines	AP & Police Guidelines

Note. Int. = international; Reg. = regional; Nat. = national. See the Legal Concepts section.

Table 5

Comparative Overview of Fundamental Rights Frameworks

Right to…	**UDHR**	**ICCPR**	**ECHR**	**CFREU**	**Gw**
Privacy	Art. 12	Art. 17	Art. 8	Art. 7	Art. 10
Data protection	N/A	N/A	N/A	Art. 8	Art. 10
Freedom of expression	Art. 19	Art. 19	Art. 10	Art. 11	Art. 7
Freedom of assembly	Art. 20(1)	Art. 21	Art. 11	Art. 12	Art. 9

Note. See the List of Abbreviations for all instruments mentioned.

Table 6

Survey Cohort Descriptives

Variable	**Value**
Age in years, mean (SD)	21.49 (2.67)
Gender, n (%)	
Male	18 (21.2)
Female	66 (77.6)
Prefer not to say	1 (1.2)
Born in the Netherlands, n (%)	
Yes	48 (56.5)
No	37 (43.5)
Length of residence, n (%)	
1 to 5 years	35 (41.2)
5 to 10 years	1 (1.2)
More than 10 years	49 (57.6)

Note. *SD* = standard deviation from the mean; n = sample size.

Table 7

Exploratory Questions Descriptives

Variable	Value
Previous participation, n (%)	
Yes	45 (52.9)
No	40 (47.1)
Participation times in the past five years, n (%)	
0	40 (47.1)
1 to 2 times	28 (32.9)
3 to 5 times	8 (9.4)
More than 5 times	9 (10.6)
Prior knowledge of FRT, n (%)	
Yes	43 (50.6)
No	29 (34.1)
Unsure	13 (15.3)
Awareness of cameras and biometric identification, n (%)	
Yes	21 (24.7)
No	64 (75.3)
Feeling safe due to number of cameras, n (%)	
Strongly disagree	6 (7.1)
Somewhat disagree	23 (27.1)
Neither agree nor disagree	13 (15.3)
Somewhat agree	32 (37.6)
Strongly agree	11 (12.9)
Awareness of the use of FRT by the Dutch police, n (%)	
Yes	16 (18.8)
No	69 (81.2)
Agreement with the use of FRT by the Dutch police, n (%)	
Strongly disagree	4 (4.7)
Somewhat disagree	26 (30.6)
Neither agree nor disagree	9 (10.6)
Somewhat agree	30 (35.3)
Strongly agree	16 (18.8)
Concern with the use of FRT, n (%)	
Strongly disagree	5 (5.9)
Somewhat disagree	16 (18.8)
Neither agree nor disagree	20 (23.5)
Somewhat agree	38 (44.7)
Strongly agree	6 (7.1)
Purposes of the use of FRT, n (%)	
Mostly for safety	59 (69.4)
Mostly for control	4 (4.7)
Both equally	7 (8.2)
Neither	10 (11.8)
Unsure	5 (5.9)
Trust erosion government, n (%)	
Strongly disagree	8 (9.4)
Somewhat disagree	17 (20.0)

Neither agree nor disagree	24 (28.2)
Somewhat agree	29 (34.1)
Strongly agree	7 (8.2)
Trust erosion law enforcement, n (%)	
Strongly disagree	6 (7.1)
Somewhat disagree	29 (34.1)
Neither agree nor disagree	13 (15.3)
Somewhat agree	23 (27.1)
Strongly agree	14 (16.5)
Trust erosion state institutions, n (%)	
Strongly disagree	8 (9.4)
Somewhat disagree	20 (23.5)
Neither agree nor disagree	26 (30.6)
Somewhat agree	22 (25.9)
Strongly agree	9 (10.6)
Political spectrum, mean (SD)	28.56 (2.67)

Note. *SD* = standard deviation from the mean; n = sample size.

Table 8

Thematic Coding Framework

Main Category	**Sub-Category**	**Code**	**#**
Political concerns	Regime risks	RR	5
	Protest surveillance	PS	9
	Future misuse	FM	1
Implementation concerns	Bias & discrimination	BD	5
	Data & privacy	DP	3
	Responsibility & accountability	RA	8
Supportive views	Conditional use	CU	5
	Institutional trust	IT	6
	Technological benefits	TB	2

Note. Thematic coding principles based on Braun & Clarke (2006).

Table 9

Thematic Coding Open-Ended Responses

Full response	**Code(s)**
"I specifically fear for the moment that AI is implemented to trace people (as Israel is currently doing already) because that is way harder to control and check, and the allocation of responsibility becomes harder, which means that it is more difficult to hold actors in law enforcement accountable for mistakes or discrimination."	RA, RR
"I would hope that it also records the abuse of police officers against peaceful protests, and it should not be used to track people when they have not committed any major crime."	PS, CU
"Misuse and privacy concerns. Also, can be used by totalitarian regimes."	RA, DP, RR
"I think the use of FRT is a slippery slope to an authoritarian police state. 10 years ago, we were baffled that the Chinese government used this technology on its citizens and now we are accepting it ourselves. I am not worried about order and safety enough to agree with the use FRT to ensure it, and I think we have been able to have a reasonably safe and orderly society without FRT, so I do not see the need to start using it now."	RR
"Not necessarily, I do believe that institutions, as well as law enforcement, should use new developments with regards to AI etc. etc. for public safety and I don't think you can make a distinction in the use of AI."	TB
"While I see the usefulness of it for things like tracking down a serial killer, I do not think the use of it is justified for control. Knowing how violent the police are at protests, I feel that the state would go out of its way to use FRT to crack down on the freedom of assembly and speech when the matter being protested does not align with the continued support of a colonial settler state that is genociding a local population (Israel)."	CU, PS
I believe that the idea behind letting law enforcement use FRT during public assemblies and protests is to identify people causing public disruptions. While that idea sounds good, in practice the interpretation of public disruptions being left to law enforcers causes the problem, since they can target even peaceful protestors, which leads to a lower perception of safety."	PS, RA
"I trust the government and law enforcement enough to not cross borders when it comes to analysing and using FRT. If you don't do anything wrong and protest peacefully then you'll be fine."	IT
"It could lead to discrimination on different matters that are under the power of the government."	BD
"What is the likelihood that employees of a government agency will nevertheless secretly violate EU rules and still use FRT when they should not? How and by whom is this checked?"	RA
"I trust the government to use it carefully and in accordance with the law."	IT
"I think it's a good development for the legal system because it allows for a more objective view of events. However, I'm concerned that these cameras will eventually be used to train AI to detect abnormal behaviour at an early stage—like they already do at some airports to identify drug smugglers and terrorists. I'm not sure how I feel about that when it's applied to everyday life. On the other hand, I've also been to China, where they already use these kinds of cameras for	TB, BD

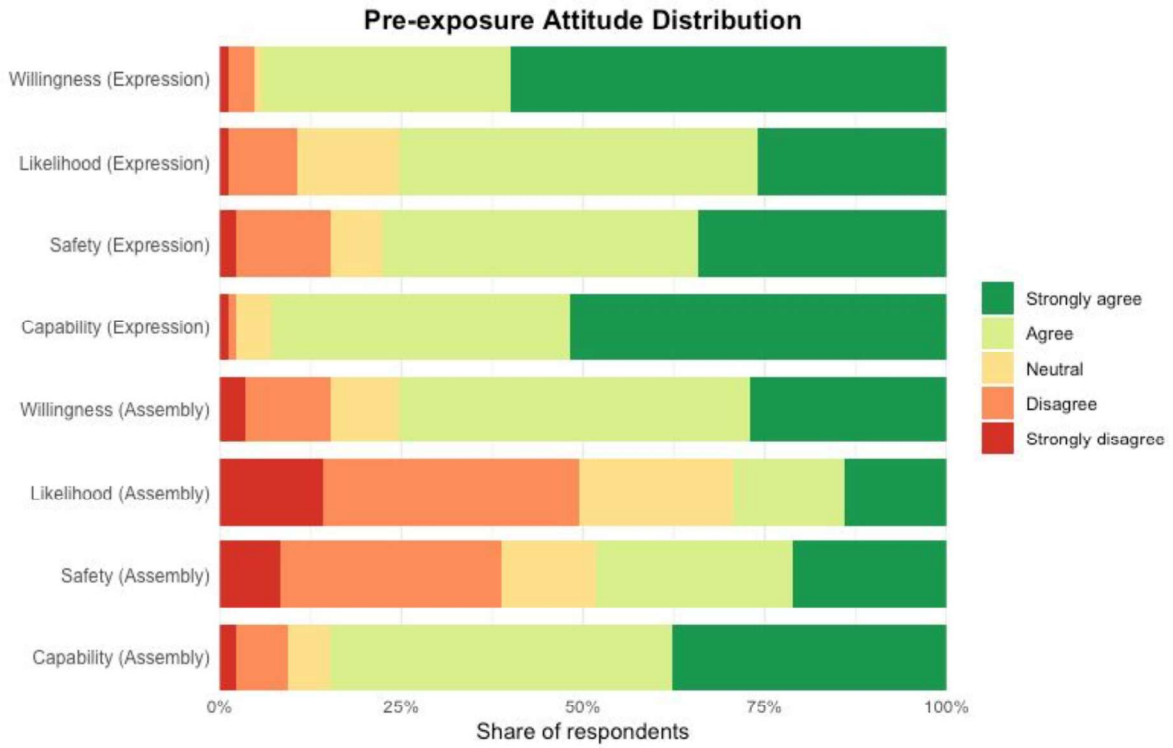
crowd control, and I was actually quite impressed by how effectively it was organized. It made me realize that, aside from safety, there can also be many other positive aspects to this kind of technology—like improving public order or efficiency in busy environments."	
"They should not be used for controlling dissent at all. they're use for retrospective identification of potential criminal actors is fine, as long as there is a human form of judgement present to prevent facial recognition biases."	CU, PS, BD
"Yes, particularly with student protests. The use of these camera footages can be used to enforce government and law enforcement upon students who want to express themselves through the form of protest or any form of activism. This is especially concerning when there are no damages to personal or private property."	PS
"In the current political climate, it seems more as technology that could aid in discriminatory practices or practices aimed at silencing political opposition."	PS, RR
"I feel that, within the subject of expressing yourself through assembly, FRT might feel intuitively wrong, but is a very logical next step in security given the technology we have access to today."	PS, CU
"Representative of the slide into fascism."	RR
"Not necessarily in the Netherlands; I think we're pretty well protected and our democracy is pretty well protected in a way that prohibits the government from using FRT for the (morally) wrong reasons."	IT
"I'm mostly concerned about the use of AI because of biases in the systems."	BD
"Abuse of this, especially since critique on government is increasingly labelled as something criminal."	PS, RA
"As I am reading up on the AI Act for different topics, I noticed that there is sometimes an incongruence with the risk in actuality and how the risk is assessed according to the legal framework. I worry that the data sets on which the FRT are trained contain biases which may consequently lead to more (legitimized) bias in law enforcement. Especially as a lot of the current protests revolve around Palestine and the police have historically been biased against foreigners."	BD, RA, PS
"Using it to gain information on where people live and then coming to people's houses and arresting them or "talking to them."	DP
"For now, I trust our government with its use, but it is hard to tell what a future government might do with it."	FM
"I am not concerned now because I have not heard of any cases where that has been a problem. So, it seems under control by the authorities."	IT
"I do not know much about the subject but how the use of FRT is intended, as described in this survey sounds to me like good intentions and safe, but if it is misused my opinion on it might change. Overall, I like the setting, and it seems like a nice way to modernise security in the Netherlands."	IT, RA
"Safe processing and storage of data. Whether citizens should have a right to know at which locations these cameras are in place. What the accuracy rate of the algorithms is (how effective is FRT at correctly locating and correctly identifying a suspect in a crime)."	DP
"I don't have any specific lack of faith or ethical or moral disagreements with the usage of FRT. I think that if regulated properly and those regulations are actually followed then I think that usage of FRT can be justified. That said, I have zero faith in the Dutch police to use it in a way I deem morally correct."	CU, RA, IT

Note. See Table 8 for the Thematic Coding Framework in terms of code abbreviations.

Figures

Figure 1

Pre-Exposure Attitude Distribution Diverging Stacked Bar Chart

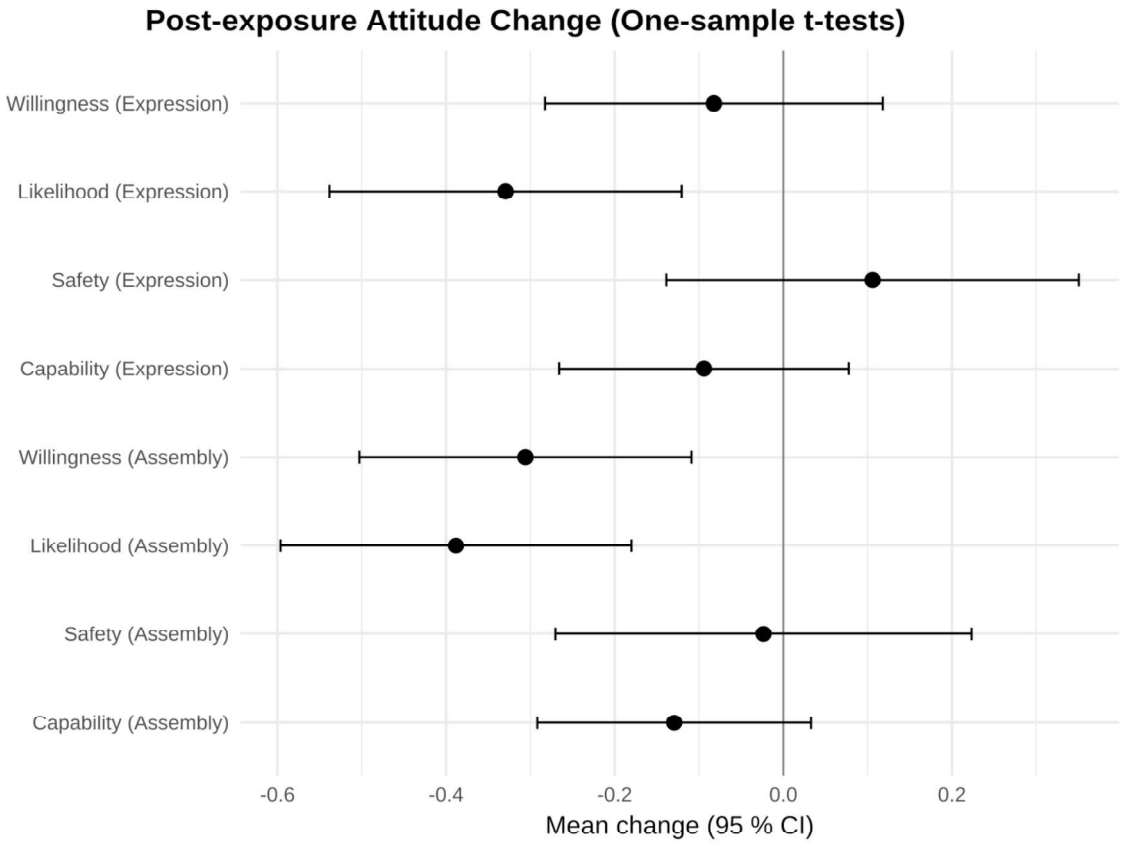


Note. Freedom of expression was referred to in the survey as "expressing myself (e.g. thoughts and opinions) in the Netherlands on matters that are important to me".

Note. Freedom of assembly was referred to in the survey as "assembling (e.g. participating in protests) in the Netherlands in support of matters that are important to me".

Figure 2

Post-Exposure Attitude Change (One-Sample t-Tests) Forest Plot



Note. See Figure 1 notes for the explanation and formulation of the variables in the survey.

Note. Respondents answered five-point Likert scale items from “extremely negative” to “extremely positive”, which were recoded to numeric values from -2 to +2, respectively.