



# Narratives in the nascent policy subsystem of AI biometrics

Patrick A. Stewart<sup>1</sup> , Jeffrey K. Mullins<sup>2</sup> and Thomas J. Greitens<sup>3</sup>

<sup>1</sup>Department of Political Science, University of Arkansas, Fayetteville, AR, USA; <sup>2</sup>Department of Information Systems, University of Arkansas, Fayetteville, AR, USA and <sup>3</sup>School of Politics, Society, Justice & Public Service, Central Michigan University, Mount Pleasant, MI, USA

**Corresponding author:** Patrick A. Stewart; Email: [pastewar@uark.edu](mailto:pastewar@uark.edu)

## Abstract


The Biden administration requested comments regarding “Public and Private Sector Uses of Biometric Technologies” in the Federal Register from October 2021 to January 2022. This generated 130 responses, helped shape the “Blueprint for an AI Bill of Rights,” and resulted in Executive Order 14110 on “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.” While the Trump administration immediately rescinded this executive order, these comments provide insight into salient AI biometrics technologies and relevant political players. We first identify AI biometric technologies before asking which institutions and individuals commented (RQ1), and what the substance and tenor of responses were regarding the opportunities and threats posed by AI biometrics (RQ2-a) based on respondent type (RQ2-b). We use text mining and qualitative analyses to illuminate how uncertainty about AI biometric technology in this nascent policy subsystem reflects participants’ language use and policy preferences.

**Keywords:** biometrics; artificial intelligence; science and technology policy; nascent policy subsystem; advocacy coalition framework

## Introduction

With the proliferation of artificial intelligence (AI) and its potential to radically reshape society without much public recourse, the U.S. federal government has, over the past decade, (Hine & Floridi, 2023; Robles & Mallinson, 2023; Schiff, 2023) initiated both formal and informal policy discussions regarding the appropriate roles for AI in general and the public policies that should be implemented. Despite the publicly visible AI policy discussions occurring at the federal level from 2016 to 2020 (Schiff, 2023), there has been, in general, a lack of coherent and overarching U.S. federal policy for governing AI (Robles & Mallinson, 2023) with this technology addressed in a piecemeal fashion by states and cities. The disjointed nature of federal policy can be seen with the Biden Administration implementing Executive Order (EO) 14110 on “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence” (Biden, 2023), only to see it rescinded by the Trump Administration with EO 14179 (Trump, 2025) and a resultant “Request for Information on the Development of Artificial Intelligence Action Plan” (National Science Foundation [NSF], 2025).

While the current majority of AI use—and hype—centers on the written word (Spisak, 2023; Spisak et al., 2021), perhaps the most concerning use of AI interfaces with the “real world” of human identity and behavior through biometric technologies. These AI-enabled biometrics (hereafter, AI biometrics)

 This research article was awarded Open Data badge for transparent practices. See the Data Availability Statement for details.

© The Author(s), 2025. Published by Cambridge University Press on behalf of The Association for Politics and the Life Sciences. This is an Open Access article, distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives licence (<http://creativecommons.org/licenses/by-nc-nd/4.0>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided that no alterations are made and the original article is properly cited. The written permission of Cambridge University Press must be obtained prior to any commercial use and/or adaptation of the article.

threaten to transform core aspects of humanity in terms of identity and behavior through both overt and covert collection of a broad range of physiological data and inferences based upon algorithmic interpretation. In 2021–2022, federal policy surrounding AI biometrics began to develop as the White House's Office of Science and Technology Policy (OSTP) requested public comments regarding "Public and Private Sector Uses of Biometric Technologies" in the Federal Register. This was used to inform policymakers regarding this nascent policy subsystem for the publication of the "Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People" (hereafter, "Blueprint"). The Blueprint thus provided an official policy forum that collected public comments to identify the numerous concerns and challenges from biometric technologies incorporating artificial intelligence—i.e., AI biometrics. Arguably, this was the first significant forum for shaping U.S. federal AI biometric policy, establishing the key technologies, stakeholders, and concerns likely to influence future regulatory discussions (Perry & Uuk, 2019). Accordingly, in this paper, we first identify and explain AI biometric technologies to distinguish between first- and second-generation biometrics. Next, we consider the institutions and individuals involved to answer our first research question (RQ1): *What are the characteristics of the commenters on the OSTP's request on biometric technologies?* We then analyze the substance and tenor of responses regarding the opportunities and threats posed by AI biometrics by asking (RQ2-a): *How do narrative strategies relate to the generation (first or second) of AI biometrics?* and (RQ2-b): *How do narrative strategies vary based on commenter characteristics?*

The initial development of the Blueprint as it relates to AI biometrics presents a unique opportunity to identify policy stakeholders and their positions regarding specific technologies, narrative strategies, and policy suggestions well before policy subsystems and governance instruments coalesce. We analyze the public comments used to develop the Blueprint based on theory and concepts from the Advocacy Coalition Framework (ACF) while building on existing AI policy analyses (Lemke et al., 2023; Schiff, 2024; Schiff & Schiff, 2023). In the following sections, we first define AI biometrics based on their generation, which in turn is premised upon whether the goal is identification (first-generation) or behavioral inferences (second-generation). From there, we use theoretical constructs from the ACF to characterize this U.S. federal policy subsystem as nascent i.e., a collection of new and emerging biometric technologies driven by computational advances, combined with a lack of established coalitions uniting around specific, identifiable policy preferences. We then consider narrative strategies used by the different types of participants commenting; specifically, we assume that the amount and type of content will reflect the commenters' backgrounds and (arguably) inherent strategies. The penultimate section involves a qualitative consideration of the comments based on the policy preferences proffered. We then provide tentative conclusions based on the analyses.

## Defining AI biometrics

Although AI biometrics, and fears regarding their use, have most recently entered elite and public discourse thanks to facial recognition technologies (FRT) misidentifying individuals based on their gender and ethnicity (Buolamwini & Gebru, 2018), biometrics of various sorts have been used for millennia to systematically and formally identify individuals. Specifically, fingerprints had been used in Babylonian business transactions as early as the fifth century BC and by the Qin dynasty in the third century BC as a means to identify individuals concerning their eligibility for civil service examinations and in mercantile transactions (Jain & Kumar, 2012; Sutrop & Laas-Mikko, 2012). Since the early 1900s, fingerprinting has been established as the major means of identifying criminals, with the Automatic Fingerprint Identification System (AFIS) being used by nearly all law enforcement agencies throughout the world (Jain & Kumar, 2012; Woodward, 1997). More recently, DNA analysis has embedded itself as a cultural norm in the identification of individuals, especially in the criminal justice system, where it has been used to help convict or exonerate individuals. In short, the systematic identification of individuals based on relatively immutable physical characteristics for official purposes has a long and established history.

With advances in sensing technology and the emergence of AI, the potential for individuals to be identified without their consent—or even their knowledge—compounded with algorithmic inferences

regarding their emotions and cognitions, behavioral tendencies, and personality traits has elevated public concern. For instance, the grocery store Kroger was considering the use of AI-enabled facial recognition technology to enable “surveillance pricing” in which different customers would be charged different prices based on their shopping habits and financial circumstances (Smalley, 2024). This use of AI biometrics has met with extensive concern among lawmakers, at least at the state level. To better understand the technologies operating under the banner of “biometrics,” this section considers the various tools biometrics comprises and organizes them based on how intrusive they are to the average individual. In other words, biometrics can be considered based on (1) the purposes for which they are used, and (2) how intrusive the data collection is in terms of potential privacy violations.

The purposes for which biometric tools are used can be categorized into two distinct generations. Sutrop and Laas-Mikko (2012) provide a useful distinction for organizing specific biometric tools in this manner. They see first-generation biometrics as being concerned with identity verification: “first generation biometrics use characteristics readily visible to the naked eye to ensure that the person identified is the person he claims to be” (2012, p. 21). The second generation of biometrics “focus on behavioral patterns with the aim of predicting suspicious behavior or hostile intentions” (2012, p. 21). While Sutrop and Laas-Mikko argue that “the difference between first- and second-generation biometrics lies in the awareness of the fact that data are collected” (2012, p. 31), an extension of this perspective is to consider how intrusive these biometric technologies are, especially as various forms stand to become a part of everyday life. Factors that play a role in how intrusive—and potentially threatening—a biometric technology’s application might prove to be (see Table 1) can include the physical invasiveness of a tool, how overt or covert data collection might be, and what level of consent should be required to acquire information (Jain & Kumar, 2012).

First-generation biometrics: identity

The first and arguably least objectionable level of first-generation biometric technology may be seen in DNA/genetic technology and dental forms of identification. DNA/genetic technology most often requires samples of blood, mouth scrapings, or hair roots to best process nuclear and/or mitochondrial

**Table 1.** Intrusiveness of first- and second-generation biometrics and % mentions in Federal Register comments on “Public and Private Sector Uses of Biometric Technologies”

	Level of physical invasiveness	Potential for covert collection	% mentions in federal register
<b>First-generation biometrics</b>			
Facial recognition	Low	High	65.4%
Vocal recognition	Low	Moderate-to-high	22.3%
Dental	High	Low	1.5%
DNA/genetics	High	Moderate	16.2%
Fingerprints/handprints	Moderate	Moderate	23.8%
Iris/retina recognition	Moderate	Low	18.5%
<b>Second-generation biometrics</b>			
Posture/head/body movements	Low	High	6.2%
Keystrokes/mouse movements	Moderate	High	7.7%
Psychophysiology	Moderate-to-High	Low-to-moderate	6.9%
Language and vocalics	Low	Moderate-to-high	3.1%
Facial/other behavior	Low	Moderate-to-high	24.6%
Other (GPS/geofencing, sensors, etc.)	Low	Moderate-to-high	9.2%

DNA (Jain & Kumar, 2012). Because DNA quality decays with time, obtaining samples with consent and then processing them in a timely manner leads to more accurate identification. With dental identification, an individual must either bite down on something, with a mold being taken, or the mouth itself must be inspected physically for dental identifiers or through scanning technology such as the dental cone beam computed tomography scan and panoramic radiographs (Franco et al., 2019). In both these approaches, consent is more likely to be required due to the physically invasive nature of these biometric tools.

By comparison, iris and retina scans as well as fingerprint/hand printing may be seen as slightly less intrusive than DNA or dental identification due to their increasingly common use in everyday activities. Because individuals must be proximate to scanners for these forms of biometrics—especially iris and retina scans in which they must look directly into a camera—there is a level of choice that offers at least the perception of control. However, especially with fingerprints, traces can be left—as is the case with the “gummy bear spoofing” attacks in which gelatin molds can stand in for the actual fingerprints. Likewise, individuals can avoid leaving traces of their fingerprints by wearing gloves or wiping surfaces after handling them. The hand, for its part, may provide a range of biometric measures, starting with the fingerprint with its distinctive patterns of ridges and valleys, and extending to palm prints, hand geometry (length, width, thickness, and height of the hand and fingers), and patterns of blood vessels and veins in the hands of individuals (Jain & Kumar, 2012; Woodward, 1997).

Finally, the most intrusive of the first generation of biometric technologies is facial recognition technologies (FRT) (Hill, 2023; Spisak, 2022) and to a lesser extent, vocalic recognition technology (Turow, 2021). This is because Western social norms and expectations are that individuals are anonymous unless they are aware and give consent to being recognized via these means. While authentication and verification, especially with personal accounts and technology, can be seen as a valid and acceptable use of both FRT and vocalic recognition technology, identification, especially in contexts where anonymity is assumed, can be cause for concern—and political action.

### *Second-generation biometrics: behavioral inferences*

Although Sutrop and Laas-Mikko’s definition of second-generation biometrics emphasizes “suspicious behavior or hostile intentions” and thus limits their scope to law enforcement and national defense (Sutrop & Laas-Mikko, 2012), a more inclusive definition has emerged recently. Specifically, second-generation biometrics may be seen as considering behavior and psychophysiology more generally, with indicators often used to make inferences about intent and personality. These inferences are then used for a broad range of purposes, such as education, marketing, human resource management, health care, and so on.

Such biometrics as posture, head, and other body movements, including walking gait and gestures, may be seen as low in the level of physical invasiveness due to the gross physical movements involved, which can be seen from a distance. Because of the low resolution needed to map these movements, identity does not necessarily need to be established; however, for these same reasons, this information may be potentially collected in a covert manner.

For their part, keystroke and mouse movements while working on computers can be seen as moderately physically invasive, as they involve tracking an individual’s behavior directly, and can even be used to infer emotions and other psychological states (Hibbeln et al., 2017). This same behavior can be—and has been—covertly collected unless individuals are directly and constantly informed that their outputs are being.

Psychophysiology, which can be seen as encompassing a range of measures such as EKG, EEG, galvanic skin response, heart rate, blood pressure, and breathing patterns (McStay, 2018; Potter & Bolls, 2012; Settle et al., 2020), can be seen as having varying levels of physical invasiveness based upon on how the data is collected. For instance, some of these measures require the physical contact of sensors with the individual for data collection. The growing use of wearables such as watches, rings, and other devices has made this commonplace. On the other hand, such indicators as heart rate, breathing patterns, and

temperature may be observed through video and other remote sensors from a distance and thus covertly collected.

With vocalics and natural language collection, there has been an advance in the ability to extract increasingly diverse types and precise levels of information, with advances in hardware and software algorithms leading to better discrimination between signal and noise (Turow, 2021). At the same time, these advances are decreasing the level of physical invasiveness while increasing the covertness by which information may be collected—much in the same manner that first-generation vocal recognition has become more commonplace, accurate, and ultimately invasive in everyday matters (Turow, 2021).

Facial and similar behavior collected through such tools as automated facial expression analysis and eye tracking, as well as pupillometric measuring dilation of pupils, can be used to infer attention, emotion, cognition, and behavioral intent (Delmas et al., 2024; Zhang et al., 2021). Because current technology relies upon video in which the face and eyes are captured relatively head-on, the potential for covert data collection can currently be seen as moderate, albeit with the potential to be much higher e.g., through the use of video conferencing tools (Bailenson, 2021; Mullins et al., 2022; Zhang et al., 2021).

Finally, the catchall category “other” includes technologies currently in use that are not directly connected to individual physiology, but that track and can limit behavior through such technologies as GPS sensors in vehicles and cell phones, or geofencing based on this information (Farahany, 2023). It also includes technologies currently being developed such as biosensors in clothing and furniture and such “invasive systems” as password pills powered by stomach acid, tattoos, and embedded wireless antennae. While there are obviously varying levels of physical invasiveness involved, it can be expected that the potential for covert data collection will range from moderate to high.

### U.S. federal policy development on AI biometrics

Concerns about the impact of AI in general escalated from 2016 to 2020 (Schiff, 2023) as a series of media stories about the ethics and impact of AI on everyday life and the nation’s security began to proliferate (Chuan et al., 2019; Galanos, 2019; Neri & Cozman, 2020). While the development of AI regulatory policies at the federal level appears to have stalled under the Trump administration with its focus on economic competitiveness, these stories help frame the policy challenges at all levels surrounding AI applications (Schiff, 2023), with increased public awareness and associated U.S congressional attention, especially regarding AI ethics (Schiff, 2024). As part of an agenda-setting process, the federal government and numerous international governments have begun to consider how to effectively govern AI applications (Taeiagh, 2021).

The resulting government publications (e.g., the Blueprint) address AI more generally, suggesting that the impact of AI was essentially unclear, the types of technology being used are dynamic and advancing rapidly, and the resultant developments are outpacing the ability of the current governmental policy process to proactively manage this area (Harris, 2021). In short, not only is there uncertainty regarding the technology itself, but also ambiguity about how to best use policy to address AI (Schiff, 2023; Zahariadis, 2019).

### Characterizing the AI biometric policy subsystem

The discussion around AI biometrics can be seen as developing within what is defined by the ACF as a “nascent policy subsystem.” This is largely due to AI biometrics being a topic new to the policymaking process (Henry et al., 2022; Ingold et al., 2017; Lemke et al., 2023; Nohrstedt et al., 2023; Stritch, 2015), whereas most mature policy subsystems have been in place for more than a decade, allowing for coalitions to form based upon shared core beliefs and/or policy preferences and providing evidence of this through a series of interactions (Sabatier, 1991; Weible & Sabatier, 2018). While AI has had a long scientific and technical gestation period, its comparatively sudden rise in practice as a transformative technology with significant societal impacts arguably left it without an obvious policy subsystem home.

Nascent policy subsystems occur when new issues arrive on the political agenda but are not absorbed into a mature policy subsystem (Henry et al., 2022; Lemke et al., 2023; Nohrstedt et al., 2023). As a result, clear coalitions are not easily discerned, there is an absence of policy forums/venues for discussion whereas decision-making or collective action may occur, and confusion exists regarding the proper jurisdictions to litigate conflicts and make policy decisions—whether public or private (Bonnicksen, 1992)—or to recommend options for moving forward (Nohrstedt et al., 2023). While it may be seen that there is a lack of clear coalitions regarding how AI is generally addressed (Schiff, 2023), the specific challenges of AI biometrics underscore and accentuate it as a nascent policy subsystem.

In what appears to be an attempt to deal with increasing public concern regarding AI biometrics—especially regarding the use and misuse of FRT—the Biden Administration can be seen as having opened an official policy forum (Henry et al., 2022) by inviting comments from the general public and interested parties to provide a venue for discussion of this nascent policy topic. More specifically, the OSTP request for information regarding “Public and Private Sector Uses of Biometric Technologies” provided individuals and organizations the opportunity to present insights and register concerns regarding AI biometrics in the official U.S. federal government record, the Federal Register. Even with the Trump Administration rescinding the resulting executive order and concomitantly issuing their own call for comments in a reframing of the AI issue, the fundamental policy issues and players remain. As a result, an important first step (RQ1) is to identify and organize those commenting based on their sector and/or identity and, for organizations other than academia, their tax status and the year they were founded.

### *Applying the narrative policy framework to understand AI biometric policy*

The key to understanding nascent policy subsystems is recognizing how competing groups and individuals express their policy narratives. Policy narratives are used by groups to communicate their policy beliefs in a strategic manner (Jones & McBeth, 2010; Shanahan et al., 2011; Stone, 1997; Zahariadis, 1995) with these narratives exhibiting key characteristics related to settings, characters, plot, and story themes (or story morals) (Shanahan et al., 2018).

For AI policies more generally, narratives have been dominated by hype regarding the innovative capacity of the technology and its ability to provide competitive advantage to the nation, as well as a lack of understanding of just what it is capable of accomplishing. These are accompanied by ethical concerns raised by its presumed transformative power (Schiff, 2024). For example, two dominant narratives of policy beliefs emphasizing ethical concerns and economic opportunity emerged during the agenda-setting stage of AI-based policies from 2016 to 2020 (Schiff, 2023). In short, AI continues to be an uncertain and ambiguous technology that is rapidly evolving and transforming on an almost daily basis (Chuan et al., 2019; Galanos, 2019; Neri & Cozman, 2020; Spisak et al., 2021).

Given these conditions of uncertainty, ambiguity, concern, and fear arising from AI’s societally transformative possibility, the role of policy narratives becomes especially important from a policy analysis perspective. This is borne out by a field experiment that showed the powerful role played by narratives in having legislators attend to and learn about AI (Schiff & Schiff, 2023). Specifically, they found that “while the provision of expert information by policy entrepreneurs remains influential, the provision of narratives was at least as likely to gain policy maker attention” (2023, p. 18). Their findings suggest that while expert knowledge does play an important role in capturing interest, so too does the ability to effectively tell a story.

For the policy subsystem of AI biometrics, the type of narrative strategy used may be seen as driven by either the type of biometric technology being referred to or the nature of the commenter (RQ2-a). More specifically, the extensiveness of an argument made as well as its rhetorical nature, e.g., whether appeals are made to logic, authority, or emotion, reflects the strategy employed. In the case of technology type, the amount and content of the comments may be driven by how AI biometrics are defined, whether as first-generation, identity-focused biometrics; second-generation, behavior-focused biometrics; biometrics inclusive of both generations, or AI as an abstract classification.



Alternatively, the narrative approach may be driven by commenter characteristics (RQ2-b). Specifically, private industry and trade associations have distinctly different goals than do private citizens, public-facing nonprofits, and even academics—although this latter group may show more heterogeneity due to their involvement with the development of the science behind the technology.

### Creating a U.S. federal policy forum on AI biometrics: The AI Bill of Rights

In early 2021, the OSTP published a “request for information” in the Federal Register on the “public and private sector uses of biometric technologies” that encouraged the public to submit comments for review as the White House considered new policies surrounding AI, biometrics, and AI biometrics. Those comments, made from October 8, 2021, to January 15, 2022, helped OSTP formulate the Blueprint, which in turn led to the formulation and implementation of EO 14110 on October 30, 2023, to establish a government-wide effort to develop new AI-based standards for safety, security, privacy protection, innovation, and civil rights (Biden, 2023; Harris & Jaikaran, 2023). While official legislative and/or regulatory action has yet to occur, these comments provide insights into the values, goals, and expectations of stakeholders in the official record provided by the Federal Register and ultimately inform the creation and publication of a framework for policy development and the issuance of a federal Executive Order to federal agencies.

### Content analyzing the Federal Register

In a fast-moving technology-driven policy arena such as is the case with AI biometrics, federal regulations are largely driven at the policy subsystem level by executive agencies. This is due to legislative institutions being slow, unwieldy, and largely underprepared to address the complex, highly technical, and accelerated pace at which inventions and innovations affect public life. Furthermore, there is the temptation to use preexisting regulations to address novel and unpredictable technologies, as has been the case with advances in the life sciences through genetic technology (Bonnicksen, 1992; Stewart & Knight, 2005). Changes that do occur through rulemaking can be seen as occupying, in the words of Hwang and colleagues (Hwang et al., 2014) “an often contradictory space in the modern administrative state, as an instrument of bureaucratic agency and a forum for democratic governance.” (p. 73).

Being aware and making use of the official federal government record, the Federal Register, is key for parties involved with public policymaking, especially as federal agencies issue regulations based upon statutory authority granted by Congress (Carey, 2013). Published in the 1930s with the expansion of the federal government due to the New Deal, the Federal Register provides a mechanism through which the public and other interested parties may provide feedback on federal rulemaking (Carey, 2013). For areas that are technically complex, requiring expertise and a level of sophistication of understanding, comments are often limited to insiders and highly motivated parties (Hwang et al., 2014; West & Raso, 2013). For instance, Stewart and McLean found that comments in the Federal Register on agricultural biotechnology were largely limited to interest groups, trade associations, and business interests (1993 = 84; 1997 = 50). Likewise, Hwang and colleagues found that “for the twenty-seven most economically significant rules the FDA has pursued since 2000, the agency received a median of one hundred comments per rule (range: 12–48,000)” (2004, p. 757).

While the advent of easy access to the Federal Register’s electronic docket enhanced the ability of the public to show their concern, these comments tend to be brief and often prompted by organized and powerful interests. Specifically, Stewart and McLean found that comments to the Federal Register in 2003 to plant-made pharmaceutical regulations increased to 847, of which around 600 were cut-and-paste forwards; this, however, did not come close to the over 275,000 comments made in response to whether genetically modified crops could be considered “organic” (Stewart & McLean, 2004). Likewise, public comments on FDA rules regarding medical technologies (Hwang et al., 2014) and tobacco products (Hemmerich et al., 2017) show prompting by established business and interest groups. In short, while the

general public does get involved in shaping policy, the specific attributes of the policy itself are driven, more often than not, by organized interests.

While the Federal Register provides insights regarding overall trends in federal government activity more generally (Carey, 2013) and patterns of business, government, and nongovernmental agency involvement in the normal business of rulemaking (Yackee & Yackee, 2006), close scrutiny of the comments themselves can provide insights regarding definitions, policy positions, and narrative strategies engaged in by the various interested parties. This approach is especially important when considering emerging technologies in the policy forums/venues of nascent policy subsystems, especially as perceptions can drive emotional response that (Stewart & McLean, 2004), in turn, can presage if not influence the policymaking that occurs in legislative arenas.

### *Methods for analyzing “Public and Private Sector Uses of Biometric Technologies”*

The approach used here was a content analysis of Federal Register comments in which the OSTP requested “input from interested parties on past deployments, proposals, pilots, or trials, and current use of biometric technologies for the purposes of identity verification, identification of individuals, and inference of attributes including individual mental and emotional states.” (Notice of Request for Information [RFI] on Public and Private Sector Uses of Biometric Technologies, FR 186 [193]: 56300–56302). The comment period started on October 8, 2021, and officially ended on January 15, 2022, although it was extended to January 26. Commenters were limited to 10 pages of comments, with the results published on October 12, 2022.

Analysis of the 1,099 pages comprised of 130 comments, involved a qualitative review of each of the comments in which extensive notes were taken regarding “biometrics,” “regulatory suggestions,” and “additional comments.” Different types of biometric tools were identified in the comments and then assigned as either first- or second-generation based on how they would be used. Policy instruments were defined based on the regulatory suggestions made in the comments and categorized by two of the authors referring to Lemke and colleagues’ five-category scheme in their exploration of Germany’s AI policy (Lemke et al., 2023). These categories involve: (1) non-state action; (2) information and education; (3) cooperation and coordination; (4) investments and incentives; and (5) regulation and legal frameworks.

Additionally, information was collected regarding the nature of the commenters based on whether they were private citizens, academics, business entities, and nonprofit organizations. For business entities, the Securities and Exchange Commission electronic filing website EDGAR (electronic data gathering, analysis, and retrieval) database was queried along with internet searches to establish whether business entities were publicly traded or not, with their absence indicating they were privately held. For the nonprofits, the IRS website allows for searches regarding tax-exempt organization status (990-*n*) based upon EIN (employer ID numbers) with determination letters, as well as tax returns from 2021, seen as indicating whether the organization was a public-facing nonprofit or social welfare organization (501c3 and 501c4, as well as international charities) or trade associations focused on membership goals (501c5, 501c6, and 509a1). Furthermore, information regarding the founding date of organizations was noted to consider their provenance in this nascent policy subsystem.

To consider the overarching narrative strategy, we analyzed the content of comments using the Linguistic Inquiry and Word Count (LIWC) software, after citations and added materials were removed. LIWC is a text analysis tool that associates words in a text with different psychological, social, or linguistic categories. Words can fall into multiple LIWC categories, and most categories are arranged hierarchically (e.g., the word “cried” is categorized in all the following hierarchical categories: affect, emotion, negative emotion, sadness). LIWC compares a text sample with its built-in dictionary to categorize each word and provides a measure indicating the proportion of words from the sample that fall into each category. Thus, the software can be used to understand the overall tone, emotion, or other psychosocial patterns of text samples (Pennebaker et al., 2015). For this study, we used LIWC 2022,



which has been validated using the Test Kitchen Corpus (TKC) which in turn was constructed from random subsets of text drawn from 15 different English language data sets, each containing 1,000 texts (Boyd et al., 2022).

LIWC includes summary variables in addition to proportion-based measures of text categories. The summary variables include raw measures (e.g., word count, words per sentence), and a set of calculated and validated measures for analytical thinking, clout, authenticity, and emotional tone. Proportion-based measures include linguistic dimensions of the text (e.g., parts of speech, pronouns) as well as psychological and social categories. Each measure indicates the proportion of words, on a scale of 0 to 100, from the response that falls into each category (Boyd et al., 2022). As a reference point, grand means for all LIWC reference datasets and means for the *New York Times* can be assessed for analytic thinking ( $M_{\text{grand}} = 56.34$ ;  $M_{\text{NYT}} = 92.57$ ), clout ( $M_{\text{grand}} = 57.95$ ;  $M_{\text{NYT}} = 68.17$ ), positive emotional tone ( $M_{\text{grand}} = 3.67$ ;  $M_{\text{NYT}} = 2.32$ ), and negative emotional tone ( $M_{\text{grand}} = 1.84$ ;  $M_{\text{NYT}} = 1.45$ ) and used as a comparison point.

For the purposes of this study, we consider the summary variables of word count, analytic thinking, and clout, and we consider affective processes based on positive and negative tones. With word count, we obtain a measure—albeit incomplete due to the potential for extensive citations and supporting documentation (which were removed from the analyzed text but contributed to the Federal Register length limit)—of effort placed into the comment. Analytic thinking and clout provide proxy measures for maintaining or even contracting, the scope of conflict by making arguments that are based on logic and authority, respectively. We measure emotional tone as two dimensions based on extensive research suggesting that—at least linguistically—emotion loads in an orthogonal manner on two factors of positive and negative affect (Brader, 2006; Marcus et al., 2000; Scherer & Meuleman, 2013). This approach has been used successfully in the policy literature to understand individual responses, with specific attention being paid to worry and anxiety (Lablih et al., 2024; Stewart & McLean, 2004).

To test mean differences in linguistic measures between focal AI biometric generations and the type of commenter, we conducted an Analysis of Variance (ANOVA). We expect those attempting to expand the scope of conflict to use emotion-based language in hopes of social contagion with a resultant affective response in those involved (Shanahan et al., 2018).

## Findings

### Biometric technologies

The majority of commenters referred to first- (60.8%) or second-generation (37.7%) biometrics specifically, while nearly one-third identified both first- and second-generation biometrics (30.8%) in their Federal Register comments (see Table 1). However, over one-fifth did not identify any specific form of biometric (22.3%). In most of these latter cases, AI and biometrics were more generally referred to by the commenters as issues of concern. In summary, first-generation biometrics provided the greatest proportion of concern and interest on their own. That said, a substantial number of commenters did not differentiate in terms of specific AI biometrics, instead responding to it as an entire class.

When specific types of biometric tools are considered, as observed in Table 1, by far the most commented upon form of first-generation biometric was that of FRT, which was seen in nearly two-thirds of all comments (65.4%), well over two-and-a-half times more than traditional and well-known forms of biometrics, that of fingerprinting and associated finger/hand biometrics (23.8%). That voice recognition technology (VRT) was the third most commented upon first-generation biometric suggests that both FRT and VRT might have commonalities based on their level of intrusiveness. For their part, forms of recognition in which eyes are scanned showed up in just under 20% of comments, followed by DNA/genetic-based recognition technologies at 16.2%, whereas dental-based forms of biometrics were rarely mentioned.

Second-generation biometrics in which behavioral patterns are observed, and as a result, personal traits, cognitions and emotions, and behavioral intent inferred, are mentioned in over one-third of the

comments. The types of technologies referred to are quite diverse but may be seen as connected with first-generation technologies. For instance, facial behavior and vocal tone and language may be seen as technological offshoots of FRT and VRT, respectively. Similarly, inferences based on eye movements and pupil dilation evolved from iris and retina scans. However, such activities as posture, gait, and body and limb movements, while mentioned in some comments, were most often not a central focus. These second-generation biometrics were often bundled with other technologies as attempts to surveil individuals, such as computer keystrokes and mouse clicks as well as the tracking of people and vehicles through sensors. Regardless, due to these second-generation biometrics often being seen as collected without the awareness and consent of the target, there was substantial concern and interest raised.

### *Commenter characteristics*

Those commenting in the Federal Register to inform the OSTP AI Bill of Rights can be seen as reflecting a broad spectrum of interests and concerns (see Appendix). While private citizens comprise 10% of the respondents ( $n = 13$ ; 10%), suggesting this policy forum is relatively insulated due to the expertise required to keep track of AI biometrics, the involvement of government agencies ( $n = 4$ ; 3.1%), public-facing nonprofit interest groups ( $n = 44$ ; 33.8%), and academic-driven comments ( $n = 29$ ; 22.3%) suggest there is a level of concern counterbalancing trade associations ( $n = 13$ ; 10%) and private firms ( $n = 27$ ; 20.8%) which presumably are interested in the economic benefits provided by the implementation of AI biometrics.

Of the nonprofits and trade associations, a substantial proportion were started within a decade of the Federal Register's request for comments ( $n = 12$ ; 20%). Specifically, three of the 13 trade associations were founded in the 10-year window prior to the Federal Register call, whereas of the 44 publicly facing interest groups commenting, nine were founded during the same window. Notably, three interest groups (Electronic Frontier Foundation, Center for Digital Democracy, and the Consumer Federation of America) collaborated on one comment, whereas no other organizations did so. In brief, the nature of the commenters suggests a nascent and growing policy subsystem.

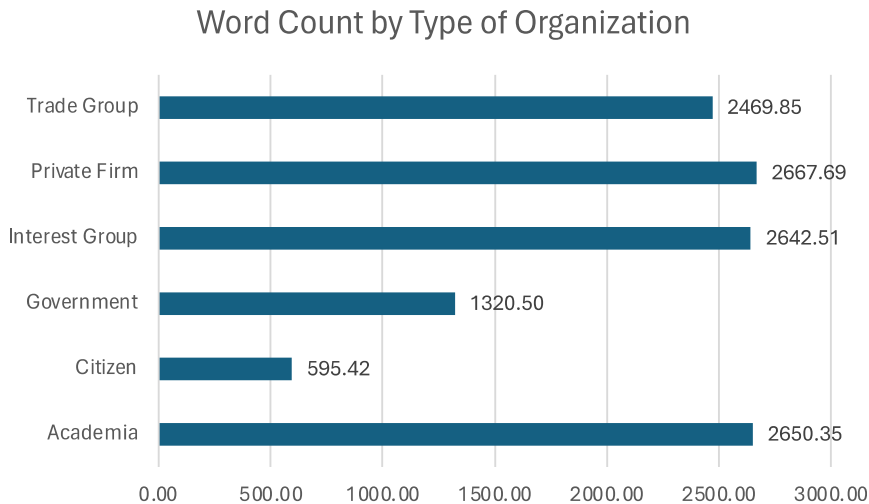
Of the private firms, as expected, most of the 17 publicly traded firms have a long history, with only two (Onfido—2012 and Pangiam—2020) being founded during the decade before the OSTP call (another two, CLEAR and ID.me were founded in 2010). On the other hand, seven of the 10 privately held firms commenting were founded in 2011 or afterward, with only the Dev Technology Group (1998) and InventionPhysics (2004) having a slightly longer history as ongoing concerns (Cyber Farm Labs, befitting its cybersecurity focus, did not leave an electronic footprint allowing for an inception date to be established).

### *LIWC analysis of Federal Register comments on AI biometric generation*

Findings regarding differences in word count based on biometric generation suggest there are significant differences. Further analysis, when entering the presence of each generation of biometric, both alone (First Generation,  $F(1, 126) = 9.625, p = .002$ ; Second Generation,  $F(1, 126) = 3.715, p = .056$ ) and their interaction,  $F(1, 126) = 0.017, p = .897$ , suggests these differences are largely driven by those not referring to specific AI biometrics; in other words, those commenters using fewest words are those not identifying any specific biometric. On the other hand, those referring to both first- and second-generation biometrics use the greatest number of words. However, when analytic language, clout-based words, and the two dimensions of emotional tone (positive and negative) are considered, no significant differences based on generation of biometric technology are found.

### *LIWC analysis of Federal Register comments on commenter characteristics*

Consideration of differences between commenters in terms of word count, with the 10-page ceiling placed on responses, suggest significant differences between the groups,  $F(5, 124) = 6.372, p < .001$ . Analysis of Figure 1 shows this is driven by substantially briefer comments by private citizens and subnational government institutions. By comparison, academics, interest groups/nonprofit

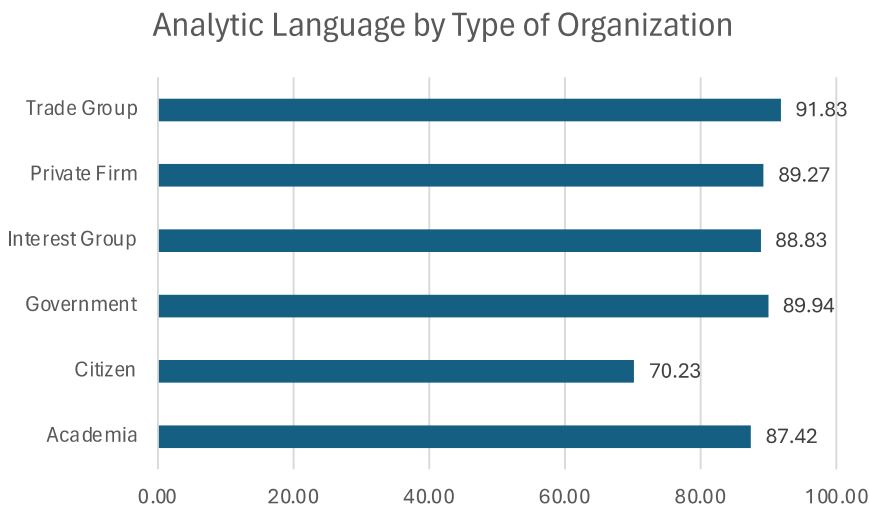


**Figure 1.** LIWC word count by type of organization.

organizations, trade associations, and private business firms submitted comments of similar length to each other, apparently making full use of the page length available to them.

The length of the comments, to an extent, may be seen as reflected in the use of analytic language as there again are significant differences between commenters,  $F(5, 124) = 7.113$ ,  $p < .001$ . This was driven by private citizens using substantially less analytic language in their comments than all others (see Figure 2). This likely reflects the substantial resources available to the organizations and individuals involved, especially as there are relatively high analytic scores which are well above LIWC's average (56.34) and comparable with the *New York Times*' average analytic score (92.57).

Clout, on the other hand, was not significantly different between commenters,  $F(5, 124) = 1.411$ ,  $p = .225$ . Moreover, the scores were comparatively low in comparison with both analytic thinking (see Figure 3) and with comparison points of LIWC's and the *New York Times*' averages (57.95 and 68.17), suggesting the language of leadership and status did not play a major role in the strategies of commenters.



**Figure 2.** LIWC analytic language by type of organization.

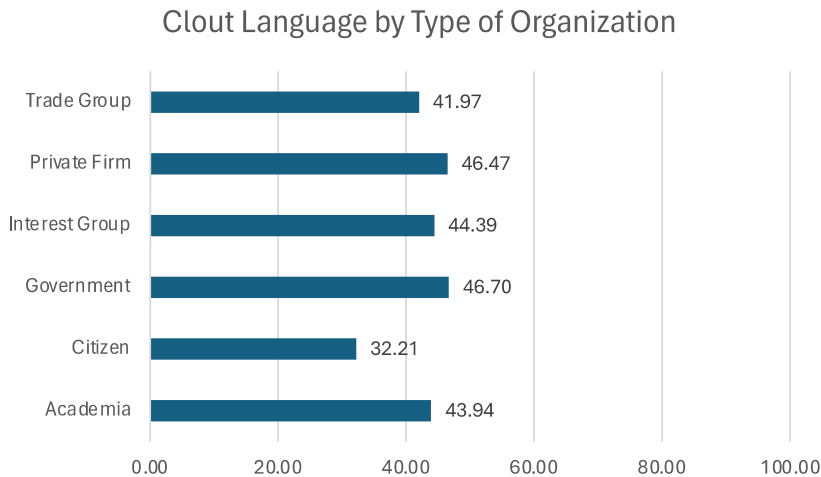


Figure 3. LIWC cloud language by type of organization.

Emotional tone, while not playing as large a role as the other factors considered, can be seen as showing differences in rhetorical strategies—albeit slight. With a positive tone, the effect of commenter type is only marginally significant,  $F(5, 124) = 1.891, p = .101$ . Although the use of a positive language tone is muted overall, trade associations use more positive language than all other organizations (see Figure 4). When compared with baselines provided by the grand mean of LIWC scores (3.67) and the average of the *New York Times* (2.32), the trade associations’ positive emotional tone is put into greater perspective when compared with that of government, citizens, and academia.

On the other hand, there are highly significant differences in the negative tone of language used based upon the provenance of the commenter,  $F(5, 124) = 6.147, p < .001$ . Specifically, academics, interest groups/nonprofit organizations, and private citizens use much more negative language than do private business firms, trade associations, and even sub-governmental organizations (see Figure 5). However, when compared with the baselines provided by LIWC’s grand mean (1.84) and the average of the *New York Times* (1.45), the negative tone expressed in the comments is rather muted.

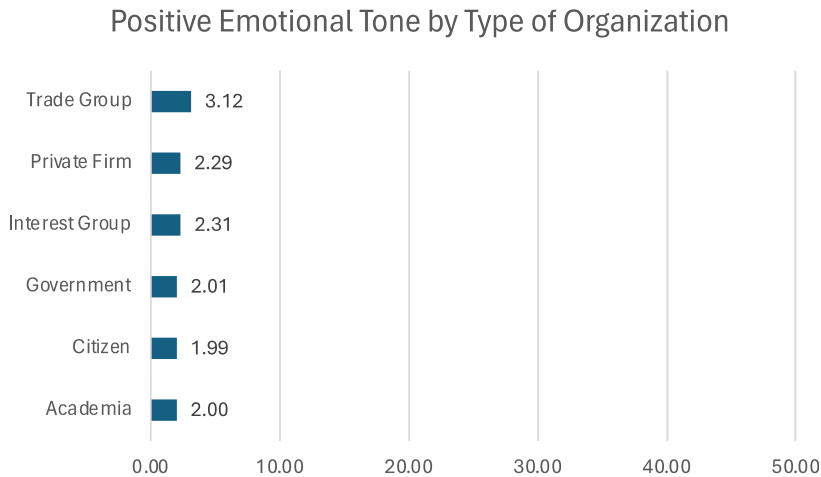
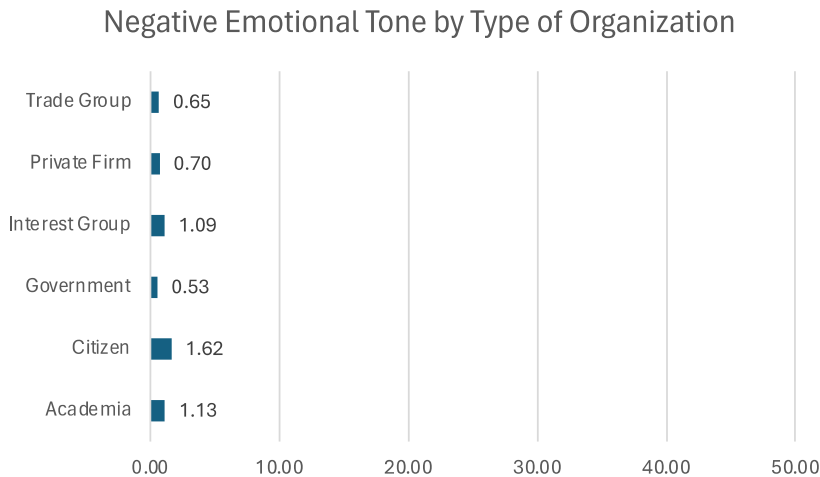


Figure 4. LIWC positive emotional tone words by type of organization.



**Figure 5.** LIWC negative emotional tone words by type of organization.

#### *Analysis of Federal Register comments regarding policy preferences*

A broad content analysis of all 130 public comments indicates that 69% of the comments (or 90 of the comments) stated policy beliefs favoring a more centralized regulatory role for government regarding the regulation of AI, biometrics, or AI biometrics. In contrast, 31% of the comments (or 40 of the comments) stated policy beliefs favoring no centralized regulatory role for government regarding the regulation of these AI-driven technologies. Policy beliefs supporting more centralized regulatory roles often focused on the risks associated with these technologies and took the form of either centralized policy frameworks where public deliberations and education could be used to implement more regulations surrounding their implementation; or specific calls for government to ban applications. Policy beliefs supporting no centralized regulatory roles typically focused more on the benefits associated with these technologies and took the form of industry self-regulation or the power of markets to correct any perceived risk associated with AI, biometrics, and AI biometrics.

Specific policy narratives also were stated in the expression of these policy beliefs. For instance, the more centralized policy framework beliefs used narratives that included themes on regulatory sandboxes, public outreach, public education, and a variety of governmental bans to stop organizations and governments from using biometric-based data in unethical or even illegal ways. For those policy beliefs supporting no centralized regulatory roles, policy narratives included themes on the role of industry expertise and industry-wide codes, the power of markets, and the need to consider the benefits of AI, biometrics, and AI biometrics more than the risks associated with those technologies.

Both sets of policy beliefs had a subset of comments where policy beliefs could be subsumed or changed that showcased the potential for policy learning. Specifically, some comments supporting a more centralized regulatory role sometimes suggested the implementation of regulatory sandboxes where regulatory experiments could be conducted working in close proximity with industry. Similarly, some comments supporting no centralized regulatory role also stated beliefs supporting the widespread adoption of rather stringent industry standards that some organizations had developed to protect privacy, prevent the misuse of data, and ensure that no biased or discriminatory impact would occur from data used by AI, biometrics, and AI biometrics.

For example, while regulatory sandboxes were only mentioned in three of the comments, the narratives explaining the purpose and previous experiences of organizations using regulatory sandboxes provided a direct linkage back to groups stating policy beliefs favoring no centralized regulation. As stated by TechNet, a network of technology leaders and senior executives:

*TechNet strongly supports the government's efforts to better understand and utilize this technology. TechNet supports regulatory sandboxes as a means to explore feasibility in a safe and collaborative framework, which have proven very successful with prior emergence of developing technologies. The potential for regulatory sandboxes, if established in a transparent and good-faith manner, is revolutionary. For example, the Consumer Financial Protection Bureau created a regulatory sandbox for businesses operating in the financial technology space. This sandbox was instrumental for both government and private sector to better understand risks, provide consumers with safe services, and predict what type of regulation would best serve this unique market without hindering innovation. This intersection of government regulation and private sector innovation should be championed as a way to meet consumer demand while ensuring a process is in place to identify and address potential risks. (p. 998).*

For comments expressing support for no centralized role, a theme of applying specific standards and codes used in some organizations to the entire industry was stated in 42 comments. As stated by the Consumer Technology Association, an advocacy group of technology companies:

*The dual goals of developing responsible AI and enabling innovation are best served through an intentional commitment to develop and implement codes of conduct, voluntary standards, and best practices that complement developing or existing policy initiatives and encourage self regulation. (p.326).*

Or, as stated by Uber as they promoted the benefits of using their processes surrounding the use of facial recognition technology and data:

*The use of facial verification technology is not a step we take lightly, so we have put in place a number of safeguards for responsible use... First, every case in which a variance is initially detected is ultimately decided by human review... Second, users are able to appeal when they feel that something has gone wrong. We have also conducted internal fairness assessments to evaluate how the technology works for people with different skin complexions... (p. 1038).*

Of particular importance for the role of policy narratives, specific characters, plots, and morals could be identified within the overarching setting of AI policy. For instance, government, the public, and AI biometric companies were the dominant characters in these policy narratives, often as villains; these characters often are presented in the comments as overreacting to their perceptions of the risks and benefits of AI biometrics in ways that generate harm (e.g., government overregulating AI in a way that hampers innovation and impairs competitive advantage, companies ignoring ethical concerns regarding the harm imposed by their technology, the public misreading AI research in ways that result in unnecessary regulations that harm businesses). Ultimately, there appears to be some consistency regarding the moral lesson that risks and benefits must be weighed appropriately for effective policy decisions to be made. Of course, what constitutes the appropriate weighting may change depending on the specific policy beliefs expressed.

## General discussion

This paper endeavors to consider the establishment of the U.S. policy subsystem concerning AI biometrics. Like AI policy generally, AI biometrics may be seen as a nascent policy subsystem, albeit one which successive Biden and Trump administrations have approached quite differently. While public policies and their outcomes will likely be slow to materialize at the federal level, our findings have implications for longer-term trends in AI biometrics as well as immediate actions occurring at the state level. It is there in the “laboratories of democracy” where change will likely occur, driven by public



perceptions of the AI biometric technologies identified in the Federal Register comments, analyzed and interpreted via many of the actors making the comments that led to the Biden Administration's EO 14110 on "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."

Although strong inferences may not necessarily be drawn from consideration of the commenter characteristics, exploration of the type of commenter—specifically private sector business organizations, nonprofit interest groups, and trade unions—suggests a substantial number of younger organizations as key stakeholders responding to the initial OSTP call for comments. This can be expected with AI biometrics due to both a burgeoning market rewarding innovation and concerns raised about the uncertain nature of how this technology will be used. Likewise, the presence of powerful and politically influential publicly traded firms such as Microsoft, Google, Cisco, and IBM (among others) suggests AI biometrics are seen as a policy subsystem of great interest to a vitally important economic sector. In short, when considering our first research question (RQ1), the background characteristics of commenters suggest a relatively substantial number of nonprofit interest groups and academics counterbalanced by trade associations and private firms, with relatively sparse numbers of comments from the general public. State and city government entities, while responding—with the former represented by attorneys general from multiple states—were not substantially involved at this juncture.

When the amount and type of language used by the commenters were considered to infer narrative strategies, what was most apparent was that commenter type—broadly defined—mattered more (RQ2-a) than generation of biometrics mentioned (RQ2-b). As expected, given the resources available to them, members of the general public used fewer words, used less analytic- and clout-based language, and had greater negativity in the tone of the language used. While subnational government units used substantially fewer words, this may be attributed to the need to be seen as interested, yet not establishing policy preferences. Overall, the relatively high level of analytic language and moderate levels of clout-based language suggests a strategy focusing on establishing expertise, yet not exerting status. Finally, while differences in positive emotional tone were slight, results suggest greater positivity from trade organizations and private firms, as well as nonprofit interest groups, when compared with subnational government organizations, individual citizens, and academics. Trade organizations and private firms, as well as subnational government organizations, were least negative with their emotional tone—which can be expected given the potential benefits offered for the trade groups and private firms, and the need for government organizations to appear as unbiased as possible.

Finally, the qualitative analysis of comments based on policy preferences suggests venue shopping for political arenas most amenable to commenter goals was a dominant theme (Lemke et al., 2023) with a substantial portion of commenters preferring centralized regulation over the current patchwork of state and urban regulations. Many of those opposed to centralized regulation suggested industry standards to self-regulate.

### *Implications for practice and policy*

With AI biometrics increasingly influencing everyday life in largely unseen ways—and as a result, underappreciated by the general public—bringing this technology to light may soon increase the likelihood of political conflict. Nationally representative surveys of citizens (Katsanis et al., 2021a, 2021b; Kostka et al., 2023; O'Shaughnessy et al., 2023) and experts (O'Shaughnessy et al., 2023) provide a snapshot of perspectives regarding the acceptable use of AI biometrics more generally, albeit in the abstract. For their part, online experiments regarding specific AI biometrics as FRT used in policing (Bromberg et al., 2020; Li, 2024; Schiff et al., 2023) and by public and private sector institutions (Doberstein et al., 2022; Lai & Rau, 2021; Zhang et al., 2021) provide insights regarding the theorized effect of different mechanisms and contexts on the support for and trust in this technology. However important these survey tools are for understanding perceptions regarding AI biometrics, comments published in the Federal Register provide uniquely important information for multiple reasons.

First, comments published in the Federal Register provide insights regarding who is interested. While the 130 comments received over three months in response to OSTP's call regarding "Public and Private Sector Uses of Biometric Technologies" for the Biden Administration are not directly comparable to the NSF's call in the Federal Register "Request for Information On The Development of an Artificial Intelligence (AI) Action Plan" for the Trump Administration, in which 10,068 comments were registered over two months in early 2025, the amount and patterns of response are revealing. Comments by institutions such as academia (29 | 82) and non-federal government (4 | 10) doubled across the two calls, whereas those institutions involved in the marketplace of products (private firms 27 | 292) and ideas (trade groups 13 | 178 and nonprofits 44 | 193) saw increases from four to 14 times, likely reflecting the scope of the call to include all AI. However, most revealing is the increased public involvement, with only 13 private citizen comments regarding AI biometrics in the call that lasted around three months during 2021–2022 whereas 9,313 individual citizens commented during just over a month (February 6–March 15) window in 2025. While these commenters are likely not representative of the U.S. general population (Sahn, 2025), the increase points to heightened awareness and concern about AI and suggests that concerned citizens are willing to put forth the effort to make their opinions known. Future research can more deeply examine these comments in light of our initial findings on public concerns around AI biometrics.

Second, text analysis tools, such as used here (i.e., LIWC), in conjunction with qualitative approaches, can provide insights regarding how the extent and type of concern is reflected in the comments. By comparison, surveys and experiments tend to reflect researcher expectations through limited and close-ended responses to discrete questions in which definitions of key concepts are often included to allow for direct statistical comparison. Importantly, text analysis and qualitative methods allow participants to share their perspectives in their own words, with both dictionaries (Boyd et al., 2022; Pennebaker et al., 2015) and expert insights used to interpret policy perspectives (Hemmerich et al., 2017; Stewart & McLean, 2004). Future research can continue to examine naturalistic responses to policy concerns and combine insights from these efforts with experimental and survey-based approaches to better inform future policy.

Finally, paying close attention to how regulations are written and implemented in light of the comments made in the Federal Register has the potential to provide insight into the enduring questions political scientists ask: who has power, and how is it exercised? This can be seen as especially important for policy issues that emerge from highly insulated issue networks (Ingold et al., 2023; Nohrstedt et al., 2023) and erupt onto the nation's policy agenda (Baumgartner & Jones, 2010; Zahariadis, 2019). AI has erupted onto the policy stage, and the Biden and Trump Administrations illustrate a clear rift in policy approaches. The potential for economic growth and displacement of entire job sectors has become a part of everyday conversation, and the threats posed through AI biometric-driven surveillance—whether interacting with government entities, in the workplace, or even in the assumed privacy of one's own home—are now in focus.

Ultimately, change can be expected in this policy arena—both as it matures and as the threats posed by various AI biometrics to values held by the U.S. public come to light. Specifically, while level of physical invasiveness of distinct AI biometrics does influence public perceptions, the threat of covert collection of biometrics and its use in a manner that is considered unfair and/or dangerous to privacy—and the liberty it provides—is what ultimately might lead to legislative action at the Federal level.

## References

- Bailenson, J. N. (2021). Nonverbal overload: A theoretical argument for the causes of zoom fatigue. *Technology, Mind, and Behavior*, 2(1), 1–6.
- Baumgartner, F. R., & Jones, B. D. (2010). *Agendas and instability in American politics*. University of Chicago Press.
- Biden, J. R. (2023). *JR. Executive Order (EO) 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*: Federal Register. <https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf>
- Bonnicksen, A. L. (1992). Human embryos and genetic testing: A private policy model. *Politics and the Life Sciences*, 11(1), 53–62.

- Boyd, R. L., Ashokkumar, A., Seraj, S., & Pennebaker, J. W. (2022). *The development and psychometric properties of LIWC-22* (pp. 1–47). University of Texas at Austin.
- Brader, T. (2006). *Campaigning for hearts and minds: How emotional appeals in political ads work*. University of Chicago Press.
- Bromberg, D. E., 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), 101415.
- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on fairness, accountability and transparency* (pp. 77–91). PMLR.
- Carey, M. P. (2013). *Counting regulations: An overview of rulemaking, types of federal regulations, and pages in the Federal register*. (R43056). Washington, D.C.: U.S. Congress. <https://ecommons.cornell.edu/server/api/core/bitstreams/bfc59f14-7d27-42d0-bf4c-b7ff152f48cd/content>
- Chuan, C.-H., Tsai, W.-H. S., & Cho, S. Y. (2019). Framing artificial intelligence in American newspapers. In *Proceedings of the 2019 AAAI/ACM conference on AI, ethics, and society* (pp. 339–344).
- Delmas, H., Denault, V., Burgoon, J. K., & Dunbar, N. E. (2024). A review of automatic lie detection from facial features. *Journal of Nonverbal Behavior*, 48(1), 93–136.
- Doberstein, C., Charbonneau, É., Morin, G., & Despatie, S. (2022). Measuring the acceptability of facial recognition-enabled work surveillance cameras in the public and private sector. *Public Performance & Management Review*, 45(1), 198–227.
- Farahany, N. A. (2023). *The battle for your brain: Defending the right to think freely in the age of neurotechnology*. St. Martin's Press.
- Franco, A., Orestes, S. G. F., de Fátima Coimbra, E., Thevissen, P., & Fernandes, Â. (2019). Comparing dental identifier charting in cone beam computed tomography scans and panoramic radiographs using INTERPOL coding for human identification. *Forensic Science International*, 302, 109860.
- Galanos, V. (2019). Exploring expanding expertise: Artificial intelligence as an existential threat and the role of prestigious commentators, 2014–2018. *Technology Analysis & Strategic Management*, 31(4), 421–432.
- Harris, L. A. (2021). *Artificial intelligence: Background, selected issues, and policy considerations*. Congressional Research Service Report, 46795.
- Harris, L. A., & Jaikaran, C. (2023). Highlights of the 2023 Executive Order on Artificial Intelligence for Congress. *Congressional Research Service (CRS) Reports and Issue Briefs*, NA-NA.
- Hemmerich, N., Klein, E. G., & Berman, M. (2017). Evidentiary support in public comments to the FDA's Center for Tobacco Products. *Journal of Health Politics, Policy and Law*, 42(4), 645–666.
- Henry, A. D., Ingold, K., Nohrstedt, D., & Weible, C. M. (2022). Advocacy coalition framework: Advice on applications and methods. In *Methods of the policy process*, 105–136. Routledge.
- Hibbeln, M., Jenkins, J. L., Schneider, C., Valacich, J. S., & Weinmann, M. (2017). How is your user feeling? Inferring emotion through human–computer interaction devices. *MIS Quarterly*, 41(1), 1–22.
- Hill, K. (2023). *Your face belongs to us: The secretive Startup dismantling your privacy*. Simon and Schuster.
- Hine, E., & Floridi, L. (2023). The blueprint for an AI bill of rights: In search of enactment, at risk of inaction. *Minds and Machines*, 33(2), 285–292.
- Hwang, T. J., Avorn, J., & Kesselheim, A. S. (2014). Life cycle of medical product rules issued by the US Food and Drug Administration. *Journal of Health Politics, Policy and Law*, 39(4), 751–780.
- Ingold, K., Fischer, M., & Cairney, P. (2017). Drivers for policy agreement in nascent subsystems: An application of the advocacy coalition framework to fracking policy in Switzerland and the UK. *Policy Studies Journal*, 45(3), 442–463.
- Ingold, K., Wiget, M., Wiedemann, R., Fischer, M., & Varone, F. (2023). *New issues on the agenda: How different are dynamics between nascent and mature subsystems?* Toronto, ON: ICPP.
- Jain, A. K., & Kumar, A. (2012). Biometric recognition: An overview. In *Second generation biometrics: The ethical, legal and social context* (pp. 49–79). Springer Science+Business Media.
- Jones, M. D., & McBeth, M. K. (2010). A narrative policy framework: Clear enough to be wrong? *Policy Studies Journal*, 38(2), 329–353.
- Katsanis, S. H., Claes, P., Doerr, M., Cook-Deegan, R., Tenenbaum, J. D., Evans, B. J., & Wagner, J. K. (2021a). A survey of US public perspectives on facial recognition technology and facial imaging data practices in health and research contexts. *PLoS One*, 16(10), e0257923.
- Katsanis, S. H., Claes, P., Doerr, M., Cook-Deegan, R., Tenenbaum, J. D., Evans, B. J., & Wagner, J. K. (2021b). US adult perspectives on facial images, DNA, and other biometrics. *IEEE Transactions on Technology and Society*, 3(1), 9–15.
- Kostka, G., Steinacker, L., & Meckel, M. (2023). Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly*, 40(1), 101761.
- Lablih, M., Bundi, P., & Portmann, L. (2024). Does anxiety increase policy learning? *Policy Studies Journal*, 52(3), 603–622.
- Lai, X., & Rau, P.-L. P. (2021). Has facial recognition technology been misused? A public perception model of facial recognition scenarios. *Computers in Human Behavior*, 124, 106894.
- Lemke, N., Trein, P., & Varone, F. (2023). Agenda-setting in nascent policy subsystems: Issue and instrument priorities across venues. *Policy Sciences*, 56(4), 633–655.

- Li, R. G. (2024). Institutional trustworthiness on public attitudes toward facial recognition technology: Evidence from US policing. *Government Information Quarterly*, **41**(3), 101941.
- Marcus, G. E., Neuman, W. R., & MacKuen, M. (2000). *Affective intelligence and political judgment*. University of Chicago Press.
- McStay, A. (2018). *Emotional AI: The rise of empathic media*. SAGE Publications.
- Mullins, J. K., Stewart, P. A., & Greitens, T. J. (2022). Facing forward: Policy for automated facial expression analysis. *Journal of the Association for Information Systems*, **23**(6), 1347–1353.
- National Science Foundation [NSF] (2025). *Request for Information On The Development of an Artificial Intelligence (AI) Action Plan*. Federal Register [https://www.nitrd.gov/coordination-areas/ai/90-fr-9088-responses/?et\\_rid=797826562&et\\_cid=5602100](https://www.nitrd.gov/coordination-areas/ai/90-fr-9088-responses/?et_rid=797826562&et_cid=5602100)
- Neri, H., & Cozman, F. (2020). The role of experts in the public perception of risk of artificial intelligence. *AI & Society*, **35**, 663–673.
- Nohrstedt, D., Ingold, K., Weible, C. M., Koebele, E. A., Olofsson, K. L., Satoh, K., & Jenkins-Smith, H. C. (2023). The advocacy coalition framework: Progress and emerging areas. In *Theories of the policy process* (pp. 130–160). Routledge.
- O'Shaughnessy, M. R., Schiff, D. S., Varshney, L. R., Rozell, C. J., & Davenport, M. A. (2023). What governs attitudes toward artificial intelligence adoption and governance? *Science and Public Policy*, **50**(2), 161–176.
- Pennebaker, J. W., Boyd, R. L., Jordan, K., & Blackburn, K. (2015). *The development and psychometric properties of LIWC2015*. <http://hdl.handle.net/2152/31333>
- Perry, B., & Uuk, R. (2019). AI governance and the policymaking process: Key considerations for reducing AI risk. *Big Data and Cognitive Computing*, **3**(2), 26.
- Potter, R. F., & Bolls, P. (2012). *Psychophysiological measurement and meaning: Cognitive and emotional processing of media*. Routledge.
- Robles, P., & Mallinson, D. J. (2023). Catching up with AI: Pushing toward a cohesive governance framework. *Politics & Policy*, **51**(3), 355–372.
- Sabatier, P. A. (1991). Toward better theories of the policy process. *PS: Political Science & Politics*, **24**(2), 147–156.
- Sahn, A. (2025). Public comment and public policy. *American Journal of Political Science*, **69**(2), 685–700.
- Scherer, K. R., & Meuleman, B. (2013). Human emotion experiences can be predicted on theoretical grounds: Evidence from verbal Labeling. *PLoS One*, **8**(3), e58166.
- Schiff, D. S. (2023). Looking through a policy window with tinted glasses: Setting the agenda for US AI policy. *Review of Policy Research*, **40**(5), 729–756.
- Schiff, D. S. (2024). Framing contestation and public influence on policymakers: Evidence from US artificial intelligence policy discourse. *Policy and Society*, **43**(3), 255–288.
- Schiff, D. S., & Schiff, K. J. (2023). Narratives and expert information in agenda-setting: Experimental evidence on state legislator engagement with artificial intelligence policy. *Policy Studies Journal*, **51**(4), 817–842.
- Schiff, K. J., Schiff, D. S., Adams, I. T., McCrain, J., & Mourtgos, S. M. (2023). Institutional factors driving citizen perceptions of AI in government: Evidence from a survey experiment on policing. *Public Administration Review*.
- Settle, J. E., Hibbing, M. V., Anspach, N. M., Carlson, T. N., Coe, C. M., Hernandez, E., & Arceneaux, K. (2020). Political psychophysiology: A primer for interested researchers and consumers. *Politics and the Life Sciences*, **39**(1), 101–117.
- Shanahan, E., Jones, M. D., McBeth, M. K., & Radaelli, C. M. (2018). The narrative policy framework. In *Theories of the Policy Process* (pp. 173–213). Routledge.
- Shanahan, E. A., Jones, M. D., & McBeth, M. K. (2011). Policy narratives and policy processes. *Policy Studies Journal*, **39**(3), 535–561.
- Shanahan, E. A., Jones, M. D., & McBeth, M. K. (2018). How to conduct a narrative policy framework study. *The Social Science Journal*, **55**(3), 332–345.
- Smalley, S. (2024October 17, 2024). Kroger's facial recognition plans draw increasing concern from lawmakers. The Record. Future Recorded News. <https://therecord.media/kroger-facial-recognition-lawmakers-concerns>
- Spisak, B. R. (2022). Complex faces and naïve machines: A commentary on facial perceptions of age, gender, and leader preferences in the age of AI. *Politics and the Life Sciences*, **41**(1), 147–149.
- Spisak, B. R. (2023). *Computational leadership: Connecting Behavioral science and technology to optimize decision-making and increase profits*. John Wiley & Sons, Inc.
- Spisak, B. R., Spisak, J., & Trask, A. (2021). *Four steps to preserving privacy and Debiasing data-informed policy*. California Management Review.
- Stewart, P. A., & Knight, A. J. (2005). Trends affecting the next generation of US agricultural biotechnology: Politics, policy, and plant-made pharmaceuticals. *Technological Forecasting and Social Change*, **72**(5), 521–534.
- Stewart, P. A., & McLean, W. (2004). Fear and hope over the third generation of agricultural biotechnology: Analysis of public response in the Federal Register. *AgBioForum*, **7**(3), 133–141.
- Stone, D. A. (1997). *Policy paradox: The art of political decision making*. WW Norton New York.
- Stritch, A. (2015). The advocacy coalition framework and nascent subsystems: Trade union disclosure policy in Canada. *Policy Studies Journal*, **43**(4), 437–455.

- Sutrop, M., & Laas-Mikko, K.** (2012). From identity verification to behavior prediction: Ethical implications of second generation biometrics. *Review of Policy Research*, **29**(1), 21–36.
- Taeihagh, A.** (2021). Governance of artificial intelligence. *Policy and Society*, **40**(2), 137–157.
- Trump, D. J.** (2025). *Removing Barriers to American Leadership in Artificial Intelligence*. Federal Register. <https://www.govinfo.gov/content/pkg/FR-2025-01-31/pdf/2025-02172.pdf>
- Turow, J.** (2021). *The voice catchers: How marketers listen in to exploit your feelings, your privacy, and your wallet*. Yale University Press.
- Weible, C. M., & Sabatier, P. A.** (2018). *Theories of the policy process*. Routledge.
- West, W. F., & Raso, C.** (2013). Who shapes the rulemaking agenda? Implications for bureaucratic responsiveness and bureaucratic control. *Journal of Public Administration Research and Theory*, **23**(3), 495–519.
- Woodward, J. D.** (1997). Biometric scanning, law & policy: Identifying the concerns-drafting the biometric blueprint. *University of Pittsburgh School of Law, Law review*, **59**, 97.
- Yackee, J. W., & Yackee, S. W.** (2006). A bias towards business? Assessing interest group influence on the US bureaucracy. *The Journal of Politics*, **68**(1), 128–139.
- Zahariadis, N.** (1995). Policy change and learning: An advocacy coalition approach. *Policy Studies Journal*, **23**(2), 378–383.
- Zahariadis, N.** (2019). The multiple streams framework: Structure, limitations, prospects. In *Theories of the policy process* (pp. 65–92). Routledge.
- Zhang, S., Feng, Y., Bauer, L., Cranor, L. F., Das, A., & Sadeh, N.** (2021). “Did you know this camera tracks your mood?": Understanding privacy expectations and preferences in the age of video analytics. In *Proceedings on privacy enhancing technologies* (2), 282–304.