Government Information Quarterly 40 (2023) 101761

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology

Genia Kostka [a,*], Léa Steinacker [b], Miriam Meckel [c]

[a] Institute of Chinese Studies, Freie University of Berlin, Berlin, Germany
[b] University of St.Gallen, St. Gallen, Switzerland
[c] Institute for Media and Communications Management, University of St. Gallen, St. Gallen, Switzerland

ARTICLE INFO

Keywords:
Facial recognition technology
Public opinion
Surveillance history
Privacy
China
US
Germany
UK

ABSTRACT

Governments around the world are adopting facial recognition technology (FRT) to improve public services and law enforcement. Past research has shown that such applications may result in discriminatory effects and threaten privacy. This study shines light on the question of what drives public opinion regarding FRT in different socio-political contexts. Based on an online survey and semi-structured interviews, this study finds that citizens in China, Germany, the United Kingdom, and the United States differ in their acceptance of the official public use of FRT. China has the highest approval rates, Germany and the US have the lowest, and the UK lies in the middle. Our results show that people are generally more willing to accept FRT in public spheres when they trust government institutions, believe the technology should be managed by the central government, and have an affinity for technology. People's awareness of a country's previous history of surveillance further shapes their perceptions of FRT. Across all four countries, we also show that privacy concerns, especially of FRT compromising one's privacy, have the biggest influence on respondents' attitudes. Expanding on existing research into FRT acceptance and usage, our results suggest that policymakers urgently need to address the current regulatory vacuum.

1. Introduction

Governments around the world use technologies like smartphones, geo-location tracking, meta-data collection, and applications of artificial intelligence (AI). On the one hand, these technologies promise to provide public services and law enforcement in order to solve urgent problems (e.g., traffic congestion, pollution control, and public security) more efficiently. On the other hand, the same technologies are also being utilized for mass surveillance, ethnic profiling, targeted repression, and privacy violations (Çelik, 2013; Gohdes, 2014; Gunitsky, 2015; Haraszti, Roberts, Villeneuve, Zuckerman, & Maclay, 2010; Xu, 2020).

One such rapidly spreading application is facial recognition technology (FRT), which matches a person's facial features from a digital image or video with identifying data. Besides FRT being installed in millions of mobile phones for access control, governments in >64 countries had also rolled out some type of FRT scheme by 2019 (Feldstein, 2019). Authorities employ FRT systems in widely different fields, including protection against crime and terrorist threats (Hamann & Smith, 2019; Interpol, 2021), border control (Mann & Smith, 2017), education (Article 192,021), and traffic management (Abacus, 2019; Su, 2019).

Researchers, policymakers, and digital activists caution against the speedy roll-out of the technology and point to substantial discriminatory effects and threats to privacy. Studies show that FRT may exacerbate systemic discrimination as people of color and transgender and non-binary individuals face disproportionate levels of tracking, judging, and inaccurate results (Braca, 2017; Rhue, 2018; Article 19, 2021). For example, research offers evidence of how FRT is employed against marginalized populations (Feldstein, 2019), including Muslim Uighur minorities in China's Xinjiang province (Leibold, 2020). Moreover, FRT is considered a major threat to individual privacy (Milligan, 1999), with the potential for "panoptic surveillance" (Gray, 2003; Introna & Wood, 2004). In 2021, Amnesty International started a global campaign, '*ban the scan,*' to prohibit the use of facial recognition scanning as it "amplifies racist policing and threatens the right to protest" (Amnesty International, 2021). The literature also points to the danger of "function creep," where technocrats transfer technologies beyond the initially intended practical goal to wider administrative and social areas (Article 192,021). All of these shortcomings have triggered a debate about what kind of regulation should be put in place to address the multiple

* Corresponding author.
E-mail address: genia.kostka@fu-berlin.de (G. Kostka).

https://doi.org/10.1016/j.giq.2022.101761
Received 27 August 2021; Received in revised form 25 August 2022; Accepted 7 September 2022
Available online 18 September 2022

shortcomings or whether the technology ought to be banned altogether (McCoy, 2002).

In this ongoing debate, the question of what drives public opinion regarding this considerable socio-technical shift is highly relevant. Yet, surprisingly little is known about how citizens perceive FRT in countries with varying socio-political contexts and a different history of surveillance. Our paper starts to fill this gap by addressing the following research questions: 1) How do people's perceptions of the use of FRT in the public sphere differ in the four countries? 2) How do political context, a country's history of surveillance, concerns about public issues, and personal traits and preferences influence individual attitudes toward FRT usage in public spheres?

The analysis is based on a mixed methods approach. First, we conducted an online survey of 6633 citizens in China, Germany, the United Kingdom (UK), and the United States (US) carried out between August and September 2019. The online survey resembles the Internet-connected population in the four selected countries and is weighted by age, gender, and region. In a second step, we conducted 22 semi-structured interviews with Chinese and German citizens in 2019 and 2020. The interviews allowed for cross-checking the results from the online survey (data triangulation) and offered a deeper understanding of the frames and narratives citizens adopt to explain their particular attitudes toward FRT.

China, Germany, the UK, and the US were selected because of a range of relevant factors. First, they constitute a politically diverse group, including a one-party authoritarian state, a federal parliamentary republic, a parliamentary constitutional monarchy, and a presidential republic, allowing us to study different political contexts. Second, governments in these countries have tested out FRT systems, ensuring that FRT would be a relevant subject of study in each country. China has most strongly embraced government applications of FRT by, for instance, equipping highway toll booths with facial recognition cameras to detect drivers who evade highway fares (Ji, Guo, Zhang, & Feng, 2018), equipping schools to monitor pupil attendance (Article 192,021), or using it for targeted surveillance in provincial pilots to track journalists and international students (IPVM, 2021). During the COVID-19 pandemic, China used FRT to enforce quarantine rules (Roussi, 2020). In the US, the adoption of FRT is also spreading, albeit not as fast as in China (Prakash, 2018): The FBI's facial recognition database currently includes 641 million images that can be searched without an official warrant (Harwell, 2019). In the UK, police departments experimented with live face-tracking (Satariano, 2019), whereas in Germany, a country where the topic of data privacy is especially prominent in public debate, the FRT roll-out is limited and adoption is confined to major airports that integrate FRT for identity verification.

Our analysis draws on technology acceptance literature (Davis, 1989; Venkatesh & Davis, 2000; Venkatesh, Morris, Davis, & Davis, 2003), privacy calculus theory (Dinev & Hart, 2006; Wadle, Martin, & Ziegler, 2019), and the trade-off model of privacy and security (Davidinev & Silver, 2004; Pavone & Degli-Esposti, 2012). We show that citizens are more willing to accept FRT in public spheres when they have trust in government institutions, believe the technology should be managed by the central government, and have a general affinity for technology. People's awareness of their country's previous history of surveillance results in them being less accepting of FRT, which expands existing research on technology acceptance and usage (Venkatesh et al., 2003). One main finding is that privacy concerns have the largest influence on respondents' (non-)acceptance of FRT in all four countries, suggesting that policymakers need to quickly address these concerns by closing the current regulatory vacuum and informing their citizens of privacy implications.

Our findings contribute to a growing body of literature on digital technologies and surveillance (e.g., Lyon, 2007; Lyon, 2017; Xu, Kostka, & Cao, 2021). As FRT applications transform people's economic, political and social lives, understanding how citizens perceive them and to what extent they approve of how their governments use them is important. Our online survey shows that acceptance of FRT uses in public spheres varies in different socio-economic and political contexts and is influenced in each country by citizens' trust in institutions and awareness of surveillance history in the past. The findings also add to the privacy calculus literature as we find in all four countries that citizens are especially critical of public uses of FRT when they fear *personal* privacy risks resulting from it. Citizens who believe FRT use by governments leads to privacy violations in general but does not affect their personal privacy are also critical but to a lesser extent. This seems to suggest that privacy concerns have a particularly strong impact on public opinion if people feel personally affected.

The paper is structured as follows: Section 2 reviews previous studies on public attitudes toward FRT and presents the conceptual framework. In Section 3, we summarize the design and data collection processes for the online survey and semi-structured interviews. This is followed by the results and a discussion in Section 4 before we conclude and offer policy implications in Section 5.

2. Literature review

In previous research, various models have been developed to measure the diverse influences on an individual's tendency to accept new technologies, including the technology acceptance model (TAM) and its extensions (TAM 2, TAM 3) and the unified theory of acceptance and use of technology (UTAUT) (Davis, 1989; Venkatesh et al., 2003; Venkatesh & Davis, 2000). These models were initially developed to assess the acceptance of information technology. While they are a good starting point for this research, some aspects of these models seem less relevant for a study of FRT acceptance. We also make use of the growing literature on privacy calculus theory (Dinev & Hart, 2006; Wadle et al., 2019), the privacy–security trade-off (e.g., Davidinev & Silver, 2004; Miltgen, Popovič, & Oliveira, 2013), and surveillance studies (Gray, 2003; Lyon, 2017). Drawing on these different literature strands, we construct a combined conceptual model that is technology-specific but can be applied to diverse national contexts.

2.1. Public attitudes toward FRT

Previous research points to varying public attitudes toward FRT in the four selected countries. In China, evidence suggests that citizens accept or even support digital surveillance (Kostka, 2019; Liu, 2022; Xu et al., 2021). Research on FRT shows that surveillance and control are not front and center in the minds of people in China when it comes to facial recognition systems, but notions of convenience, efficiency, and improved security are (Kostka, Steinacker, & Meckel, 2021). Public discussions are generally more positive about the state's use of FRT but less accepting of the technology's application by the private sector (Brown, Statman, & Sui, 2021). Existing research on FRT acceptance highlight that Chinese citizen show growing concerns about privacy (Kostka, Steinacker, & Meckel, 2021), and in a poll of 6100 Chinese citizens regarding FRT, 83% indicated that they would like to have more control over their data (The Nandu Personal Information Protection Research Center, 2019).

For Germany, insights into public opinion and FRT can so far only be found in studies assessing citizens' acceptance of surveillance technologies more generally (Heek, Julia, & Ziefle, 2017). A 2016 survey of 2083 Germans showed that 60% of respondents believed increased video surveillance in public spaces is reasonable (Wichmann, 2016). In 2019, another survey with 671 Germans found that 50% of the respondents would agree with the official use of automated facial recognition under strict conditions, while 22% wanted to ban FRT completely, 11% were unsure or did not answer, and 17% favored an unlimited use of the technology (Mičijević, 2019).

For the UK, a survey of 4109 people (Ada Lovelace Institute, 2019) found that most respondents feared the normalization of surveillance but would accept FRT when there is a clear public benefit and certain

restrictions are in place; 49% of the respondents supported the use of FRT by the police if appropriate safeguards are insured, whereas the majority of them were against its use in schools (67%) or on public transport (61%), and even more opposed the use of FRT by companies for commercial benefit, like customer tracking in shops (77%).

For the US, a survey by the Pew Research Center found that 56% of the 4272 respondents trust law enforcement agencies to use FRT responsibly, while 36% trust technology companies and 18% trust advertisers, which demonstrates that acceptance differs depending on who is employing the technology (Smith, 2019). Another study by the Center for Data Innovation, which polled 3151 US citizens, found that only a minority of 26% wishes for strict governmental limitations on the use of FRT, and even fewer (18%) would want to limit the technology if it is used at the expense of public safety (Castro & McLaughlin, 2019). Another study examining FRT in police body cameras also finds that respondents generally approved of this application, especially women and Trump voters (Bromberg, Charbonneau, & Smith, 2020).

Overall, these findings offer insights into public attitudes, but as single-country case studies, they do not point to international differences. Cross-country studies on FRT are scarce. One exception is Kostka, Steinacker, & Meckel, 2021, a study using the same dataset but focused on both public and private uses of FRT, and perceptions of the risks and benefits. The study finds that people's perceptions of benefits (e.g., improved security or notions of convenience) override concerns about surveillance and control in the four countries. In this present study, we use the same dataset but focus only on public uses of FRT and study the political context and surveillance history rather than the perceived risks and benefits in general.

2.2. Political context and attitude

A country's political context strongly influences the acceptance levels of digital technologies. Trüdinger and Steckermeier (2017) show that, in the case of Germany, there is a positive relationship between people's political trust and their acceptance of government surveillance technologies. Pavone and Degli-Esposti (2012) and Degli-Esposti and Gómez (2015) also find that in Spain, citizens who trust political institutions perceive surveillance technologies as security-enhancing, while those who mistrust their government regard these technologies as mainly privacy-infringing. In their study of public attitudes toward FRT in the US, Brewer, Bingaman, Dawson, Painstil, and Wilson (2021) find a significant relationship between citizens' support for the development of FRT and their trust in government. In other words, whether citizens trust their government or political institutions is a critical factor in understanding public attitudes toward FRT. The findings point toward acceptance of FRT use in the public sphere being higher among citizens who have more trust in government (H1).

Studies have found that citizens trust certain providers more to handle biometric technologies (Krol, Parkin, & Sasse, 2016). For instance, a UK study on biometrics surveying 282 participants found that respondents are more comfortable with biometric data being stored by a government than by a company (Buckley & Nurse, 2019). Surveys on FRT also find that citizens in the US and UK trust law enforcement agencies or government actors more than advertisers or commercial companies (Ada Lovelace Institute, 2019; Smith, 2019). In China, citizens also show a preference for government agencies as the main provider: A study on China's social credit system found that 77% of respondents trust the central government and 48% their local government to use personal data most responsibly, while only 8% believe the same of private enterprises (Kostka, 2019). Based on these findings, we hypothesize that acceptance of FRT use in the public sphere is higher among citizens who support the central government as an FRT provider and manager (H2) and support local governments as FRT providers and managers (H3).

2.3. Surveillance history

A country's previous history with government surveillance further influences public opinion (Samatas, 2005). Among the four countries in our study, China and (East) Germany have a recent history of government surveillance in the service of political repression. During the Cultural Revolution, Chinese leaders relied on human informants to spy on citizens and created a pervasive atmosphere of fear to ensure public support for the Chinese state and, in particular, Mao Zedong. After Mao died in 1976, China continued to use surveillance methods to prevent opposition to the Chinese Communist Party's rule. In East Germany, the State Security Service (known as the "Stasi") also utilized an extensive system of informants and spies to control the population.

These previous experiences with state surveillance likely affect citizens' attitudes toward new digital technologies; however, existing studies come to different conclusions about how it does so. Samatas (2005) finds that older Greeks who previously experienced authoritarian surveillance are more indifferent toward surveillance and the direct monitoring of people. He explains: "Having experienced some of the most immediate and transparent forms of repressive surveillance, they find it hard to become agitated by the new amorphous surveillance infrastructure, where surveillance is used for a multitude of purposes, many of which are commercial" (Samatas, 2005: 189). By contrast, Freude and Freude (2016) argue that previous surveillance practices during World War II in East Germany have resulted in higher-than-normal concerns for Germans about data privacy and surveillance by the government. We follow this argument and assume that these collective memories and current experiences of government surveillance will negatively affect citizens' attitudes. Thus, we hypothesize that FRT acceptance is lower among citizens who are aware that their government previously used surveillance in a negative way (H4).

2.4. Concerns about public issues

Existing research further shows that a nation's socio-political context significantly shapes the acceptance of digital technologies and surveillance (Kostka, Steinacker, & Meckel, 2021; Samatas, 2005). Citizens' concerns are shaped by different issues in their country, and the severity of such concerns potentially influences their views of FRT. Depending on the context, citizens might be more or less concerned about violations of rules and regulations, crime, terrorist threats, border control, or socially unacceptable behavior. Trüdinger and Steckermeier (2017), for instance, show that, besides political trust, the fear of crime and terrorism fosters an acceptance of surveillance practices in Germany. Recent research conducted in the UK and US also finds that support for police use of FRT is higher when respondents are told it is used to identify potential terrorists or those wanted for serious violent crimes (Bradford, Yesberg, Jackson, & Dawson, 2020) or when respondents have general concerns about public security and crime (Castro & McLaughlin, 2019). In addition to terrorism and crime, we also add concerns about violations of rules and regulations, border control, and socially unacceptable behavior in our survey to reflect the range of FRT adoption in China, including employing FRT in education or traffic control sectors. We assume that acceptance of FRT use in the public sphere is higher among citizens who have concerns about public issues. We divide public issues into the following concerns: violation of rules and regulations (H5), crime (H6), terrorist threat (H7), border control (H8), and socially unacceptable behavior (H9).

2.5. Individual preferences and traits

The literature on the privacy calculus and the privacy–security trade-off stresses that individual attitudes toward digital technologies are preceded by a decision-making process – a calculus or trade-off – where individuals weigh the benefits against the risks or costs associated with a particular technology (Davis & Silver, 2004; Dietrich & Crabtree, 2019;

Dinev & Hart, 2006; Pavone & Degli-Esposti, 2012). The general notion of the privacy–security trade-off is that citizens understand the risks and benefits associated with FRT and accept that the state violates personal freedoms or invades privacy in exchange for delivering on the promise of greater security (Dietrich & Crabtree, 2019). Nissenbaum (2004) stresses the importance of contextual factors such as norms and values on privacy preferences. While the privacy literature has looked predominantly at privacy in terms of having an intrinsic value and is a non-negotiable element in Western democracies, recent research suggests that in China, privacy has more of an instrumental value: Privacy is seen as instrumental to larger social goals such as maintaining social order (Kostka, Steinacker, & Meckel, 2021; Zhang, Guo, Deng, Fan, & Gu, 2019). A recent study on the COVID-19 contract-tracing app finds a rich variety of attitudes toward surveillance and privacy issues in China (Liu & Graham, 2021). The study highlights a whole range of privacy issues, including citizens feeling "fatalism to the possibility of privacy," "privacy tradeoffism," privacy protectionism, and "not (that) private." In our survey, we study citizens' privacy concerns and include two different measures: one measure of general concerns about FRT resulting in privacy violations and one more specific measure with regard to concerns that FRT threatens people's individual privacy. We hypothesize that acceptance of FRT use in the public sphere is lower among citizens who perceive FRT as a threat to privacy in general (H10) and to their individual privacy in particular (H11).

A large body of research has also provided evidence that attitudes toward technology are a key factor influencing the adoption of new digital technologies and innovations. Citizens with an affinity for technology are often classified as "technology optimists," while those with an aversion to technology are "technology pessimists." Findings show that technology optimists are more likely to accept the Internet and other innovations (Edison & Geissler, 2003; Modahl, 1999) and to be technology-affine (Edison & Geissler, 2003). Liu and Graham (2021) also find that general technology attitudes are important to explain citizens' views on contact-tracing apps in China. Their interviewees expressed a variety of attitudes toward technology ranging from "trust in technology" and "doubting the algorithm" to "doubting the data." For this study, we also aim to study the influence of technology affinity, and we follow Edison and Geissler's definition of technology affinity or attitude "as positive affect toward technology (in general)" (Edison & Geissler, 2003:140). As a crude measure, we developed a *technology affinity index* that includes respondents' beliefs in FRT reliability, beliefs that FRT represents a desirable future, and a measure of how frequently one has used FRT in either the private or government spheres. We hypothesize that acceptance of FRT use in the public sphere is higher among citizens who are more "tech-affine" (H12).

Based on these studies, we derive a conceptual framework with political context and attitude, country-specific history of surveillance, and concerns of public issues as the key variables to explain variations in the social acceptance of public use of FRT. We use various sociodemographic factors, including age, gender, income, education, ethnic group, and living in urban and rural areas, as control variables. Fig. 1 summarizes our conceptual framework.

3. Methodology

This study uses an online survey and in-depth interviews to explain variations in citizens' attitudes toward the use of FRT in public spheres. This mixed methods approach offers numerous advantages. First, the interview data provided a means of checking the findings on overall FRT acceptance from the online survey. Second, interviews allowed for deeper inquiry into the explanatory variables and helped us identify frames and narratives citizens adopt to explain their particular attitudes toward FRT.

3.1. Survey data

A Berlin-based survey firm cooperated with mobile app and website providers in China, Germany, the UK, and the US to conduct a large online survey in the four countries between August and September 2019. We used "river sampling" as our sampling method, drawing participants from a base of between 1 million and 3 million users.[1] From a network of >40,000 participating apps and mobile websites, the firm recruited respondents through >100 apps for our survey, including different topics and formats such as shopping (e.g., Amazon), photo-sharing (e.g., Instagram), lifestyle (e.g., DesignHome), and messaging (e.g., Line). Participants were offered small financial and non-monetary rewards as an incentive to join, such as premium content, extra features, and vouchers. Participants did not know the topic of the survey before opting in to participate and underwent a pre-screening that included questions on socio-demographics and a test to ensure they (and not a machine) answered the survey. After successful pre-screening, the participants were directed to our survey.

Our survey consisted of a total of 36 questions grouped into several dimensions: individual characteristics and beliefs (14 questions), political attitudes and context (six questions), perceived functions of FRT (six questions), perceived social norms (five questions), and institutions and media (five questions). A professional translation company translated the survey questions and the authors double-checked translations with the help of native speakers. The authors also piloted and improved the survey with 100 respondents in each country before its full launch. The rate of participants who fully completed the survey was 70% (China), 73% (Germany), 69% (UK), and 67% (US), respectively. The average time participants spent on the survey was 9.75 min. Several consecutive identical answers or disproportionately short periods for completion of a questionnaire prompted invalidation. This cleaning method provided us with a final sample size of 6633 respondents.

The survey is a non-probability online survey using quota sampling based on age (18–65), gender, and region. Sampling quotas were created from population statistics published by Barro Lee Census Population Data (2017) and adjusted for the Internet penetration data published by Pew Global Attitudes Survey (2017) and regional statistics for China from Statistica (2016). Thus, the sample resembles the Internet-connected population – meaning slightly younger and maybe more technology-affine than the overall population. In China, regional samples included quotas for the three main regions of China: Central (37%), Western (21%), and Eastern (42%). In the other countries, equal attention was paid to ensure accurate representation of local regions, including adequate representation of federal states in Germany, counties in the UK, and states in the US. The maximum weight was 1.8, and the overall margin of error for estimates is 2.4% for China and Germany and 2.5% for the UK and the US. In the Appendix, Table A1 provides an overview of the sample populations, and Table A2 details summary statistics.

We used Software R for ordered logistics regression for the analysis. Our dependent variable of interest is "social acceptance of the public use of FRT." The question reads: "*Do you accept or oppose the use of facial recognition technology in the public sphere*?" The possible responses were *strongly oppose*, *somewhat oppose*, *neither oppose nor accept*, *somewhat accept*, and *strongly accept*. We investigated levels of acceptance by studying different political contexts and attitudes, a country's history of surveillance, concerns about public issues, and individual preferences and traits concerning privacy and technology affinity. Table 1 lists the measurements and hypotheses related to our selected dependent and independent variables. We control for people's age, gender, city,

[1] River sampling allows both first-time and regular survey-takers to participate. The method does not include a fixed number of potential survey respondents, as the survey is displayed on offer walls within apps and websites and can, thus, reach millions of users.

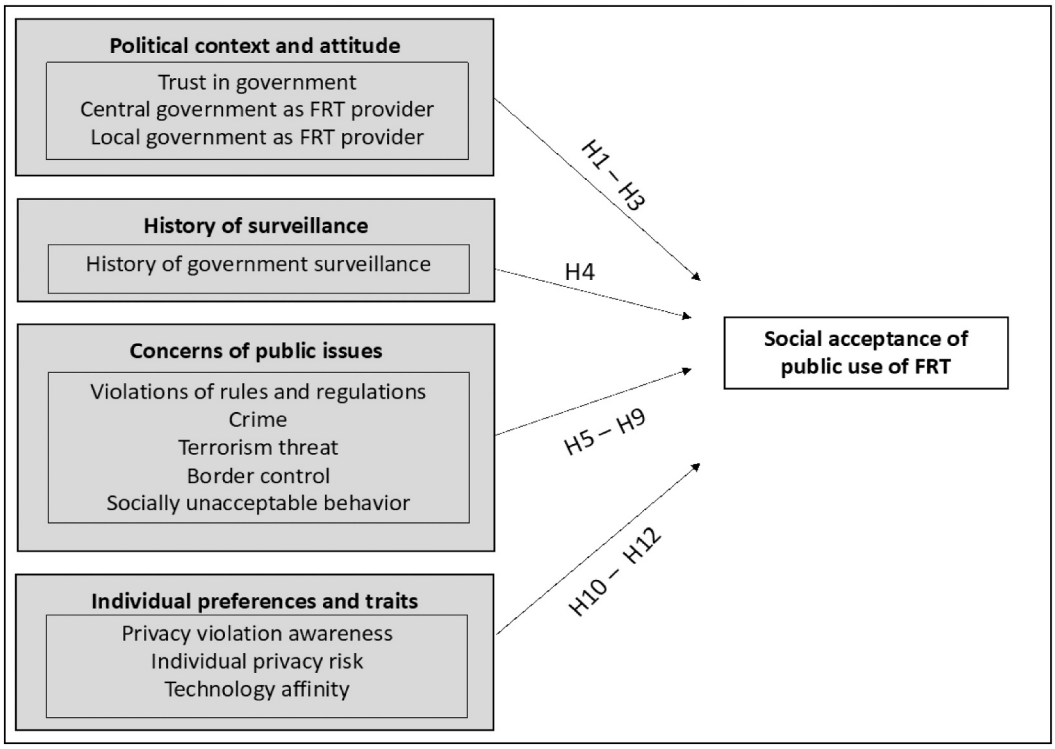

Fig. 1. Conceptual framework.

ethnicity, education, and income. Out of the 6633 respondents in our sample, 8.1% ($N = 535$) had "never heard about FRT" before taking the survey. We *excluded* these respondents from our analysis, which left us with 6099 citizens: 1628 in China, 1538 in Germany, 1524 in the UK, and 1409 in the US.

3.2. Interview data

The analysis also includes 22 semi-structured interviews with Chinese and German citizens conducted between November 2019 and January 2020 to gain insights into the frames and narratives citizens adopt to explain their particular attitudes toward FRT. We chose China and Germany because the survey showed stark differences in FRT acceptance in both countries and because the authors' language abilities and networks allowed access to informants there. We used personal networks and the snowball method to select informants from somewhat diverse backgrounds in terms of age, gender, and region/city size. By relying on different 'entry points' in our personal networks in different regions, we sought to minimize the biases of the snowball method. Table A5 in the Appendix provides more detailed information on the sample. The 22 interviews include 11 interviews in Germany and 11 interviews in China. Every time, the interviews were conducted by a single individual either in person or via telephone calls in Chinese or German. On average, the interviews lasted 60 to 90 min and were not recorded so as to protect the informants' identities as much as possible. The interview questionnaire included questions on knowledge and usage of FRT (four questions), general attitudes toward FRT (five questions), knowledge and views on the country's use of surveillance in the past, and privacy issues (five questions). The questionnaire also incorporated several open-ended questions to give interviewees room to share their thoughts and reflections. We took detailed notes, translated them into English, and used manual coding. For the coding, we first identified all mentioned themes and narratives and then analyzed the frequency of these themes in the interview materials.

4. Results

4.1. Acceptance of public use of FRT

Our survey finds that acceptance of public use of FRT varies across countries, with 51% of Chinese respondents showing the highest level of acceptance, while only 37% of their American and 38% of their German counterparts strongly or somewhat accept FRT for public use. The UK responses are in between, with 42% of respondents expressing acceptance of the technology. Opposition to FRT shows interesting cross-country variation. While a rather low share (i.e., 22%) expressed either some or strong opposition to FRT in China, the share is much higher in Germany (38%), the UK (33%), and the US (37%). Fig. 2 summarizes the levels of acceptance by country.

Within individual countries, there are regional variations in FRT acceptance, as summarized in Fig. 3. In China, 54% of citizens living in the more economically developed eastern part of the country somewhat or strongly accept FRT in public spheres, while this rate is lower for the central and western regions with 50% and 44%, respectively. That the more educated and affluent population more strongly supports surveillance technologies has also been found in previous studies in China (e.g., Kostka, 2019; Liu, 2022). The more affluent or educated part of the population, which proportionally lives in Eastern China, possibly perceives trust issues in society to be more severe (Wu & Shi, 2020) and might believe that FRT uses in public spheres result in higher security (Authors). Moreover, as previous research has shown, surveillance technologies are more heavily enforced on socially disadvantaged groups (Lyon, 2018). In Central and Western China, the population is more ethnically diverse, and a higher share of the population lives in rural areas; they are often stigmatized as being uncivilized and prone to crime (Murphy, 2004; Liu, 2022). Thus, ethnic profiling and social exclusion in China might explain the lower support for FRT uses in public spheres in Central and Western China. In Germany, acceptance seemed slightly higher in the East (the former GDR), with 42% either somewhat or strongly accepting the technology as compared with 38% in the West. Given East Germany's history with Stasi surveillance

Table 1
Measurements and hypotheses.

Category	Measurement	Hypothesis
Dependent variable: Social acceptance of the public use of FRT		
Acceptance of FRT in the public sphere *Do you accept or oppose the use of facial recognition technology in the public sphere?*	*1 = Strongly oppose, 2 = Somewhat oppose, 3 = Neither oppose nor accept, 4 = Somewhat accept, 5 = Strongly accept*	H0: Acceptance of FRT use in the public sphere is higher among citizens who live in a democracy.
Political context and attitude		
Trust in government *How much do you trust government institutions in your country?*	*1 = Not at all, 2 = Very little, 3 = Somewhat, 4 = A lot, 99 = Prefer not to answer* *Dummy: 0 = Not at all/ Very little/Somewhat/ Prefer not to answer, 1 = A lot*	H1: Acceptance of FRT use in the public sphere is higher among citizens who have more trust in the government.
Support government as FRT provider *In which of the following cases do you support the use of FRT? When it is managed by…*	*1 = Local government, 2 = Central government, 3 = Private companies, 4 = Public-private partnerships, 5 = None of the above* *Dummy: 0 "No," 1 "Yes"*	H2: Acceptance of FRT use in the public sphere is higher among citizens who support the central government as FRT provider/manager. H3: Acceptance of FRT use in the public sphere is higher among citizens who support the local government as FRT provider/manager.
History of surveillance		
History of government surveillance *Do you think the government in your country has used surveillance against its own citizens in a negative way in the past?*	*0 = No, 1 = Yes, 99 = Don't know; for regression dummy variable: 0 = No/ Don't know, 1 = Yes* *Dummy: 0 "No/Don't know," 1 "Yes"*	H4: Acceptance of FRT use in the public sphere is lower among citizens who think their government has negatively used surveillance against its own citizens before.
Concern about public issues		
Issues of concern *Are you concerned with any of the following issues in your country?*	*Violation of rules and regulations* *Crime* *Terrorist threats* *Border control* *Socially unacceptable behavior* *For each of the concerns listed above: 0 = No, 1 = Yes*	H5–H9: Acceptance of FRT use in the public sphere is higher among citizens who are concerned about (5) the violation of rules and regulations, (6) crime, (7) terrorist threats, (8) border control, and (9) socially unacceptable behavior in their country.
Individual preferences and traits		
Privacy violation awareness *Do you think FRT increases privacy violations?* **Individual privacy risk** *Do you think FRT poses a threat to your privacy?*	*Privacy violation awareness:* *Dummy 0 = No; 1 = Yes* *Individual privacy risk:* *Dummy 1 = No, 2 = Maybe, 3 = Yes, 99 = Don't know*	H10: Acceptance of FRT use in the public sphere is lower among citizens who believe FRT increases privacy violations. H11: Acceptance of FRT use in the public sphere is lower among citizens who perceive FRT as posing a threat to their own privacy.
Technology affinity *Use frequency: How often do you use facial recognition technologies (e.g., on your smartphone)?* *Reliability: Do you think FRT is more reliable or less reliable than other identification methods (e.g., fingerprints, identity cards)?* *Desirable future: Do you think FRT represents a desirable future?*	***Combined variable: FRT use frequency (5–7) + reliability (1) + desirable future (1)*** ***FRT Use frequency:*** *1 = Never, 2 = Several times in my life, 3 = Several times a year, 4 = Several times a month, 5 = Several times a week, 6 = Most days, 7 = Everyday* ***FRT is reliability perception:*** *1 = More reliable, 2 = Neither more nor less reliable, 3 = Less reliable, 99 = Don't know* *(Dummy: 0 = Neither more nor less reliable/Less reliable/don't know, 1 = More reliable)* ***FRT presents a desirable future:*** *1 = Yes, 2 = No, 99 = Don't know* *(Dummy: 0 = No/don't know, 1 = Yes)*	H12: Acceptance of FRT use in the public sphere is higher among citizens who are "tech-affine."

methods, this slightly higher positive attitude is surprising. Berlin's results were reported separately, as it includes both the former West and East Berlin; the acceptance level was 39%. In the UK, the highest acceptance can be found in Scotland, with 43% of citizens either strongly or somewhat supporting FRT in public spheres, followed by England (42%), Greater London (40%), Northern Ireland (36%), and Wales (35%). Opposition to FRT is particularly strong in Northern Ireland and Wales, with 18% and 15% of respondents, respectively, strongly opposing the technology. Acceptance levels in the US are high in the South (39%) and Midwest (38%) but lower in the Northeast (35%) and West (32%).

4.2. Effects on FRT acceptance

Our hypotheses generated a range of predictor variables related to political context and attitudes (H1−H3), the role of history with surveillance (H4), country-specific concerns of public issues (H5–H9), and individual preferences and traits (H10−H12). We used ordered logit regressions for our analysis (Fig. 4). Our focus was on respondents who indicated they were aware of FRT (N = 6099) to ensure a basic frame of reference for the subject matter of the study. In the Appendix, we also present the regression results for the total sample in Fig. A1, adding a dummy variable for democracy (H0). The variable for democracy is not significant, which suggests that variables other than political regime type have greater explanatory power to explain FRT acceptance levels. Tables A3 and A4 in the Appendix report on generalized variance inflation factors (GVIFs) and Goodness of fit tests.

Our analysis finds that trust in the government has a significant positive association with FRT acceptance in public spheres in China, the UK, and the US; thus, the higher the trust in government, the more accepting respondents are toward the use of FRT in the public sphere, which supports H1. Germany is an outlier here as we cannot find a significant relationship between trust in the government and acceptance of FRT uses in public spheres. This might be because of potentially negative associations with state surveillance given its history; even if Germans trust their government (to do its job), surveillance is a no-go for many. For all four countries, we find that acceptance of FRT uses in the public is higher among citizens who support the central government as the FRT provider, with Germany, the UK, and the US showing a significant relationship, thus supporting H2. For China, the UK, and the US, there is also a significant positive association between FRT acceptance and citizens who support local governments as the FRT provider, which means H2 is supported. We conclude that, in general, trust in the government and its role as an FRT provider leads to higher acceptance of

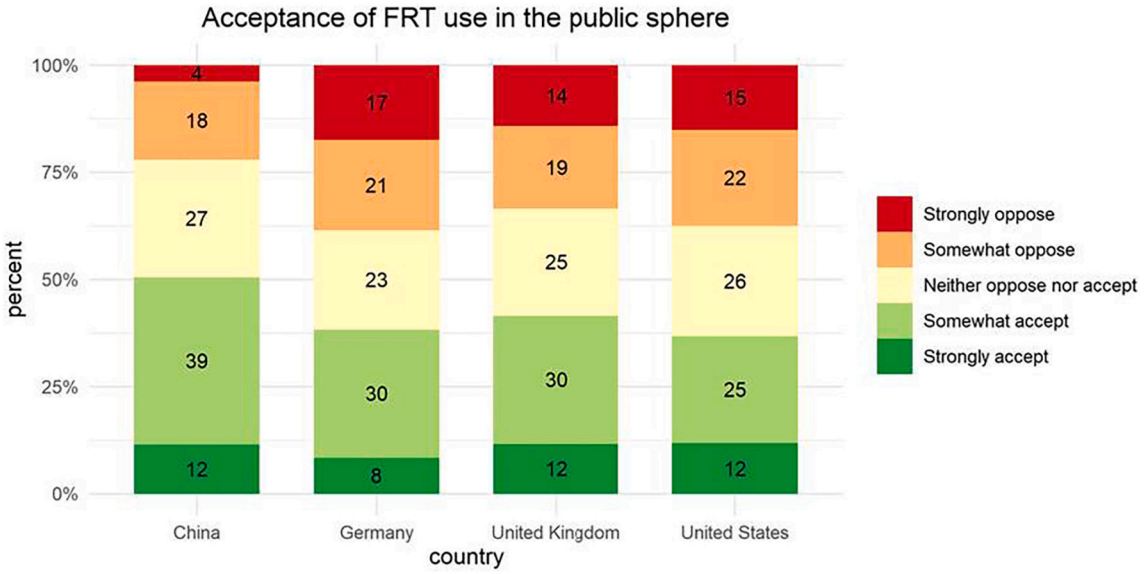

Fig. 2. Acceptance of FRT use in the public sphere.
Note: China = 1628, Germany = 1538, UK = 1524, US = 1409, weighted.

FRT uses in public spheres.

Another explanatory factor is respondents' awareness of past use of government surveillance. For all countries, we find that acceptance of FRT uses in public is lower among citizens who think their government has previously used surveillance in a negative way, with a significant association in Germany and UK, which partially supports H4.

Our model also looked at the role played by respondents' concerns about particular public issues. The results show there is no significant relationship in any of the countries between concerns about violation of rules or concerns about crime and acceptance of FRT use in public; thus, we cannot find support for H5 and H6. Concerns about terrorism threats show a positive association in all four countries, with significant positive associations in Germany, the UK, and the US, which supports H7. Concerns about border control have a positive but insignificant association with FRT acceptance in public spheres; thus, H8 is not supported. Concerns about socially unacceptable behavior are positively associated with FRT acceptance in Germany but insignificant for the other three countries, thus partly finding no support for H9.[2]

Finally, our findings show that individual preferences and traits concerning privacy and technology affinity are the most important factors explaining the variance in FRT acceptance rates. We find that acceptance of FRT use in the public sphere is lower among citizens who generally perceive privacy violations from FRT usage, with a significant negative relationship for all four countries, supporting H10. Interestingly, in all four countries, the negative association is the highest for perceived threats to one's personal privacy compared with perceived threats to privacy violations in general. This suggests that respondents are more likely to oppose FRT in public if they perceive possible infringements of their *own* privacy, supporting H11. Technology affinity is another important explanatory variable: Except for Germany, where we find no significant relationship, it is strongly and positively linked to FRT acceptance in China, the UK, and the US, which supports H12. We also included various sociodemographic variables as control variables; most are not significantly associated with acceptance, except for gender and education in Germany. Table 2 summarizes the findings for the individual hypotheses by country. Interestingly, the hypotheses on privacy threats – in terms of both general awareness and perceived personal privacy risks – are the only factor that can be supported in all four countries.

4.3. Common frames based on interviews

To triangulate the findings from our survey and to further investigate how people make sense of FRT, we conducted 22 in-depth semi-structured interviews in China and Germany. As acceptance of FRT use in public was the highest in China and very low in Germany, we selected the more extreme cases to study citizens' beliefs and preferences. Interviewees in both countries reported similar levels of acceptance as expressed by the survey respondents but highlighted a rich variety of different narratives and opinions about the perceived risks and opportunities of the public use of FRT. Interpretations of the influence of local surveillance histories on attitudes of trust in actors, technology, and privacy varied. These frames are not comprehensive or exclusive, as one interviewee can express multiple narratives, but they illustrate common narratives expressed during the interviews. Table 3 summarizes the most common frames, and Tables A6 and A7 in the Appendix offer key summaries of the interviews.

4.3.1. Common frames in China

4.3.1.1. Technology advocates. A common response among interviewees in China was to self-identify as "true believers in FRT benefits" and to express a generic faith in technological progress. Many interviewees voiced a strong belief that the central and local governments' use of FRT in public places increases security. One interviewee noted: "The extensive use of FRT by customs and the Public Security Department is a prime example of technology benefiting our society by making it more secure" (Int_CN_001). Interviewees frequently cited specific examples of how FRT has helped fight crimes, as noted by the following interviewee:

> It's become relatively safer now since the digitization [and use of FRT]. Earlier, it was more chaotic. For example, there were people who went to university with a fake identity and still got away with it. Since digitization, such behavior has become impossible. Also, many

[2] For China, concerns about public issues seem to play an insignificant role in explaining varying FRT acceptance levels among Chinese citizens. Instead, previous research suggests that beliefs in greater convenience and improved efficiency are key factors influencing Chinese respondents' attitude toward FRT. This indicates that personal benefits are more highly valued than benefits like improved public security (Kostka, Steinacker, & Meckel, 2021).

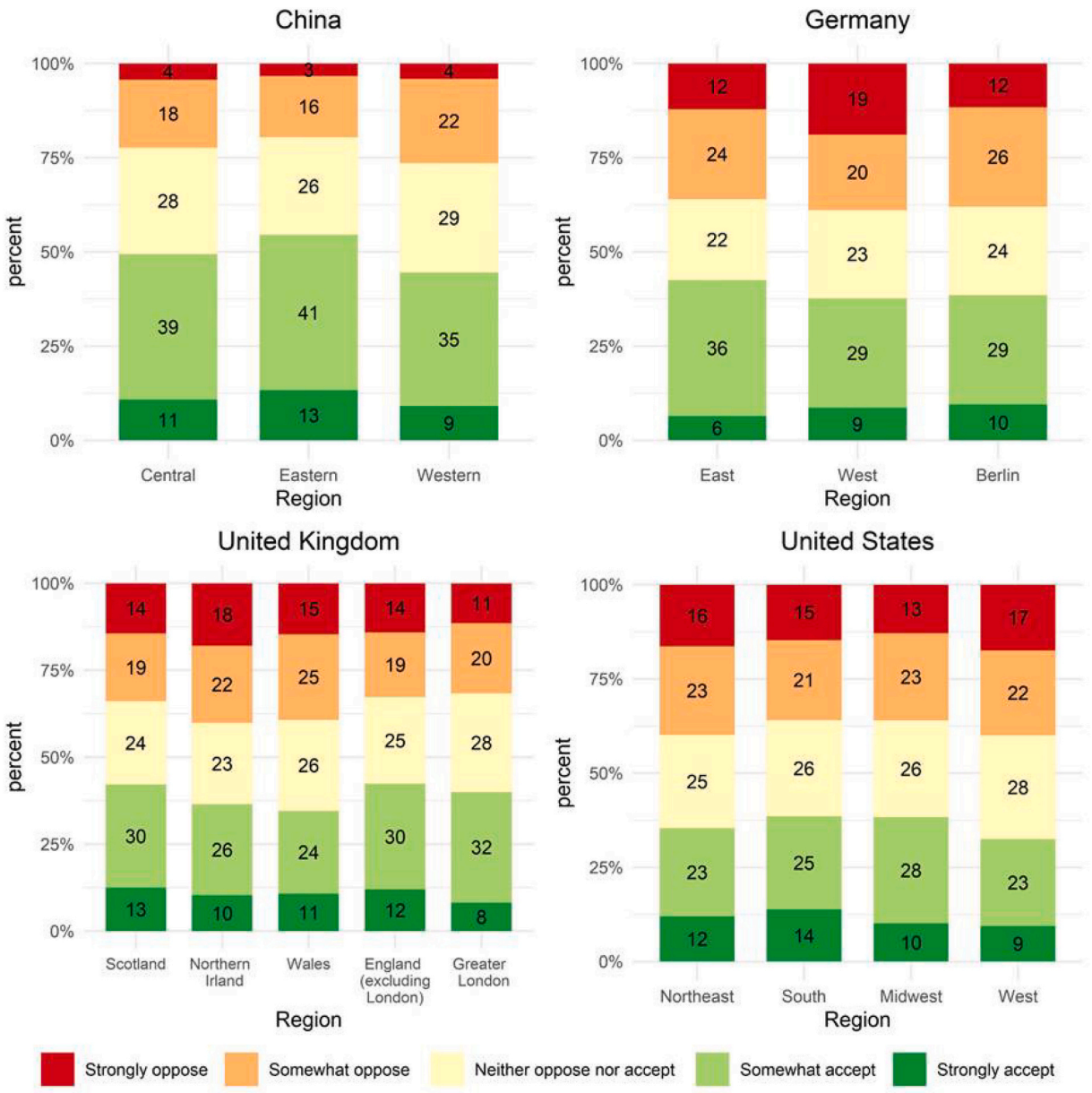

Fig. 3. Acceptance of FRT use in the public sphere by regions.
Note: Total N = 6099. Distributions vary for regions: in China Central, N = 601; East, N = 686; West, N = 341; in Germany, East Germany, N = 172; West Germany, N = 1228; Berlin, N = 139; in the UK, Scotland, N = 207; Northern Ireland, N = 96; Wales, N = 37; England (excluding London), N = 1082; Greater London, N = 102; in the US, Northeast, N = 269; South, N = 556; Midwest, N = 317; West, N = 268. For the US, we used census data (US Bureau of Census 1995) to divide the states into four regions.

crimes used to remain unsolved because there were no surveillance cameras.

(INT_CH_007)

Interviewees shared a general sense that the benefits of FRT in public spaces outweigh the risks, and there was often no understanding of why one would not use the technologies. This finding supports the results from the survey where technology affinity was found to be strongly associated with FRT acceptance in China (H12). Many interviewees also linked FRT to convenience, as this interview quotation illustrates: "I would choose *convenience* because I'm a good citizen who obeys the law, and I'm not afraid my privacy would be infringed on by others because I have faith in the rule of law in our country" (Int_CN_008).

It is not that interviewees were unconcerned about privacy violations arising from increased usage of FRT in public places; on the contrary, many informants brought it up. This response by one informant is typical: "Sometimes I feel I have no privacy and worry about it when FRT becomes too prevalent" (Int_CN_006) and "I think at the moment our personal information is not managed very well by the government. There have often been leaks of such information" (Int_CN_009). Despite awareness of and complaints about privacy violations, many interviewees had the mindset that certain benefits outweigh the risks. One interviewee summarizes the trade-off as this: "It is something like an exchange of legal will (法意的交换). I would give up part of my privacy rights in exchange for a safer environment, more social order, and a more convenient lifestyle" (Int_CN-004) and further explains that "It is something like a social contract. I would give up part of my privacy in exchange for common public security" (Int_CN-004).

4.3.1.2. Full government loyalty. Interviewees frequently expressed full trust in the government's capability to use FRT sensibly. Common

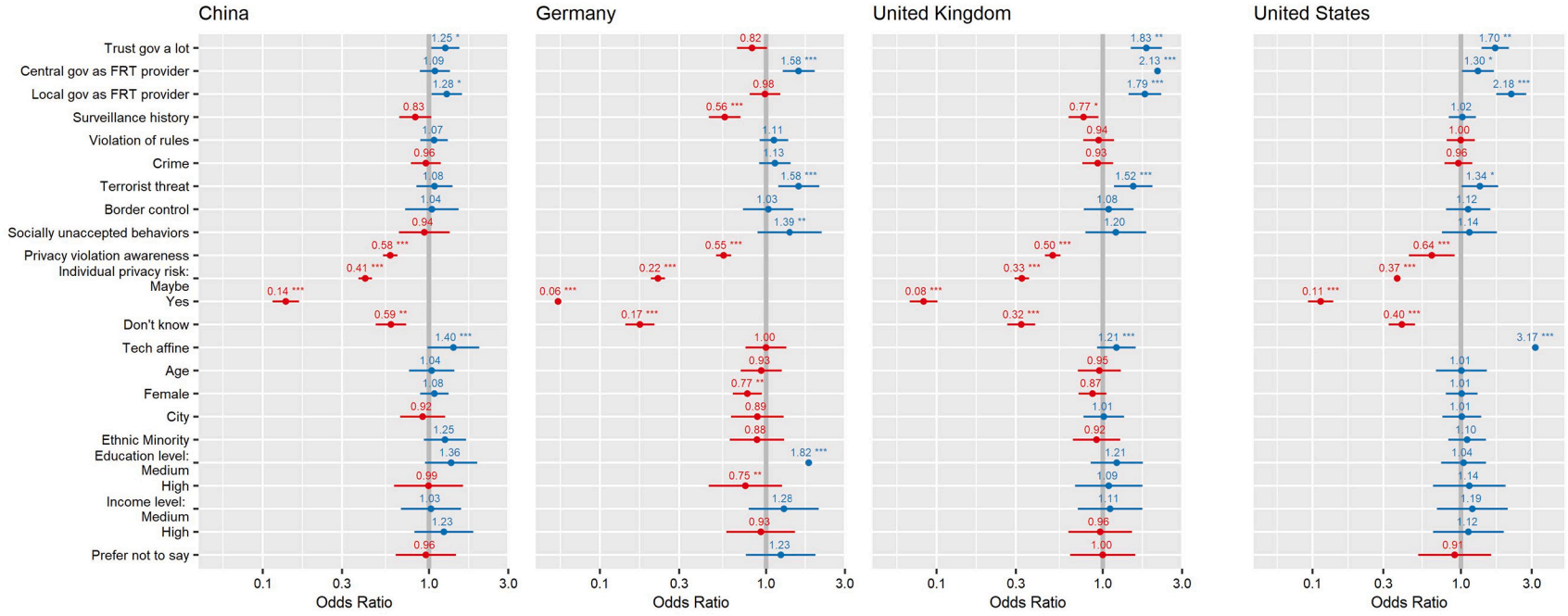

Fig. 4. Ordered logistic regression: Acceptance of FRT use in public spheres.

Table 2
Overview of hypotheses for acceptance of FRT use in the public sphere.

Hypotheses	China	Germany	UK	US
H1 Trust in government (+)	Supported	Not supported	Supported	Supported
H2 Support for central government as FRT provider (+)	Not supported	Supported	Supported	Supported
H3 Support for local government as FRT provider (+)	Supported	Not supported	Supported	Supported
H4 History of surveillance (−)	Not supported	Supported	Supported	Not supported
H5 Concerns – Violations of rules (+)	Not supported	Not supported	Not supported	Not supported
H6 Concerns – Crime (+)	Not supported	Not supported	Not supported	Not supported
H7 Concerns – Terrorist threats (+)	Not supported	Supported	Supported	Supported
H8 Concerns – Border control (+)	Not supported	Not supported	Not supported	Not supported
H9 Concerns – Socially unacceptable behavior (+)	Not supported	Supported	Not supported	Not supported
H10 Privacy violation awareness (−)	Supported	Supported	Supported	Supported
H11 Individual privacy risk (−)	Supported	Supported	Supported	Supported
H12 Technology affinity (+)	Supported	Not supported	Supported	Supported

Table 3
Common frames on FRT use in the public sphere.

China	Commonness* (n = 11)	Germany	Commonness* (n = 11)
(1) Technology advocates	9	(1) Regulation and law seekers	7
(2) Full government loyalty	6	(2) Trust in central government	5
(3) Resignation	6	(3) Resignation	4
(4) Fear and worries	8	(4) General skeptics	6

* Interviewees could express multiple frames as the frames are not mutually exclusive.

responses stress trust in the country in general, and frequent statements included "I trust my country. The more it knows about my information, the better" (Int_CN_003) or a reference to duty: "It's our duty to provide personal information to the Public Security Department. Such public institutions are reliable due to their high credibility – their acts are aimed at managing society" (Int_CN_001). Government bureaus were generally regarded with high trust when dealing with citizens' personal information: "The Public Security Department captures criminals and helps find missing persons. There also needs to be strict regulations inside the Public Security Department in terms of managing and using personal information. Overall, I'm quite satisfied at this point with the government using FRT" (Int_CN-004). These findings echo the results from the survey, showing that trust in government institutions is strongly linked with FRT acceptance. In addition to trust and duty, pride was also mentioned: "I trust the Chinese government very much. (…) I'm very proud of the social governance structure in our country" (Int_CN_011).

While respondents expressed a generally high level of trust in government agencies, such trust did not extend as much to state-owned or private companies. One interviewee explained: "The reason I don't worry so much is that now FRT is used more often by the government. I rather trust the government (…) when FRT is used by commercially oriented apps, I'm more worried" (Int_CN_006). The "hierarchy of trust" is also linked to actors' different levels of technical capacities, as described by this interviewee:

> The government has a comparatively high principle of code of conduct, even if it has some bad intentions, it doesn't dare to do so openly. I find big companies like state-owned enterprises or BAT [Baidu, Alibaba, and Tencent], their principles are slightly lower than the government's, but at least their technology is advanced and more reliable than others. Thirdly, there are also private smaller companies – even if they don't have any bad intentions to leak privacy, I don't think technically they can protect the data. Lastly, [at the bottom] there are malicious individuals, who are not worth trusting at all (…) so if FRT is provided by the government or big enterprises, I would trust it more. I can still sue them if problems appear (…). (Int_CN_007).

Interviewees in China frequently mentioned trust and duty, but only one raised the topic of regulations:

> There should also be strict regulations inside the Public Security Department in terms of managing and using personal information. (…) To better protect and manage personal information, our country still has a lot to do in terms of legislation – for example, it needs to be stipulated who has the right and qualification to manage personal information." (Int_CN_004).

4.3.1.3. Resignation. Many interviewees seemed helpless or resigned over FRT software creeping into their daily lives. Common narratives formed around statements such as "my personal information has already been stolen by Jack Ma. (…) The information has already been leaked before the arrival of FRT, and it's still happening. The use of FRT doesn't really worsen or ameliorate this problem" (Int_CN_003). It was common for large private enterprises such as Alibaba to be blamed, without interviewees being aware that it is also the absence of enforced regulations and government rules that allows companies like Alibaba to use personal data irresponsibly. Interestingly, interviewees frequently noted that they have no choice in matters such as protecting personal data from big large tech companies and, therefore, had given up. One interviewee concluded:

> Alibaba rules the whole payment system like a bandit. (…) [Transportation company] DiDi is the same (…) You simply can't choose. It doesn't matter whether you let your face be scanned or not – your personal information is already in Alipay anyway. As a result, if Alibaba is promoting FRT, I will also use it because they already have my information. (Int_CN_002).

Interviewees repeatedly stressed their view that the Chinese Communist Party can also get access to all the data anyway (Int_CN_003). The resignation extended to beliefs that privacy issues are not taken seriously in China:

> Frankly, as for the privacy issue, there is nothing to talk about in this country. I work in the property management industry, and I'm very aware of how much house owners' personal information is worth because this information is sellable. Real estate developers always sell the information of property owners to someone else because in China, those doing this would not really face a serious criminal charge. Even if such activities are caught, the punishment is tiny. (…) This makes privacy out of the question in China because privacy is so worthless here. The best solution to pursue privacy in China is not to leave any trace on the Internet, to be very honest. (Int_CN_007).

The overall sense is that, since so many private companies have the biometric data already, the "government might as well steal or abuse our biometric information" (Int_CN_002). In a way, the rampant use of FRT

by private companies paved the way for FRT use in public spheres in China. Citizens are also aware that the government has multiple avenues of surveillance and that FRT represents one tool of many: "If the government really intends to find you, it can trace you anytime anywhere very easily. (…) We, the common people, don't really worry so much about it that we need to hide the front cameras on our smart phone" (Int_CN_008).

4.3.1.4. Fear and worries. Finally, a small group also openly expressed concern about and fear of the result of widespread adoption of FRT in public spaces. One of the biggest fears relates to certain government actors abusing their power:

> Regarding the Public Security Department, you can only pray they don't abuse their power to go after you. There's nothing we can do with such an authoritarian government. The only thing you can do is to pray it doesn't turn against you (…) the Chinese government is still afraid of public opinion. Most of the time, public opinion is a relatively effective way [to check the government]. (Int_CN_007).

An interviewee who lives in China but works in Hong Kong also notes:

> A while ago, the Hong Kong government introduced something like "smart lamp posts" in the city. (…) The people in Hong Kong showed strong opposition to these smart lamp posts because they believed such things were infringing on their privacy. (…) If the government really wanted to take revenge when the time is ripe, the government would definitely be able to use this technology to find protestors. (Int_CN_008).

4.3.2. Common frames in Germany

4.3.2.1. Regulation and law seekers. German interviewees expressed much less generic faith in FRT technology than their Chinese counterparts, reflecti

ng a widespread skepticism in the population that the survey results also highlighted. A very common concern was that relevant regulations and laws are not (yet) in place to ensure the secure handling of data. One interviewee summarized this as follows: "I'm a bit reserved when it comes to FRT implementation in public spaces. Security isn't sure yet, and the legislature hasn't created the necessary framework to eliminate all abuse" (Int_GER_007). Many interviewees called for more regulation to ensure personal biometric data is not leaked, for instance: "More regulations would be good to make sure the data does not come into the wrong hands" (Int_GER_001). In general, there was the sense that "technology and science are far ahead of social development in terms of the legal framework and control" (Int_GER_007).

4.3.2.2. Trust in central government. Opinions differed about whom to trust, with a large share of German interviewees trusting the central government. This is commonly expressed in statements such as: "I don't worry about the public use of FRT. The German government knows everything about me anyway. The tax office knows all my financial accounts; they can find me anyway. I'm completely transparent, after all" (Int_GER_004). However, there was less trust in local governments:

> I wouldn't trust, for example, the government of the federal state Brandenburg to control the data because of the current political situation and extreme right-wing parties there. It should really just stay under the control of the central government, but with strict guidelines and limitations.
>
> (Int_GER_007)

Many interviewees also expressed worries that private companies abuse their data:

> [With regard to who should provide FRT] The state. Certainly not private companies. Everything owned by the government is limited to a territory. Why should a private provider get access to this information? I would rather entrust it to the government (…) even though I don't really approve of it [revealing private information].
>
> (Int_GER_011)

Private companies are often seen as profit-seeking: "I'm strongly against private companies using FRT, which would turn into profiteering; things like this should be solely government and state-owned" (Int_GER_005). However, a minority of interviewees were in favor of commercial companies running FRT as doing so would limit the government's stake in the collection of vast amounts of data: "I would prefer only to use FRT privately; otherwise, it would be too much surveillance for my taste" (Int_GER_008). The interviewee grew up in East Germany, which could explain the sensitivity toward state use of FRT.

4.3.2.3. Resignation and general skeptics. Finally, there was a common narrative of general resignation and skepticism about FRT use in public spaces. Similar to the situation with the Chinese interviewees, one group of German interviewees were simply resigned to the slowly growing technology "creep[ing] in" and voiced an overriding feeling of helplessness and lack of choice: "I can't do anything against this trend because, if they want the data, they will have it" (Int_GER_004); and "I will have to accept it, I don't have a choice. (…) even though it's very difficult in terms of the data protection law" (Int_GER_002). Skeptics, in particular, emphasized issues with privacy issues: "I don't know how safe FRT is. I can't really form an opinion about that. Every technology has security holes, but I can't say anything about it" (Int_GER_006).

4.4. Attitudes toward surveillance past

As China and Germany both employed surveillance methods in the past, including during extreme periods such as the Cultural Revolution in China, Nazi Germany, and the State Security (Stasi) in the former East Germany, we also asked respondents both in the survey and during the interviews whether the previous use of surveillance methods influenced their attitudes toward FRT today and, if so, how they experienced that influence. The survey results found that FRT acceptance in China was not significantly associated with the country's history of surveillance, but there was a significantly negative association in Germany (H4). Our findings from the interviews were surprisingly varied and provide further insights into this topic.

In China, interviewees generally showed little awareness of the variety of surveillance methods used in the past and the present. Of course, this is a sensitive topic, and it is possible that interviewees self-censored their responses. Moreover, as these issues are not publicly discussed or debated in state-sanctioned media, and social media is highly censored, it is equally likely that the propaganda apparatus managed to push their preferred narratives (i.e., that FRT is an effective instrument ensuring social order) onto the general public. One informant noted, for instance:

> Chinese people have no idea about the surveillance history in their country. I think a high degree of the surveillance state is built on advanced technology (…) However, it is too short a period for us since the economic reforms and new prosperity; therefore, we greatly welcome new technologies as we think they represent a bright future.
>
> (INT_CH_003)

Another interviewee also notes that the China of today holds a lot of benefits compared with Mao's time: "I think in Mao's time, we wouldn't really accept any new stuff because back then, we were very conservative (…) since the economic reforms, it has become better" (INT_CH_009).

In Germany, generally speaking, awareness of governments' uses of

surveillance methods in the past seemed to have a greater influence on interviewees' opinions about FRT uses in public spheres today. One interviewee explained how Germany's history with the Nazi regime and the subsequent *Aufarbeitung* (historical evaluation) in history classes shaped his view of FRT:

> If there were machines everywhere, scanning my face, I would feel like I'm under constant surveillance. That could be connected to my parents' experience in the Third Reich. They experienced this kind of regime, where everyone was under surveillance and spying on each other, and also in the post-war period. I grew up with books like '1984' and 'A Brave New World' (…) that specifically deal with such dystopias. (…) Honestly, I would feel very uncomfortable with the government being in charge. It's a dangerous tool that can easily be abused. I'm not sure whether the data would be safer in the hands of a company, though (…). As long as it's not a lawless state (*Unrechtsstaat*), it could be in the hands of the police, but as no one can be sure it will stay that way, we have to be careful.
>
> (Int_GER_009)

With regard to the interviewees' experiences with the Stasi, the responses were mixed. Some interviewees were surprisingly open about FRT uses, stating that it was "not as bad" in East Germany. One interviewee noted:

"The state [GDR] had a monopoly on the use of force (*Gewaltmonopol*); you were used to it, it gave you a feeling of security as well. (…) I think that FRT is acceptable" (Int_GER_003). Another interviewee noted: "As a former East German, I know I can't defend myself anyway when they have the data. Also, I have nothing to hide" (Int_GER_004). However, other interviewees were more skeptical:

> I'm from [the former] East Berlin. This affects my attitude toward FRT. (…) Because we witnessed how a government abused information, even though I didn't actually experience it myself, but I heard about it."
>
> (Int_GER_007)

Overall, similar to the findings from the online survey, the interviews suggest that Germans are more skeptical about FRT usage in public, partly because of negative experiences with a controlling surveillance state. One informant summarizes this as follows: "Germans always fear that everything could be surveilled and spied on; the Chinese are probably less afraid of that, just as East Germans are not afraid of it too much, either, I think" (Int_GER_010).

4.5. Discussion

Acceptance levels of FRT use in public spheres in the four countries correlate closely with cross-country differences in political contexts. Trust in the respective governments and their administrations plays a key role in the development of these acceptance levels. Of those respondents who "somewhat accept" or "strongly accept" FRT, in Germany only 41% "somewhat" or "strongly" trust in the government, while in China this is significantly higher at 73%, similar to the US (72%) and the UK (74%). Moreover, when asked whether the government should play a smaller or bigger role in the development of infrastructure and the collection of surveillance data, among those who accept the public use of FRT, in China, 73% of respondents somewhat or strongly accepted this claim, while in Germany, only 37% answered the same. UK and US respondents lie in the middle at 57% and 59%, respectively.

Different historical contexts also help explain the variations in acceptance levels. The previous use of government surveillance results in lower FRT acceptance. This effect was most visible in Germany, which is not surprising given its history of surveillance both during the periods of the GDR and Nazi Germany. The effect of a negative use of surveillance in the past was not significant in China, possibly because Chinese citizens are relatively used to surveillance and generally do not see a strong link between FRT and government surveillance. Interestingly, interviews showed that while citizens in Germany trust their government to some extent, this is matched with a strong demand for stricter regulations and laws on data protection. In China, interviewees addressed the need for stricter regulations to a lesser degree, partly because China lacks independent third-party regulators, and many government regulatory institutions are often dysfunctional.

Different concerns about public issues also explain FRT acceptance levels, albeit to a lesser extent. As Fig. 5 shows, concerns about violations of rules and regulations and socially unacceptable behavior are more of an issue in China, while crime and terrorist threats are a greater concern among respondents in the UK and US. As a result, the perceived need for the public use of FRT varies according to different political contexts. If citizens are concerned about terrorist threats, they are more in favor of FRT use in public. Notably, though, concerns about crime and

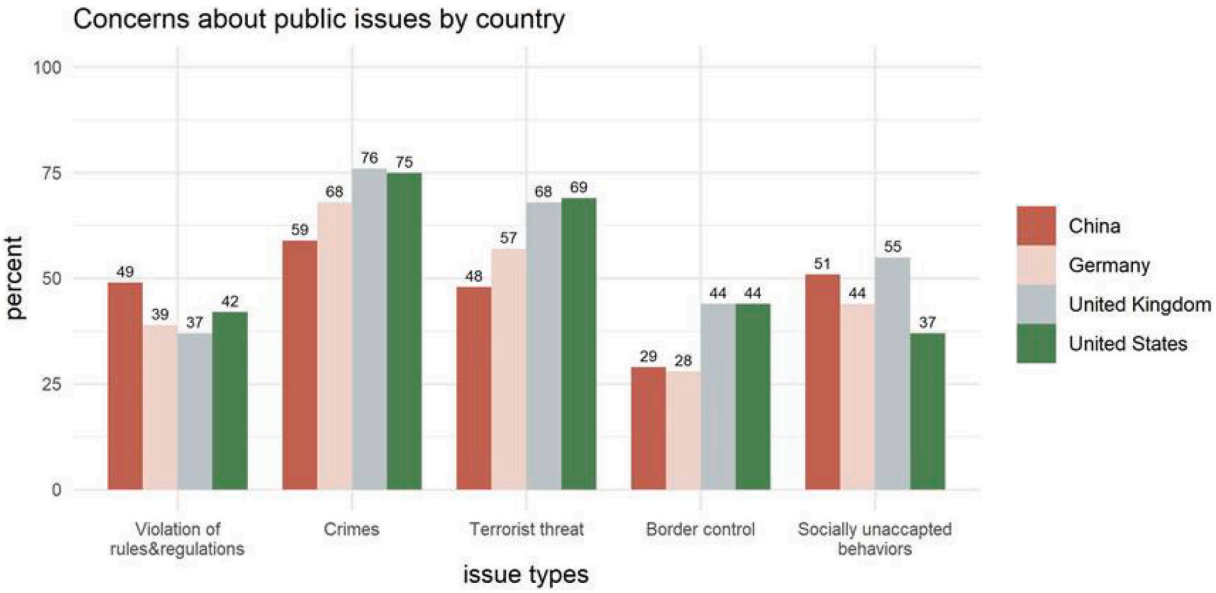

Fig. 5. Concerns about public issues – by country.

border control were not significantly related to FRT acceptance; yet, in the interviews, lowering crime rates and increasing security or social order is often stated as a key FRT application.

We further find that individuals' privacy and technology preferences and traits have a very strong influence on their acceptance levels of FRT use in public spheres. Privacy concerns have the strongest negative effect on people's acceptance levels. Interestingly, a much larger share of the respondents (41%) believe FRT gives rise to privacy violations in general, while, when asked more specifically with regard to their own privacy a bit later in the survey, only 25% of the respondents viewed FRT as a threat to their own individual privacy. Of the 41% who answered yes to privacy violations in general, 42% continued answering yes when asked about violations to their individual privacy, while 47% suddenly answered "maybe," 7% answered "no," and 3% said they "don't know." Respondents seem to find it easier to think of FRT as a possible threat in a general sense than as a potential threat to their own individual safety. Possible explanations are the lack of knowledge or simply an attitude of denial since the majority of respondents have been exposed to or used FRT before, and admitting possible privacy infringements in a survey or interview might make respondents anxious. Overall, concerns about privacy violations in general or on an individual level result in lower FRT acceptance in all four countries, including China. This outcome is important since these results do not confirm common claims that Chinese citizens do not care about privacy. Instead, the findings in general support previous studies on 'contextual integrity' showing that a range of contextual factors such as socio-political beliefs and norms influence citizens' risk–benefit privacy calculations (Nissenbaum, 2004).

5. Conclusion

Acceptance of the use of facial recognition technology in public spheres varies across countries. Based on an online survey conducted among Internet users in China, Germany, the UK, and the US, we show that acceptance of the use of FRT on the general population varies across countries, with 51% of Chinese respondents showing the highest level of acceptance, while only 37% of Americans and 38% of Germans are strongly or somewhat accepting of FRT for public use. The UK responses fall somewhere in between, with 42% of respondents expressing acceptance of FRT in public spheres. These findings support previous studies that find a rich variety of public attitudes toward surveillance and digital technologies in different socio-political contexts (Kostka, Steinacker, & Meckel, 2021; Kostka & Habich-Sobiegalla, 2022; Liu & Graham, 2021).

While investigating the factors driving attitudes toward FRT in these four countries, we found striking similarities. Trust in the government, concerns about terrorist threats, and a high level of technological affinity among citizens are significantly positively linked with FRT acceptance. By contrast, awareness of a country's negative past use of surveillance methods and concerns regarding privacy violations result in a more cautious attitude toward the use of FRT in public settings. We further find that citizens in all four countries are equally concerned about privacy violations, thus rejecting previous assumptions that citizens in China do not care about privacy. Overall, the findings show quite a lot of similarities in the drivers of FRT acceptance across national contexts, even if the overall rates of acceptance are different.

The findings contribute to the technology acceptance literature (e.g., Davis, 1989; Venkatesh et al., 2003), which previously highlighted the importance of perceived efficacy and technology usefulness in shaping individual attitudes toward technology. Our findings add to this literature by showing that political context matters. Historical experiences of surveillance and trust in government institutions also influence citizens' attitudes toward digital technologies. Our results further support findings from previous studies on the use on contract tracing apps (CTAs) during the COVID-19 pandemic (e.g., Riemer, Ciriello, Peter, & Schlagwein, 2020; Wnuk, Oleksy, & Maison, 2020; Zhang, Kreps, & McMurry, 2020), which found that trust in government institutions (Altmann et al., 2020; Habich-Sobiegalla and Kostka, 2022) and experience with technology (e.g, familiarity or have prior experience with fitness or health tracking apps) positively influence citizens' willingness to install CTAs (Abeler et al., 2020).

This study also adds to the existing privacy calculus theory (Dinev & Hart, 2006; Wadle et al., 2019) and privacy–security trade-off model literature (Davis & Silver, 2004; Pavone & Degli-Esposti, 2012) by showing that citizens are particularly critical of FRT uses in public when they perceive FRT uses as a threat to their *individual* privacy (rather than just believing the technology leads to privacy violations in general). In other words, privacy concerns are particularly effective at shaping public opinion if citizens feel personally affected by it. In all four countries, a large share of respondents (41%) stated that FRT is a threat to privacy violations in general, while only a quarter believe that FRT threatens their individual privacy, and many are unsure. This indicates that there is some uncertainty among citizens about the exact ways in which FRT affect their individual privacy.

This study offers several policy implications. First, while concerns about personal privacy are very strongly associated with acceptance rates across all four countries, a large share of citizens is actually unaware of how FRT applications affect their own individual privacy. These concerns need to be addressed, for instance by informing citizens about existing regulations and laws that protect their rights, complemented with broader education strategies explaining the effects of FRT on privacy matters. Second, our findings suggest that citizens are willing to accept FRT in public spheres if they trust the government, especially if the technology is managed by the central government. This suggests that nuanced regulation must be enacted to guide and limit the use of FRT by such governments in appropriate ways. However, the adoption of FRT in public spheres is ongoing on an international scale, and it is conceivable that public opinion could shift as FRT software gets more widely adopted.

Our research has some limitations that may provide avenues for further research. First, as this was a non-probability online survey using mobile phones and desktops, the sample only resembles the Internet-connected population in each country and is biased toward the younger population. Further research should avoid such "coverage bias" (Dijk & Jan, 2005) and include subpopulations that are older and without access to the Internet. Second, our sampling method has various selection biases in terms of topical self-selection and economic self-selection (Lehdonvirta, Oksanen, Räsänen, & Blank, 2020). Participants in our survey may already have a particular affinity with technology, which could positively affect their stance toward technology adoption, including the various uses of FRT. The rewards-based recruitment might have also resulted in participants associating the positivity of incentives with positivity toward FRT.[3] Third, our analysis is based on single-item measures, and future research could conduct a multigroup analysis, including a multi-item measure for the dependent variable and considering the moderating effect of age for certain

[3] Some questions in the survey may have been interpreted differently across countries. As the use cases of FRT in public spheres vary widely between the four contexts studied, mentions of FRT conjure up diverse associations and scenarios. This could influence the connotation participants have when asked about its acceptability. Some questions might also have been misunderstood. For instance, one-fifth of the German respondents reported seeing FRT in public on the streets and at railway stations. But given that by 2019, only the Berlin Südkreuz train station had experimented with FRT, and despite an introductory disclaimer explaining what we mean by "FRT," some respondents seem to have confused standard video cameras with FRT software. Essentially, unless clearly stated, one cannot know if a simple camera installation is connected to FRT. In addition, our survey likely also contains question biases as offering possible issues or consequences as options may have induced the respondents to report their views accordingly (on limited answer possibilities and acquiescence bias, see Furnham, 1986).

explanatory variables. Fourth, our interview sample was small and the materials do not claim exhaustiveness in covering all possible frames and narratives of how citizens view and understand FRT. Future research could also include participant observation to learn more about the reported versus actual behavior of citizens toward digital technologies. Lastly, in the case of China, the reported levels of FRT acceptance might be higher, as it could be difficult for citizens to hold dissenting views of technologies that are officially endorsed by the government. Although participants were aware that any identifying data was anonymized and analyzed for research purposes only, we cannot dismiss the possibility of preference falsification as some more cautious respondents may have given false answers due to concerns about reprisals from the state.[4] For instance, in the survey, variables such as trust in government might be overreported, while examples of the previous history with surveillance might actually be underreported among respondents. Our interviews helped as a check against our survey findings, but there may also have been a certain amount of self-censorship.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors gratefully acknowledge the excellent research support by Danqi Guo and Sophia Wischmann. Genia Kostka acknowledges funding from the European Research Council Starting Grant (Grant No. 852169), and Miriam Meckel and Léa Steinacker express their gratitude to the Swiss National Science Foundation for partly funding the survey.

Appendix

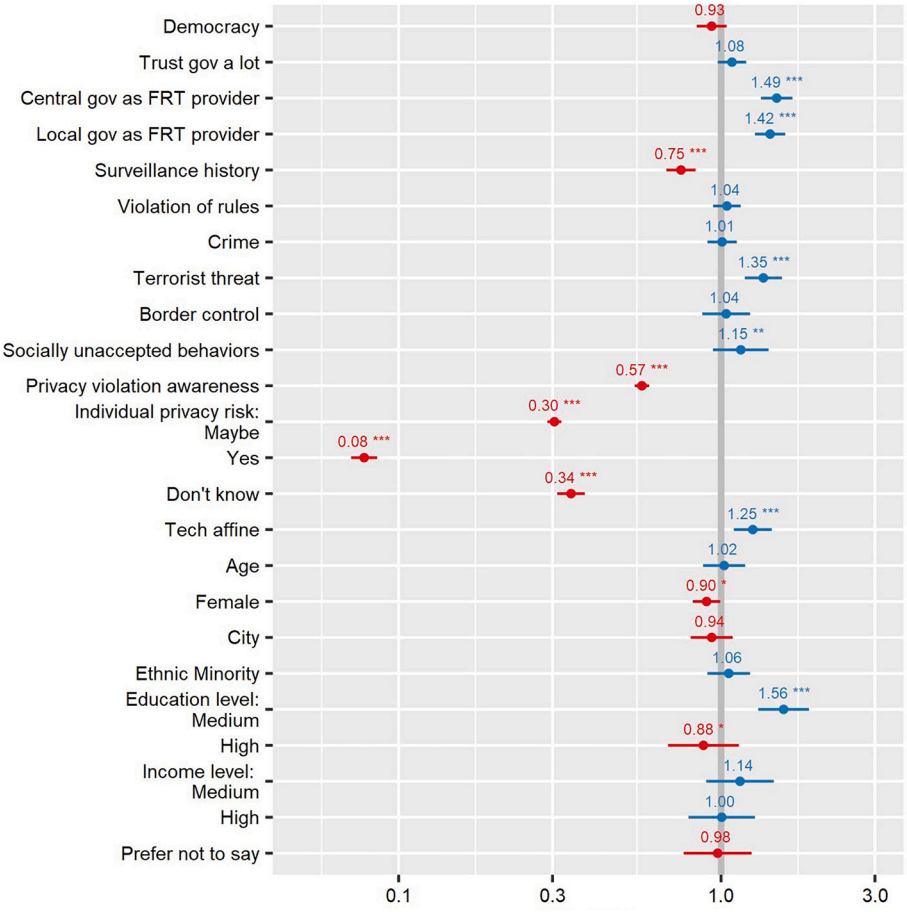

Fig. A1. Ordered logistic regression: Acceptance of FRT use in the public sphere – total sample.

[4] The risk of preference falsification is larger in China than in Germany, the US, or the UK as citizens in authoritarian China are more likely to practice self-censorship to politically sensitive questions in surveys (Jiang & Yang, 2016). Recent research finds some evidence for this preference falsification by documenting high rates of nonresponses to politically sensitive questions across Chinese surveys, especially among marginalized groups such as women, members of lower social classes, and non-Party members (Ratigan & Rabin, 2020; Shen & Truex, 2021). However, this research's main focus is on FRT, which seems to be of a less sensitive nature than the research in the cited papers, which focus on political trust in the government. In our survey, we observed low rates of nonresponses and conclude that self-censorship may have some (but likely not a huge) influence on our research outcome.

Table A1
Total country and sample population.

	Four countries		China		Germany		UK		US	
	Total	Sample	Total	Sample	Total	Sample	Total	Sample	Total	Sample
Population	1900 M	6099	1411 M	1628	84 M	1538	68 M	1524	337 M	1409
Gender										
Male	50.63%	51.55%	51.07%	53.90%	49.42%	51%	49.69%	50.40%	49.29%	50.70%
Female	49.37%	48.45%	48.93%	46.10%	50.58%	49%	50.31%	49.60%	50.71%	49.30%
Age										
1–18-35	25%	46%	25%	68%	20%	35%	24%	38%	24%	40%
2–36-50	21%	33%	22%	27%	18%	38%	19%	33%	19%	36%
3–51-65	21%	21%	21%	5%	23%	27%	19%	29%	19%	24%
Internet-connected	77%	100%	72%	100%	88%	100%	92%	100%	91%	100%

Source: Census.gov (2022); Statistica (2021).

Table A2
Summary of dependent and independent variables.

FRT Acceptance in the Public Sphere *(weighted, in %)*							
	Measurement	Strongly oppose	Somewhat oppose	Neither oppose nor accept	Somewhat accept	Strongly accept	N
		12.5	20.1	25.4	31.2	10.9	6099
Control Variables Sociodemographic							
Age	18–35	10.8	22.2	27.6	29.3	10.1	2788
	36–50	14.6	17.9	23.7	32.9	10.9	2032
	51–65	12.8	19.2	23.2	32.3	12.5	1279
Gender	Male	12.9	20.4	23.5	31.7	11.5	3144
	Female	12.1	19.8	27.5	30.6	10.1	2955
Living area	Rural	11.4	21.3	25.4	31.1	10.8	2135
	City	13.1	19.5	25.4	31.2	10.9	3964
Ethnic Group	Minority	15.1	20.1	25.2	28.0	11.6	866
	Majority	12.0	20.3	23.1	33.4	11.1	4314
	Don't know	12.2	19.4	36.2	23.4	8.9	920
Education *(grouped)*	Low	28.9	16.1	21.2	22.6	11.2	420
	Medium	11.2	20.8	27.7	30.5	9.8	3987
	High	11.4	19.6	21.0	34.8	13.2	1692
Income *(grouped)*	Low	13.5	21.9	28.4	27.5	8.6	798
	Medium	11.4	20.2	24.6	32.4	11.4	2227
	High	13.2	19.0	21.8	33.7	12.4	2318
	Prefer not to say	12.4	21.6	35.8	23.4	6.8	756
Political context and attitude							
Trust in government	Not at all	32.8	19.9	22.0	18.2	7.0	650
	Very little	12.8	26.7	26.5	26.8	7.2	1312
	Somewhat	7.5	21.3	26.2	34.6	10.3	2102
	A lot	10.9	13.8	21.2	37.4	16.7	1657
	Prefer not to answer	10.7	18.7	41.1	21.7	7.8	379
Perceived role of government	Smaller	20.1	27.1	19.3	26.0	7.5	767
	Neither smaller nor bigger	9.5	19.5	30.9	31.5	8.6	1715
	Bigger	12.5	18.0	20.7	34.6	14.2	2850
	Don't know	11.5	22.2	36.8	22.5	7.0	767
Support FRT provider *(multiple responses)*	Local government	8.4	13.2	21.7	39.7	17.1	2051
	Central government	8.3	15.4	23.1	38.1	15.2	2743
	Private companies	11.6	14.4	21.5	33.2	19.2	1230
	Public-private partnership	6.2	17.6	23.7	38.0	14.5	3214
	None of the above	29.2	27.5	27.4	11.3	4.7	1184
History of surveillance	No	4.4	15.5	21.6	41.7	16.7	1446
	Yes	23.0	24.3	19.9	23.5	9.3	2384
	Don't know	6.5	18.6	33.6	32.5	8.8	2269
Concerns about public issues							
Issues of concern *(Multiple responses)*	Violation of rules and regulations	12.5	17.9	23.0	33.0	13.6	2563
	Crime	11.5	20.1	24.6	32.2	11.7	4217
	Terrorist threats	10.8	19.3	24.4	33.2	12.4	3643
	Border control	11.5	17.9	24.6	32.7	13.3	2199
		10.2	19.8	23.9	33.5	12.6	2862

(*continued on next page*)

Table A2 (*continued*)

FRT Acceptance in the Public Sphere *(weighted, in %)*							
	Measurement	Strongly oppose	Somewhat oppose	Neither oppose nor accept	Somewhat accept	Strongly accept	N
		12.5	20.1	25.4	31.2	10.9	6099
	Socially unacceptable behavior						
	None of the above	15.0	18.6	31.0	26.8	8.6	678
Individual preferences and traits							
	General awareness:						
	Privacy violations						
	Yes	20.3	30.0	22.7	21.9	5.1	2526
Privacy awareness	No	7.0	13.1	27.3	37.7	14.9	3573
	Personal risk awareness:						
	No	2.0	5.6	17.8	46.7	27.8	1292
	Maybe	5.8	22.4	30.1	34.6	7.0	2851
	Yes	36.4	30.4	16.7	12.0	4.5	1505
	Don't know	4.7	12.9	46.2	28.4	7.7	451
Technology affinity	Yes	9.0	8.9	14.3	41.7	26.1	841
	No	13.0	21.9	27.2	29.5	8.4	5258

Table A3
Generalized variance inflation factors (GVIFs).

	China			Germany			UK			US		
	GVIF	Df	GVIF^(1/(2*Df))	GVIF	Df	GVIF^(1/(2*Df))	GVIF	Df	GVIF^(1/(2*Df))	GVIF	Df	GVIF^(1/(2*Df))
gov_trust_group	3.405834	1	1.84549	1.786976	1	1.336778	2.539988	1	1.593734	2.092457	1	1.446533
central_gov	2.59804	1	1.611844	1.498136	1	1.223983	2.000765	1	1.414484	2.033107	1	1.42587
local_gov	1.26841	1	1.126237	2.276145	1	1.50869	1.977749	1	1.406325	2.610799	1	1.615797
govsurgroup	2.344303	1	1.531112	1.881673	1	1.371741	1.931838	1	1.389906	2.056298	1	1.43398
violation_rules	3.247967	1	1.802212	3.975406	1	1.993842	5.289066	1	2.299797	5.135293	1	2.266119
crime	2.675189	1	1.6356	2.926675	1	1.710753	4.079493	1	2.019775	4.092337	1	2.022953
terrorist_threat	1.817529	1	1.348158	1.547727	1	1.244077	2.172566	1	1.473963	2.15914	1	1.469401
border_control	2.328532	1	1.525953	2.032121	1	1.425525	2.887591	1	1.699291	1.884544	1	1.372787
socially_unaccepted_behaviors	1.653766	1	1.285988	2.715142	1	1.647769	2.214814	1	1.488225	2.312506	1	1.520693
privacy_violation_gen	4.5288	1	2.128098	4.216287	1	2.05336	3.990258	1	1.997563	4.017866	1	2.004462
privacy	4.45701	3	1.282844	6.374219	3	1.361668	4.966837	3	1.306211	6.222391	3	1.356208
tech_affine	11.769942	1	3.430735	12.92728	1	3.595453	11.878356	1	3.446499	11.949437	1	3.456796
age	1.931822	1	1.3899	2.041877	1	1.428943	2.152267	1	1.467061	2.140742	1	1.463127
gender	3.889983	1	1.972304	3.18841	1	1.785612	2.579584	1	1.606108	2.94396	1	1.715797
city_rural	1.110502	1	1.053804	1.215104	1	1.102318	1.19553	1	1.093403	1.341252	1	1.158124
ethnic_minority	2.639969	1	1.624798	1.240012	1	1.113558	1.729064	1	1.314939	2.608294	1	1.615021
education_level	5.256651	2	1.514179	11.500262	2	1.841522	7.993564	2	1.681454	8.587082	2	1.711833
income_level	35.10514	3	1.809513	114.735084	3	2.204361	50.75186	3	1.924164	67.259311	3	2.016626

Table A4
Model evaluation.

	Residual deviance	AIC	Hosmer–Lemeshow tests $\chi 2$, (p-value)
China	4238.168	4292.168	19.089 (0.2097)
Germany	3959.908	4013.908	70.763 (0.0000)
UK	3973.167	4027.167	20.921 (0.1394)
US	3850.753	3904.753	15.643 (0.4068)
Total	16,346.15	16,402.15	70.854 (0.0000)

Note: The Hosmer–Lemeshow goodness of fit test provides information on how well the model is specified. Germany and the total sample failed the test with $p < 0.000$. Failing the test does not mean the model is a bad fit but rather that the model can be made more complicated (for instance, by adding interaction or nonlinearity) to fit the data. However, the model can easily run into the danger of overfitting.

Table A5
Informants' sociodemographic background.

	Germany (n = 11)	China (n = 11)
Age		
18–35	4	7
36–50	1	1
51–65	3	3
>65	3	0
Gender		
Male	4	4
Female	7	7
Country of origin		
East Germany	9	From China
West Germany	2	
City size		
Major city	9	6
Nonmajor city	2	5

Table A6
Acceptance levels – interviews.

Acceptance of FRT	Germany (n = 11)	China (n = 11)
Strongly oppose	–	–
Somewhat oppose	2	1
neutral	2	2
Somewhat accept	5	5
Strongly accept	2	3

Table A7
Content summary interviews.

Int. no.	Country of origin	Current city	Age	Gender	Profession	Acceptance	Key findings
1	East Germany	Hamburg	33	F	HR Management	Somewhat Accept	■ Convenience over privacy, have nothing to hide ■ Less and less fear about FRT ■ FRT is great for protection and security, esp. for women on the street (Former East German, young generation)
2	East Germany	Jüterbog	33	F	Civil servant	Somewhat accept	■ Convenience over privacy, esp. convenience for private use of FRT ■ Find there is no choice but to accept the public use of FRT (Former East German, old generation)
3	East Germany	Berlin	67	F	Tax accountant	**Strongly accept**	■ Convenience over privacy ■ East Germany's past has a positive influence ■ Security feeling/demands greater than the fear about FRT
4	East Germany	Berlin	49	M	Handymen construction	**Strongly accept**	■ Convenience is very important (Former East German, escaped from the GDR, so not pro-Stasi)
5	East Germany	Jülich	70	M	Retired natural scientist	Neutral	■ Strongly support the use to detect criminals and other security purposes in the public ■ Against private use of FRT (Former East German, left GDR at age 21)
6	East Germany	Berlin	54	F	Retired nurse	Somewhat accept	■ Privacy over convenience ■ Private use OK, cautious about public use ➔ especially against "surveillance," but find detecting criminals necessary (Used to be a party member in the GDR, so not totally opposed to the system)
7	East Germany	Berlin	70	M	Retired natural scientist	Somewhat support (private use) Somewhat oppose (public use)	■ Distrust use by private companies

(*continued on next page*)

Table A7 (*continued*)

Int. no.	Country of origin	Current city	Age	Gender	Profession	Acceptance	Key findings
8	East Germany	Berlin	30	F	Doctor	Neutral – somewhat oppose	■ Public use not ready due to missing laws (Former East Germany, but very young, ballet dancer, now a doctor) ■ Privacy over convenience ■ Private use OK but not in the public (Former West German, grew up in West Berlin)
9	West Germany	Berlin	52	F	Piano teacher, Composer	Somewhat oppose	■ Privacy over convenience ■ Only accept limited use for security purposes ■ Distrust state use of FRT – dangerous instrument (Former East German, fled from GDR with family)
10	East Germany	Berlin	51	F	Biotechnology expert	Somewhat accept	■ Convenience over privacy ■ Support both private and public use ■ Support the use by the state
11	West Germany	Berlin	24	M	Student of industrial engineering	Neutral	■ Privacy over convenience ■ Do not accept public and private use of FRT ■ Only supports the state using it, not private actors
Int. Nr	Country Origin	City Now	Age	Gender	Profession	Acceptance	Key findings
1	China	Foshan (Guangdong)	58	F	Middle school teacher (retired)	**Strongly support**	■ Security over convenience ■ Private use necessary to keep up the trend ■ It's our duty to provide personal info to Public Security Department
2	China	Shanghai	25	F	Freelancer designer	Neutral	■ Security over convenience ■ Worry about the abuse of personal information by both government and private companies ■ It's the values and interests behind FRT that defines how this technology will be used
3	China	Beijing	24	F	Playwright	Somewhat against	■ Convenience over security ■ FRT for payment redundant, susceptible to info leaks and misuse ■ Many technical errors reported ■ FRT helps government control riots more easily
4	China	Shanghai	29	M	Legal assistant	Somewhat accept	■ Security over convenience ■ Support use in public because it raises efficiency and makes procedures more transparent ■ Worry about misuse of the collected data
5	China	Foshan (Guangdong)	27	M	IELTS teacher	Neutral	■ Convenience over security (FRT does not bring more security) ■ Forced to use
6	China	Shenzhen	24	F	Branding, marketing	**Strongly accept**	■ Convenience over security ■ FRT increases efficiency esp. in public transport and public services ■ Security over convenience (no privacy in China)
7	China	Shenzhen (Guangdong)	26	M	Marketing for a property management company	Somewhat accept	■ FRT saves us trouble from remembering many passwords ■ Worry personal information being misused by private companies, not government
8	China	Hongkong	25	F	HR in a state-owned company	Somewhat accept	■ Convenience over security (I'm a lawful citizen, no fear of privacy infringement) ■ Worry info misuse by private companies
9	China	Longyan (Fujian)	54	F	Former laid-off worker from a factory (retired)	Somewhat accept	■ Security over convenience ■ Following the trend is important ■ FRT is a safer technology than fingerprints
10	China	Longyan (Fujian)	47	F	Customer services in a property management company	Somewhat accept	■ Security over convenience ■ FRT is a safer technology, and it offers convenience
11	China	Guoluo (Qinghai)	54	M	Tailings trade	**Strongly accept**	■ Convenience over security ■ FRT is a basic and powerful function now for us common people

References

Abacus. (2019). Facial recognition is enforcing traffic laws in Shenzhen. In *South China Morning Post, August 16*. https://www.scmp.com/abacus/tech/article/3029548/facial-recognition-enforcing-traffic-laws-shenzhen [accessed May 6, 2021].

Abeler, J., Altmann, S., Milsom, L., Nosenzo, D., Toussaert, S., & Zillessen, H. (2020). Support in the US for app-based contact tracing of Covid-19, 13 April. Available at: https://osf.io/n7w48/.

Ada Lovelace Institute. (2019). *Beyond face value: Public attitudes to facial recognition technology*. Ada Lovelace Institute. September 2 https://www.adalovelaceinstitute.org/beyond-face-value-public-attitudes-to-facial-recognition-technology/ [accessed May 6, 2021].

Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., … Abeler, J. (2020). Acceptability of app-based contact tracing for COVID-19: Cross-country survey study. *JMIR mHealth and uHealth, 8*(8), Article e19857. https://doi.org/10.2196/19857

Amnesty International. (2021). *Ban dangerous facial recognition technology that amplifies racist policing*. Amnesty International. January 26 https://www.amnesty.org/en/latest/news/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/ [accessed May 6, 2021].

Article 19. (2021). Emotional entanglement: China's emotion recognition market and its implications for human rights. Article 19, January https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf.

Braca, A. (2017). An investigation into Bias in facial recognition using learning algorithms. In *MSc research project*. Dublin, IRL: National College of Ireland. http://norma.ncirl.ie/3074/1/annyebraca.pdf [accessed May 6, 2021].

Bradford, B., Yesberg, J. A., Jackson, J., & Dawson, P. (2020). Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. *The British Journal of Criminology, 60*(6), 1502–1522.

Brewer, P. R., Bingaman, J., Dawson, W., Painstil, A., & Wilson, D. C. (2021). *Explaining public attitudes toward facial recognition technology*. Available at SSRN. https://doi.org/10.2139/ssrn.3897970.

Bromberg, D., Charbonneau, É., & Smith, A. (2020). Public support for facial recognition via police body-worn cameras: Findings from a list experiment. *Government Information Quarterly, 37*(1), Article 101415.

Brown, T. G., Statman, A., & Sui, C. (2021). Public debate on facial recognition technologies in China. In *MIT Case Studies in Social and Ethical Responsibilities of Computing, Summer 2021*. https://doi.org/10.21428/2c646de5.37712c5c

Buckley, O., & Nurse, J. R. C. (2019). The language of biometrics: Analysing public perceptions. *Journal of Information Security and Applications, 47*, 112–119.

Castro, D., & McLaughlin, M. (2019). Survey: Few Americans want government to limit use of facial recognition technology. In *Particularly for Public Safety or Airport Screening*. Center for Data Innovation. January 7 https://www.datainnovation.org/2019/01/survey-few-americans-want-government-to-limit-use-of-facial-recognition-technology-particularly-for-public-safety-or-airport-screening/ [accessed May 6, 2021].

Çelik, B. (2013). The politics of the digital technoscape in Turkey: Surveillance and resistance of Kurds. *New Perspectives on Turkey, 49*, 31–56.

Census.gov. (2022). International database census.Gov. Retrieved February 23, 2022, from https://www.census.gov/data-tools/demo/idb/#/pop?POP_YEARS=2022&menu=popViz&popPages=BYAGE&ageGroup=1Y&FIPS=CH.

Davidinev, D. W., & Silver, B. D. (2004). Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science, 48*(1), 28–46.

Davis, D. W., & Silver, B. D. (2004). Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science, 48*(1), 28–46.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

Degli-Esposti, S., & Gómez, E. S. (2015). Acceptable surveillance-orientated security technologies: Insights from the SurPRISE project. *Surveillance and Society, 13*(3/4), 437–454.

Dietrich, N., & Crabtree, C. (2019). Domestic demand for human rights: Free speech and the freedom-security trade-off. *International Studies Quarterly, 63*(2), 346–353.

Dijk, V., & Jan, A. G. M. (2005). *The deepening divide - inequality in the information society*. London, UK: SAGE.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-commerce transactions. *Information Systems Research, 17*(1), 61–80. https://www.jstor.org/stable/23015781.

Edison, S. W., & Geissler, G. L. (2003). Measuring attitudes towards general technology: Antecedents, hypotheses and scale development. *Journal of Targeting, Measurement and Analysis for Marketing, 12*(2), 137–156.

Feldstein, S. (2019). *The global expansion of AI surveillance*. Carnegie Endowment for International Peace. September https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 [accessed May 6, 2021].

Freude, A. C. H., & Freude, T. (2016). Echoes of history: Understanding German data protection. In *Newpolitik - German policy. Translated. Vol. 1, edited by Bertelsmann Foundation* (pp. 85–91). Gütersloh, DE: Bertelsmann Foundation.

Furnham, A. (1986). Response bias, social desirability and dissimulation. *Personality and Individual Differences, 7*(3), 385–400.

Gohdes, A. R. (2014). *Repression in the digital age: Communication technology and the politics of state violence*. PhD dissertation. Mannheim, DE: Universität Mannheim https://ub-madoc.bib.uni-mannheim.de/37902/ [accessed May 6, 2021].

Gray, M. (2003). Urban surveillance and Panopticism: Will we recognize the facial recognition society? *Surveillance and Society, 1*(3), 314–330.

Gunitsky, S. (2015). Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics, 13*(1), 42–54.

Habich-Sobiegalla, S., & Kostka, G. (2022). Sharing is caring: Willingness to share personal data through contact tracing apps in China, Germany, and the US. *Information, Communication & Society*. https://doi.org/10.1080/1369118X.2022.2113421

Hamann, K., & Smith, R. (2019). Facial recognition technology: Where will it take us? *Criminal Justice, 34*(1), 9–13. https://www.americanbar.org/content/dam/aba/publications/criminal_justice_magazine/spring-2019/cj-34-1-spring-2019-issue.pdf [accessed May 6, 2021].

Haraszti, M., Roberts, H., Villeneuve, N., Zuckerman, E., & Maclay, C. (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge, MA: Mit Press.

Harwell, D. (2019). FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches. *The Washington Post*. July 7 https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/ [accessed May 6, 2021].

Heek, V., Julia, K. A., & Ziefle, M. (2017). The surveillance society: Which factors form public acceptance of surveillance technologies? In M. Helfert, C. Klein, B. Donnellan, & O. Gusikhin (Eds.), *Smart cities, green technologies, and intelligent transport systems - SMARTGREENS 2016 and VEHITS 2016* (pp. 170–191). Cham, CH: Springer.

Interpol. (2021). Identifying terrorist suspects: Biometrics and battlefield data help police to identify terrorists. Interpol https://www.interpol.int/en/Crimes/Terrorism/Identifying-terrorist-suspects [accessed May 6, 2021].

Introna, L., & Wood, D. (2004). Picturing algorithmic surveillance: The politics of facial recognition systems. *Surveillance and Society, 2*(2/3), 177–198.

IPVM. (2021). Punishing Journalists PRC Province's Latest Mass Surveillance Project, Won by Neusoft Powered By Huawei, November 29 2021. https://ipvm.com/reports/henan-neusoft.

Ji, J., Guo, X., Zhang, M., & Feng, C. (2018). 人脸识别技术在高速公路打逃中的应用探讨 *[Pinyin: Rén liǎn shíbié jìshù zài gāosù gōnglù dǎ táo zhōng de yìngyòng tàntǎo, English: Discussion on Application of Face Recognition Technology in Highway [Toll] Evasion].*中国交通信息化 *[Pinyin: zhōngguó jiāotōng xìnxī huà, English: China ITS Journal]. 1*.

Jiang, J., & Yang, D. L. (2016). Lying or believing? Measuring preference falsification from a political purge in China. *Comparative Political Studies, 49*(5), 600–634.

Kostka, G. (2019). China's social credit systems and public opinion: Explaining high levels of approval. *New Media & Society, 21*(7), 1565–1593.

Kostka, G., & Habich-Sobiegalla, S. (2022). *In times of crisis: Public perceptions towards COVID-19 contact tracing apps in China, Germany and the US, New Media & Society*. April 2022. https://doi.org/10.1177/14614448221083285.

Kostka, G., Steinacker, L., & Meckel, N. (2021) (6th„ *30. Between security and convenience: Facial recognition technology in the eyes of citizens in China, the UK and the US* (pp. 671–690). Public Understanding of Science.

Krol, K., Parkin, S., & Sasse, A. (2016). "I don't like putting my face on the internet!": An acceptance study of face biometrics as a CAPTCHA replacement. In *Conference: IEEE ISBA 2016*. https://www.researchgate.net/publication/297788521_I_don%27t_like_putting_my_face_on_the_Internet_An_acceptance_study_of_face_biometrics_as_a_CAPTCHA_replacement [accessed May 6, 2021].

Lehdonvirta, V., Oksanen, A., Räsänen, P., & Blank, G. (2020). Social media, web, and panel surveys: Using non-probability samples in social and policy research. *Policy & Internet, 13*(1), 134–155.

Leibold, J. (2020). Surveillance in China's Xinjiang region: Ethnic sorting, coercion, and inducement. *Journal of Contemporary China, 29*(121), 46–60.

Liu, C. (2022). *Who supports expanding surveillance? Exploring public opinion of Chinese social credit systems*. International Sociology. https://doi.org/10.1177/02685809221084446

Liu, C., & Graham, R. (2021). Making sense of algorithms: Relational perception of contact tracing and risk assessment during COVID-19. *Big Data & Society, 8*(1). https://doi.org/10.1177/2053951721995218. Online first. [accessed May 6, 2021].

Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge, UK: Polity Press.

Lyon, D. (2017). Digital citizenship and surveillance| surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication, 11*, 824–842.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Cambridge: Polity Press.

Mann, M., & Smith, M. (2017). Automated facial recognition technology: Recent developments and approaches to oversight. *UNSW Law Journal, 40*(1), 121–145.

McCoy, S. (2002). O'big brother where art thou?: The constitutional use of facial-recognition technology. *John Marshall Journal of Computer & Information Law, 20*(3), 471–493.

Mičijević, A. (2019). Mehrheit der Deutschen befürwortet Einsatz von Gesichtserkennung – aber unter Auflagen. In *Handelsblatt, June 25*. https://www.handelsblatt.com/technik/digitale-revolution/digitale-revolution-mehrheit-der-deutschen-befuerwortet-einsatz-von-gesichtserkennung-aber-unter-auflagen/24491158.html?ticket=ST-1332294-00JZSmVJsOcgIZjEupDm-ap5 [accessed May 6, 2021].

Milligan, C. S. (1999). Facial recognition technology, video surveillance, and privacy. *Southern California Interdisciplinary Law Journal, 9*(1), 295.

Miltgen, C. L., Popovič, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "big 3" of technology acceptance with privacy context. *Decision Support Systems, 56*, 103–114.

Modahl, M. (1999). *Now or never: How companies must change today to win the battle for internet consumers*. New York, NY: Harper Business.

Murphy, R. (2004). Turning peasants into modern Chinese citizens:"Population quality" discourse, demographic transition and primary education. *The China Quarterly, 177*, 1–20.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79–119.

Pavone, V., & Degli-Esposti, S. (2012). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science, 21*(5), 556–572.

Prakash, A. (2018). Facial recognition cameras and AI: 5 countries with the fastest adoption. In *Robotics Business Review, December 21*. https://www.roboticsbusinessreview.com/ai/facial-recognition-cameras-5-countries/ [accessed May 6, 2021].

Ratigan, K., & Rabin, L. (2020). Re-evaluating political trust: The impact of survey nonresponse in rural China. *The China Quarterly, 243*, 823–838. https://doi.org/10.1017/S0305741019001231

Rhue, L. (2018). Racial Influence on Automated Perceptions of Emotions. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765.

Riemer, K., Ciriello, R., Peter, S., & Schlagwein, D. (2020). Digital contact-tracing adoption in the COVID-19 pandemic: IT governance for collective action at the societal level. *European Journal of Information Systems, 29*(6), 731–745.

Roussi, A. (2020). Resisting the rise of facial recognition. *Nature, 587*, 350–353. https://www.nature.com/articles/d41586-020-03188-2 [accessed May 6, 2021].

Samatas, M. M. (2005). Studying surveillance in Greece: methodological and other problems related to an authoritarian surveillance culture. *Surveillance and Society, 3*(2), 181–197.

Satariano, A. (2019). Police use of facial recognition is accepted by British court. In *The New York Times, September 4*. https://www.nytimes.com/2019/09/04/business/facial-recognition-uk-court.html [accessed May 6, 2021].

Shen, X., & Truex, R. (2021). In search of self-censorship. *British Journal of Political Science, 51*(4), 1672–1684.

Smith, A. (2019). *More than half of U.S. adults trust law enforcement to use facial recognition responsibly*. Pew Research Center. September 5 https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/ [accessed May 6, 2021].

Statistica. (2021). Internet usage in the United States - statistics & facts. Statista. Retrieved February 23, 2022, from https://www.statista.com/topics/2237/internet-usage-in-the-united-states/#dossierKeyfigures.

Su, F. (2019). Intelligent traffic management system drives collaboration for Shenzhen traffic police. Huawei https://e.huawei.com/de/publications/global/ict_insights/201902271023/Success-Story/201904161628.

The Nandu Personal Information Protection Research Center. (2019). 使用人脸识别 超七成受访者担心信息泄露 [The usage of facial recognition technology—over 70 percent worry about privacy issues]. Southern Metropolis Daily, December 6. http://epaper.oeeee.com/epaper/A/html/2019-12/06/content_52097.htm [accessed May 6, 2021].

Trüdinger, E.-M., & Steckermeier, L. C. (2017). Trusting and controlling? Political trust, information and acceptance of surveillance policies: The case of Germany. *Government Information Quarterly, 34*(3), 421–433.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 46*(2), 186–204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478.

Wadle, L.-M., Martin, N., & Ziegler, D. (2019). *Privacy and personalization: The trade-off between data disclosure and personalization benefit. In UMAP'19 adjunct: Adjunct publication of the 27th conference on user modeling, adaptation and personalization* (pp. 319–324). Association for Computing Machinery. https://doi.org/10.1145/3314183.3323672

Wichmann, M. (2016). Mehrheit der Bürger spricht sich nach Anschlag von Berlin für mehr Polizei und Videoüberwachung aus. *YouGov*. December 28 https://yougov.de/news/2016/12/28/mehrheit-der-burger-spricht-sich-nach-dem-anschlag/ [accessed May 6, 2021].

Wnuk, A., Oleksy, T., & Maison, D. (2020). The acceptance of Covid-19 tracking technologies: The role of perceived threat, lack of control, and ideological beliefs. *PLoS One, 15*(9), Article e0238973.

Wu, C., & Shi, Z. (2020). Education and social trust in transitional China. *Chinese Sociological Review, 52*(2), 115–143. doi:10/ghrx62.

Xu, X. (2020). To repress or to co-opt? Authoritarian control in the age of digital surveillance. *American Journal of Political Science, 65*(2), 309–325.

Xu, X., Kostka, G., & Cao, X. (2021). Information asymmetry and public support for social credit Systems in China. *Journal of Politics, 2022*. https://doi.org/10.1086/718358 [accessed August 21]

Zhang, B., Kreps, S., & McMurry, N. (2020). Americans' perceptions of privacy and surveillance in the COVID-19 pandemic. *PLoS One, 15*(12), Article e0242652.

Zhang, H., Guo, J., Deng, C., Fan, Y., & Gu, F. (2019). Can video surveillance systems promote the perception of safety? Evidence from surveys on residents in Beijing, China. *Sustainability, 11*(6), 1595. https://doi.org/10.3390/su11061595

Genia Kostka is Professor of Chinese Politics at the Freie Universität Berlin. Her research focuses on digital transformation, environmental politics and political economy with a regional focus on China.

Léa Steinacker, PhD, is a Lecturer at the University of St. Gallen and a researcher focused on the socio-technical dimensions of artificial intelligence, including facial recognition and speech synthesis technology.

Miriam Meckel is Professor of Communication Management at the University of St. Gallen, Switzerland. Her research focuses on digital skills and professional communication, (mis)information strategies on the internet and the social and economical impact of digital transformation.