Depictions of Privacy Invasion and Surveillance in Artworks and Potential Lessons For Privacy Communication

Tess Eschebach
University of Chicago
Chicago, Illinois, USA
eschebach@uchicago.edu

Emma I. C. Peterson
University of Chicago
Chicago, Illinois, USA
eicp@uchicago.edu

Nathaniel Kim
University of Chicago
Chicago, Illinois, USA
ntckim@uchicago.edu

Bingning (Jolin) Liu
University of Chicago
Chicago, Illinois, USA
bingning680@uchicago.edu

Marc Downie
University of Chicago
Chicago, Illinois, USA
marcdownie@uchicago.edu

Douglas Pancoast
School of the Art Institute of Chicago
Chicago, Illinois, USA
dpanco@saic.edu

Blase Ur
University of Chicago
Chicago, Illinois, USA
blase@uchicago.edu

Abstract

User-facing communication about privacy (e.g., privacy policies, privacy tools' user interfaces) is frequently ignored and often ineffective. In contrast to these arguably staid interfaces, artworks often focus on provocation, engagement, and critical interpretation. For decades, artists have created *privacy art*—artistic media in galleries relating to the surveillance and privacy of individuals. What are artists saying about privacy, and how? Crucially, what lessons might they have for designing privacy-focused user interfaces? To this end, we compiled over 800 privacy artworks, qualitatively analyzing a sample. Common topics spanned artistic media (from paintings to immersive installations) and eras. Artworks built upon familiar concepts (e.g., cameras, homes) to speculate on society's future and present personal information (e.g., artist, viewer, public). We discuss lessons for making non-artistic privacy communication more engaging and powerful through directing attention (e.g., lighting, collage) and setting a tone (e.g., unsettling, fun, mundane).

CCS Concepts

• **Security and privacy → Human and societal aspects of security and privacy**; *Usability in security and privacy*; • **Applied computing** → *Fine arts*; *Media arts.*

Keywords

Usable Privacy, Art, Privacy Art, Artworks, Qualitative Analysis, Privacy Communication

ACM Reference Format:
Tess Eschebach, Emma I. C. Peterson, Nathaniel Kim, Bingning (Jolin) Liu, Marc Downie, Douglas Pancoast, and Blase Ur. 2026. Depictions of Privacy Invasion and Surveillance in Artworks and Potential Lessons For Privacy Communication. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 26 pages. https://doi.org/10.1145/3772318.3791074

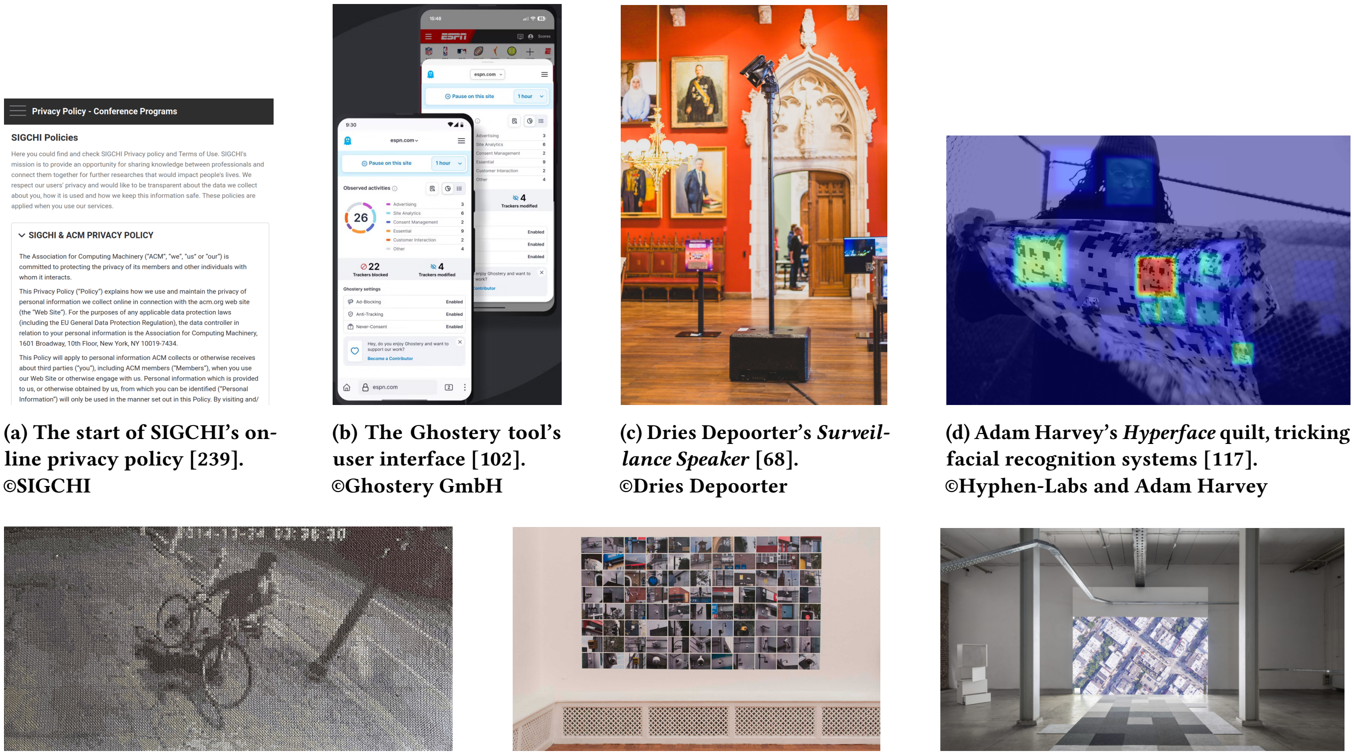
CHI '26, Barcelona, Spain

ACM ISBN 979-8-4007-2278-3/26/04
https://doi.org/10.1145/3772318.3791074

1 Introduction

Communicating with users about privacy decisions is a major focus of usable privacy research [86]. To date, however, privacy topics have typically been communicated to users through lengthy and abstract privacy policies [171, 172, 214, 228] or user interfaces that are similarly abstract and difficult for users to understand [53, 86, 200]. While researchers have proposed some alternative communication mechanisms [285] including icons [112, 122], "nutrition" labels [134, 215], and comics [255], for the most part, these methods have not been widely adopted. Notably, existing privacy user interfaces often fail to capture societal values or to "critique, speculate, [or] present critical alternatives" [276]. More generally, one might argue that privacy concepts are usually communicated to users in ways that are staid, boring, and corporate, which might help explain why users often ignore these communications [221]. Thus, some pro-privacy researchers have suggested the use of different design methods—including speculative [76], critical [14], and value-sensitive [90, 139, 236] design—to provoke reflection [276].

Primarily separate from the community of usable privacy researchers and practitioners, artists have been creating artworks about privacy for decades. Rather than needing to conform to typical corporate and academic communication constraints, artists have a far wider mandate to comment on the political and personal. Broadly, art can "mobilize the masses" and "tackle the most difficult and most important [tasks]" [23]. In computing, art can be a "distinctive way to illuminate key technical and social issues" [118]. Privacy-focused art has become an increasingly clear part of the artistic canon, with artists' statements explaining how they seek both to expose and to resist privacy invasions [40, 54, 181, 182, 271]. Even outside of the privacy realm, artists use diverse media and techniques to explore complex topics in computing [246]. Ongoing discussions in HCI have advocated for the further integration of arts-based methods in computing to illuminate new knowledge [74, 175, 229]



Privacy Policy - Conference Programs

SIGCHI Policies

Here you could find and check SIGCHI Privacy policy and Terms of Use. SIGCHI's mission is to provide an opportunity for sharing knowledge between professionals and connect them together for further researches that would impact people's lives. We respect our users' privacy and would like to be transparent about the data we collect about you, how it is used and how we keep this information safe. These policies are applied when you use our services.

SIGCHI & ACM PRIVACY POLICY

The Association for Computing Machinery (“ACM“, “we“, “us” or “our“) is committed to protecting the privacy of its members and other individuals with whom it interacts.

This Privacy Policy (“Policy“) explains how we use and maintain the privacy of personal information we collect online in connection with the acm.org web site (the “Web Site“). For the purposes of any applicable data protection laws (including the EU General Data Protection Regulation), the data controller in relation to your personal information is the Association for Computing Machinery, 1601 Broadway, 10th Floor, New York, NY 10019-7434.

This Policy will apply to personal information ACM collects or otherwise receives about third parties (“you“), including ACM members (“Members“), when you use our Web Site or otherwise engage with us. Personal information which is provided to us, or otherwise obtained by us, from which you can be identified (“Personal Information“) will only be used in the manner set out in this Policy. By visiting and/

(a) The start of SIGCHI's online privacy policy [239]. ©SIGCHI

9:30

espn.com

Pause on this site 1 hour

Observed activities

Advertising	3
Site Analytics	6
Consent Management	2
Essential	9
Customer Interaction	2
Other	4

26

22 Trackers blocked

4 Trackers modified

Ghostery settings

Ad-Blocking	Enabled
Anti-Tracking	Enabled
Never-Consent	Enabled

Hey, do you enjoy Ghostery and want to support our work?

Become a Contributor

espn.com

(b) The Ghostery tool's user interface [102]. ©Ghostery GmbH

(c) Dries Depoorter's *Surveillance Speaker* [68]. ©Dries Depoorter

(d) Adam Harvey's *Hyperface* quilt, tricking facial recognition systems [117]. ©Hyphen-Labs and Adam Harvey

(e) Francine Leclercq's tapestry *Embroidered Surveillance* [146]. ©Francine LeClercq

(f) James Bridle's collage *Every CCTV Camera* [38]. ©James Bridle

(g) Eva and Franco Mattes's *My Little Big Data* [168]. ©Eva and Franco Mattes

Figure 1: An informal comparison of standard privacy communications (Figures 1a–1b) and privacy art (Figures 1c–1g).

and inform user interface design [4]. As Bardzell and Bardzell articulate, “We can improve knowledge not just by developing better formal methods of data collection and analysis (i.e., a strategy embraced by traditional science); we can also improve it by being more experienced and sensitive embodied thinkers in the first place (i.e., a strategy embraced in the arts and humanities)” [14].

To date, the handful of efforts to catalog privacy and surveillance art have had a very limited scale. For instance, the International Association of Privacy Professionals has a webpage collecting 35 artworks about privacy [126]. Others have made small (e.g., top 10) lists of surveillance artworks [77]. Cahill et al. assembled an online database of 31 artworks discussing surveillance in Canada post-9/11 [48]. Similarly, various art galleries have held small exhibitions focused on privacy or surveillance [48, 58]. To our knowledge, no existing collection includes more than a few dozen pieces.

This flurry of artistic activity in communicating privacy topics to humans raises a number of questions. At a high level, what are these artworks saying about privacy, and how are they doing so? Furthermore, what lessons might these artworks' techniques have for interaction designers, who are also tasked to communicate privacy topics to humans, albeit frequently under different constraints? To this end, we brought together an interdisciplinary team of researchers with backgrounds in usable privacy, media studies, and fine art. We explore provocative and novel approaches to privacy communication for end users. Specifically, we answer the following research questions:

RQ1: What is the shape and scope of practice in privacy art? What works are being created to highlight the surveillance and privacy of individuals, in what media, and by whom?

We assembled a database of 859 artworks we characterize as *privacy art*, or artworks that relate to the privacy or surveillance of individuals and that have been exhibited in art venues (e.g., galleries, museums). In total, 332 different *privacy artists* created these works. Creating this largest-of-its-kind database required a structured discovery process combining keyword searches, snowball sampling, and feedback and suggestions from practicing privacy artists. While we used this database to answer our research questions, we also contribute to the community an interactive website[1] of our database as an artifact intended to facilitate future research on privacy art.

We first wondered what aspects of privacy these artworks covered. To that end, we qualitatively coded digitally archived descriptions (e.g., images, videos, artist statements, media coverage) on a sample of 73 artworks. We primarily used weighted random sampling to select artworks from our large database, giving us a broad set of artworks to answer our next two research questions:

RQ2: What components and subjects are artists highlighting in their privacy and surveillance artworks?

First, we observed a visual language that featured familiar forms like surveillance devices (e.g., cameras, microphones) and homes,

[1] Our full database can be found at our website: **https://privacyart.net**

closely mapping to imagery and metaphors in end-user privacy communication [183, 190, 289]. Privacy art in our database commonly highlighted the existence and impact of the surveillance of individuals by governments and/or corporations. Some works focused on the bi-directional relationship between surveillance and identity, as well as privacy risks heightened by artificial intelligence (AI). The artworks additionally presented means of resisting surveillance, encompassing specific real and speculative approaches, as well as general techniques (e.g., camouflage). Some privacy art commented on, and provocatively collapsed, distinctions between public and private. Finally, some built upon an artist's personal experiences and data. Broadly, subjects observed in privacy art included the artist, the viewer, specific individuals, groups in aggregate, and even surveillance devices themselves.

To inform the design of privacy communication *outside* artistic contexts, we focused on the following question:

RQ3: What mechanisms do privacy artworks employ to communicate about privacy and surveillance?

We observed a number of mechanisms that conveyed artworks' key messages about privacy. Privacy artworks in our sample uniquely directed attention primarily through visual methods (e.g., spotlighting with actual light). In contrast, other artworks employed collage and aggregation techniques to overwhelm viewers. Some artworks are presented through the "eyes" of a surveillance system, displaying the viewpoints of CCTV cameras and computer vision bounding boxes over images. Similarly, some works allow the viewer to interactively explore a piece. However, this interaction may be compulsory to experience a piece, and information may be withheld, violating a viewer's control. Surprisingly, artworks differed widely in tone, ranging from unsettling to fun, from formal to familiar (e.g., a childhood bedroom), stirring negative emotions through either direct communication or selective juxtaposition.

We conclude by exploring how components and mechanisms in privacy art can inform provocative privacy communication approaches (Section 6). Our insights suggest early-stage design opportunities for interaction designers and human-centered privacy researchers. We also offer strategies for pro-privacy companies and organizations, such as Mozilla, Brave, and DuckDuckGo.

2 Background and Related Work

In the digital age, surveillance has seeped into many aspects of life. Scholars have suggested that the world is under an ever-watching panoptic gaze of public and private entities [13, 167, 290]. Furthermore, constant data collection driving surveillance may lead to self-censorship [167]. As a result, communicating with end users about privacy topics is critical [1, 20]. Unsurprisingly, then, privacy communication and interface design are key areas of research [86, 153].

2.1 Usable Privacy Communication

Privacy communications span many formats, including educational materials, research tools, and interfaces for privacy settings. We focus on communications by usable privacy researchers and pro-privacy companies to provoke privacy reflection. Common methods of communicating about privacy—like text privacy policies, cookie banners, and LEDs on physical devices [226]—can be opaque and dull, offering little to engage users [112, 134, 138, 178, 228]. Prior work has explored alternative communication approaches, such as icons [20, 67, 122, 226] or privacy "nutrition labels" [134, 215]. Unfortunately, even icons communicating "simple and familiar concepts" often require clarification text [112], and icons may be interpreted differently across cultures [122]. Furthermore, these works primarily focus on updating existing privacy communications, like privacy policies or data-use notifications [112, 122, 134, 215].

Usable privacy research has detailed overarching themes in privacy imagery [183, 190] and communication design [112, 226], which we revisit in Section 6. Oates et al. categorize privacy as illustrated by everyday individuals [190]. Motti et al. take a broader approach, compiling digital images from end users, web designers, and professionals—specifically, "journalists and content-creators" [183]. We expand this research by analyzing works from professional *artists*. Differently, Habib et al. explore privacy icon design [112], and Schaub et al. detail how effective privacy notices are displayed to users through timing, channel, modality, and control [226].

Some researchers have suggested creating more engaging or "entertaining" [255] privacy communications. For example, Schlegel et al. suggest animated eye imagery to show how much user data is accessed [228]. Additional strategies proposed include video games, table-top games [26], comics [150, 255], and videos [243] seeking to change user behavior [285]. Researchers have found that interactivity increases system transparency [215] and that user curiosity [138] promotes engagement with privacy policies. For example, privacy policies formatted as comics hold user attention better than text-based policies [255]. Researchers have tested novel mediums such as virtual reality [131, 153], theater [131, 195, 241, 242], electrical muscle stimulation [70], and dance [56] to highlight data collection.

2.2 Prior Characterizations of Privacy Art

In recent years, there has been a "proliferation of critical surveillance artworks" [182]. The work of artists like Dries Depoorter [121], Kyle McDonald [164], and Trevor Paglen [41] has received coverage from major news publications, though surveillance art has largely been ignored by usable privacy and design research. Brighenti defines "surveillance art" as "contemporary artwork that in some way hints to or deals with topics, concerns and procedures that fall within the interest of surveillance studies" [40]. Because we are interested in communication to end users, we focus on artworks related to the surveillance or privacy of an *individual*. Our definition both excludes works that would fall under Brighenti's definition (e.g., surveillance of an organization) and includes works that Brighenti's would not (e.g., about privacy policies or practices).

Surveillance art may highlight specific surveillance technologies [18, 246]. For example, the use of cameras in the 1895 film *Workers Leaving the Lumière Factory* [159] invoked what was soon considered a form of workplace surveillance [287]. Artists similarly highlighted the impacts of introducing CCTV and personal video cameras by inviting viewers to surveil themselves [246, 271, 287]. While we focus on artworks that employ surveillance technologies to critique those technologies, some contemporary artists employ similar surveillance [11, 18, 246] or AI [246] technologies to enable interactivity, not comment on privacy. Thus, our work is distinct from Stark and Crawford's analysis of data ethics in art, despite overlapping artists. Stark and Crawford predominantly focus on *artist's personal beliefs* about the use of surveillance technologies and AI in art [246] with limited design recommendations (namely "defamiliarization"—presenting familiar concepts novelly). While we see some themes around AI and algorithms, our analysis centers on the *design mechanisms used in artworks* that focus on individual privacy (even if surveillance technologies are not used).

Prior scholarship outside of computer science (e.g., media arts, art history, architecture) explores themes that define the surveillance art space. This includes resistance to surveillance [132, 181], constructing public and private space [119, 128, 234], and importantly *gaze*: how the viewer observes and how they are observed [40, 182, 271]. In our analysis, we observe and expand upon these existing themes, and many more (e.g., speculating on the future, creating fun or unsettling tones), which we then discuss in relation to privacy communication outside artistic contexts (Section 6).

While surveillance art has been defined as a body of work, to our knowledge no one has created any large databases mapping surveillance art. Instead, artistic analyses of surveillance art have typically focused on a single artist or small set of works [132, 280]. Scholarly analysis of surveillance art generally explores fewer than a dozen artists at a time [40, 54, 181, 182, 271] and primarily discusses contemporary art [40]. Cahill et al. collected 31 artworks focused on surveillance in Canada [48], while popular media outlets have discussed similarly small sets [77, 116, 176]. To our knowledge, the largest collection was a book by Bertrand and Bridle [28] cataloging 43 artists, 26 of whom met our inclusion criteria (see Section 3.2). In contrast, we compile 859 artworks across 332 artists.

Data-Handling and Consent in Art Galleries. Within artistic spaces the line between ethical boundaries and censorship is murky and highly contested [10, 174]. There are limited guidelines for consent inside a venue—content warnings [10], notifications of being recorded [35, 188]—or being the subject of a piece. On the latter point, the ethics of photographing people from public vantage points has been widely debated [174, 179, 192, 210, 254]. Standardization is mainly relegated to a venue's website privacy policy [152]. Through artist interviews, Stark and Crawford find a debate playing out as some artists express concerns about invading the public's privacy, while others believe they have a "social and even legal exception" [246] to use personal data [246]. Though surveillance technologies are increasingly used in contemporary art, Stark and Crawford also argue that art critics may not understand the implications of data collection [246]. While scholars across disciplines have argued for increased considerations of privacy and data in art venues [152, 246], the debate continues over the "eternal and recurrent dualities of [. . .] ethics/artistic expression" [174].

2.3 Approaches to Design

The foundations of interaction design are situated within the humanities/artistic spaces [15, 98], science fiction media [34, 251, 279], critical theory [15], and applied arts [14]. However, artworks and the discourse around them are seldom cited in the HCI literature [205]. Even previous surveillance and privacy design research has not studied the richness of the established space of surveillance art existing in parallel [88, 259, 279]. Here, we outline design methodologies (e.g., value sensitive, emotional, persuasive, critical, speculative) employed to conceptualize privacy. We discuss these methodologies in the context of our own findings in Section 6.

Interaction design has a rich history in HCI with applications for the practice community and as mechanism for Research Through Design (RtD) [204, 288]. Design often focuses on consumer products in everyday contexts [82, 88, 98, 259, 279], allowing researchers to more directly engage with users [204] and grapple with wicked problems [288] like privacy. RtD takes many forms [204], including tangible prototypes [140], design workbooks [99, 228], fictional narratives, and participatory storytelling workshops [66, 104, 111, 148] to facilitate discussion for designers, researchers, and end users. Privacy by Design (PbD) focuses on embedding privacy choices into tools by default based on predefined concerns. Previous work has argued that design methods can inform more holistic viewpoints and considerations for the addressed privacy concerns [277]. Design methods often focus on provoking reflection, as we explore here.

Privacy is a key value that is often central to discourse about data-driven technologies [39, 57, 89–91, 139, 236, 277]. *Value sensitive design* (VSD) centers the values experienced uniquely by different people, cultures, and contexts [39, 90] throughout the design process to identify unintended consequences for stakeholders [90, 139, 236]. Workbooks can be used as "value levers" [236] to help developers *anticipate* privacy concerns early in design [277]. In our study, we explore how different topics and mechanisms in privacy art may prompt reflections on privacy.

Researchers and designers may also provoke reflection through *emotional design.* Positive emotions are often favored to promote connection to technologies [69, 96, 130, 189, 281]. Discomfort and creepiness may be favored for privacy provocation [22, 113, 147]. Researchers explore creepy violations of privacy by analyzing technologies [143, 258] and embedding creepiness into designs or stories to foster discussion [217, 219, 237] for researchers [213, 219, 248] and with users [177, 237, 248]. For example, privacy dashboards provide visualizations of users' data [84, 233], presenting overly specific personalization and data inferences [217]. Uniquely, *CreepyLeaks* uses electrodes to induce a mild electric stimulation when data is leaked to third parties [237]. We explore novel methods from privacy art for evoking creepiness in Section 6.3.1.

Persuasive technologies seek to change a user's behavior, such as via mobile games that show security scenarios to enhance smartphone users' security awareness [93–95]. However, persuasive designs promote a specific point of view and can obfuscate information to manipulate and deceive users through *dark patterns* that often encourage consumerism [24, 87, 108]. In our study, we seek to promote viewer/user reflection. While *critical designs* are created with a specific point of view [15, 17, 76], these designs *critique* everyday practices surrounding consumerist products [14, 76, 269]. For example, Teyssier et al. create *Eyecam*, a realistic anthropomorphic webcam of a human eye, which exaggerates the feeling of being watched to prompt reflection on the ubiquitous device [259]. Thus, similar to privacy art, critical designs prompt reflection on common practices. We elaborate on this point in Section 6.

Speculative design explores near-future technologies—often consumer products [82, 88, 98, 259, 279]—that are technologically plausible [98]. Researchers and viewers "think about the future [and. . .] critique current practice" [12, 76]. For example, Fox et al. create a catalog of near-future menstrual tracking tools informed by current applications' privacy policies to explore possible futures [88]. We expand upon speculative approaches in privacy art in Section 6.1.

Design fictions place speculative design artifacts within their broader societal contexts and narratives [32, 137, 249]. Derived from film theory [137], design fictions are used to analyze filmic media [154, 256, 275], but may also be a tool to investigate the context of future technologies [32, 34, 155, 244, 251, 259, 278, 279]. For example, Wong et al. employ a workbook of near-future scenarios inspired by a science fiction novel to explore "how researchers can understand and make use of cultural representations of new and emerging technologies to interrogate their privacy implications" [279]. Differently, Blythe et al. conduct workshops with participants to create their own design fictions about privacy in alternative historical contexts [34], arguing for the importance of critique in a world with more limited privacy [34]. In this study we look towards art as inspiration for speculative designs (Section 6.1).

2.4 Communicating Computer Science with Art

The importance of design is understood to be the "ease" [15] in which it can be integrated into everyday life [15, 76], leading to debates in HCI if design is never or sometimes art [76]. However, opportunities for interaction design exist outside the confines of the *everyday* and within the arts. For example, Blythe et al. argue for the importance of "magic machines" (rather than those governed by plausibility) to broadly explore and critique technologies [33]. Ongoing discussion in HCI have explored a greater integration and appreciation of the humanities [16] and arts-based methods [175] in computing research [51, 75, 149, 185, 229, 252]. For two years, CHI hosted an art gallery, Art.CHI, to showcase the work of digital artists [83, 161]. HCI researchers may even identify as artists themselves [253]. Some research has looked at how artistic aesthetics may inform user interface design [4]. However, within HCI the broader fine arts community remains underexplored, with calls for interaction design to explore the methods of interactive art [74]. As an interdisciplinary team, we engage with a broad range of artworks across medias relating to surveillance and privacy. As Zimmerman argued for the "lost opportunity for the HCI research community to benefit from the added perspective of [interaction] design thinking in a collaborative research environment" [288], we argue for the importance of art as a perspective for the HCI community.

Both specific to privacy and broadly, some prior works used art to convey computer science topics [60]. For example, Hemment et al. worked with artists to explain AI's social issues [118], while other computer scientists had artists help develop privacy tools [81, 208]. Plaut et al. suggested "using problematic technology to teach about problematic technology" [208]. Elsden et al. worked with artists to create interventions limiting personal information shared on Zoom [81]. Privacy artists have also engaged computer scientists to create artworks, such as Rubin and Hansen's *Listening Post* [60]. In contrast to previous studies, where artists [81, 208] were consulted to design specific pieces, our work synthesizes general tactics.

3 Methods

We began with a structured discovery process (Section 3.1 and Appendix A) to assemble a database of privacy art. We then qualitatively analyzed (Section 3.3) a sample of works from this database to characterize communication methods in privacy art using iterative open coding. This let us draw connections between different works and explore privacy artists' mechanisms, topics, and techniques.

3.1 Creating a Database of Privacy Art

Our discovery process began with creating a *Foundation Set* sourced from keyword searches, research team members' prior knowledge (see Section 3.4), suggestions from experts (e.g., practicing artists), and dozens of students in an interdisciplinary course on privacy art. We conducted initial keyword searches between Fall 2024 and Spring 2025 using search engines (primarily Google and DuckDuckGo) and arts databases including the MoMA Collections [191], Ars Electronica's Prix Archive [136], and Smithsonian Libraries Art and Artist Files [151]. Keywords included common surveillance and privacy terms from media, research, and literature. These ranged from simpler searches like "privacy art" to more specific searches like "facial recognition artworks." Specifically, our searches combined each of four art terms (*art, artwork(s)*, *artist(s)*, and *exhibition*) with one or more privacy or topic terms:

- *Privacy terms:* privacy, (mass-/counter-) surveillance
- *Topic terms:* (location) tracking, circumvention, phone, facial recognition, (personal) data, social media, camera

To augment keyword searches, we relied on expert knowledge to ensure our database included key instances of privacy art. For instance, we received input from three practicing artists with backgrounds in media, arts, and architecture, as well as library subject specialist in the arts. These experts particularly provided insight on historic artworks where organized digital documentation may be more limited. Additionally, we crowdsourced 61 submissions from 24 different students in an interdisciplinary course on privacy art taught by members of our study team. For each artwork, we applied the inclusion/exclusion criteria detailed in Section 3.2.

For all artworks, we learned about the piece by visiting the contributing artists' personal websites to review descriptions of the work. We investigated all other works by that artist, again applying our selection criteria. For artists without a personal website, we relied on exhibition pages, media coverage, or academic literature.

To expand our database, we further investigated contributing artists and exhibition venues from the Foundation Set in a process similar to snowball sampling. First, we collected the names of artists with artworks exhibited in shows alongside pieces in the Foundation Set. Works found through this broadened search were placed into *Set 2*. For *Set 3*, we repeated this process with venues and artists from Set 2.

Website. To share our database with the wider scientific and artistic communities, we created a website for searching our database: privacyart.net. The website, constructed using Astro/React and MySQL, has a grid view of all artworks in the database with an image of each. Clicking on an artwork gives the title, artist, year, and links to the artworks. Users can search by title or artist name.

3.2 Artwork Selection Criteria

Similar to how previous work has examined privacy representations in specific media, such as television [92] and (amateur) drawings [190], we focus on *publicly exhibited artworks in formal settings* like galleries, museums, and arts festivals. These have unique interaction techniques, constraints, and tropes, allowing for more specific and feasible mappings of the spaces. To most readily translate our findings to usable privacy research, we chose to focus on the privacy and surveillance of *individuals*, as opposed to larger groups or organizations. We focus predominantly on *visual* art for more direct applications to designing interfaces and notifications [20, 183, 220, 226]. We set formal inclusion and exclusion criteria via iterative team discussions while collecting initial artworks. Potential edge cases were flagged for discussion with our larger team and included or excluded based on team consensus. Our full selection criteria follow:

(1) We only include pieces that were at some point displayed in galleries, as public art (e.g., installations in public buildings/parks), or publicly accessible digitally in an art context.

(2) We only include works typically displayed as an "artwork." Works in literature, film, or long-form media format were excluded unless displayed or exhibited as an artwork in a more formal setting. The ephemeral experience of formal settings is more similar to privacy communications in the wild, providing immediate visual or short-form experiences. We similarly considered works exploring privacy in theater [131, 195, 241, 242] out of scope. Works in formal settings have consistent interaction modes, where viewers can enter and exit the space (e.g., gallery) at will, unlike singular, self-contained experiences of theater or film.
   - *Example:* Hito Steyerl's short film *How Not to Be Seen* [250] was exhibited in art galleries, so it is included.
   - *Edge case:* George Orwell's novel *1984* [196], though widely known for commentary on surveillance, is a book not primarily exhibited as an artwork, so it is excluded.

(3) Since we care about privacy communication with end users, not the inner workings of surveillance entities, we only include works that focus primarily on the privacy of an individual or the general public.
   - *Example:* Kyle McDonald's *ICESPY* [173], concerning citizen surveillance (i.e., identification) of ICE agents, is in scope since it involves privacy invasions of individuals (specific government workers).
   - *Edge case:* Trevor Paglen's *Black Sites* [197], centered on exposing CIA secret prisons, is not in scope, since it exposes the practices of an organization without commenting directly on the surveillance of individuals.

(4) We included pieces that artists did not themselves present as privacy art if they prompted significant critical discussion relating to privacy (e.g., in media discussing the piece). Art is subject to interpretation past intent.
   - *Example:* Arne Svenson's *The Neighbors* [254] consists of photographs taken through windows, prompting outrage from (unwitting) subjects who felt their privacy had been invaded. While the artist said the piece is about life's unnoticed moments, most critical discussion has mentioned privacy, so we include it.
   - *Edge case:* Jason Bruges's *Platform 5* [45] might be seen as involving anonymity or data persistence. We did not find such commentary from the artist/media, so we exclude it.

(5) Many historical oil paintings depict private or intimate moments. We included those for which ensuing critical/scholarly discussion focused on privacy invasion. The voyeuristic facet of viewers' intrusion into private moments connects these works to others more overtly focused on privacy invasion.
   - *Example:* We include Edgar Degas's *Woman Bathing in a Shallow Tub*, as critical analysis often highlights the voyeuristic invasion of privacy of looking through a keyhole at a seemingly oblivious subject [27, 42].
   - *Edge case:* Mary Cassatt's *The Bath* [52], while portraying a private moment in the home, is typically discussed as tender and innocent, not invasive [284], so we exclude it.

3.3 Data Analysis

Because of the size of our database and time-intensive qualitative coding process, we coded a weighted sample of artworks from our database. Because pieces in our Foundation Set were the first suggested by experts or identified by keyword searches, we wanted to oversample those; we did so by weighting them 1.5× works in Sets 2–3. To ensure a breadth of styles and perspectives, we ensured that each artist appeared only once in our sample.

We analyzed 73 sampled artworks using iterative open coding [223]. We employed a rigorous codebook development and consensus-coding process. Each piece was coded in MAXQDA by at least two researchers and all disagreements were resolved within the broader team. All artworks, independent of media, were coded as compiled PDFs containing information from the artist's website (e.g., images, artist statement). If an artist statement was not available, we included text about the work from art criticism or other scholarly literature. If a video or interactive digital element was embedded, coders experienced the element in a web browser and applied codes (e.g., perspective, interactivity) to applicable screenshots [223]. However, most codes were already present in text.

Though there is inherent subjectivity in qualitative and artistic analysis, we applied codes as rigorously as possible to our compilations of images and text about the work. For example, audiovisual component codes (Section 4.2) were derived from observable or audible elements. Beyond cataloging formal elements relevant to privacy communication, we also identified affective aspects aligned with interaction design practices (Section 2.3). More subjective themes, such as topics (Section 4.3) and ambiance (Section 5.4), emerged through textual analysis. Where possible, we used in-vivo-style coding [223]. While an artist may not explicitly outline *why* they used particular mechanisms (e.g., color scheme, composition), artist statements can be informative as to which values may be ascribed to a work as a whole.

Initially, two researchers independently coded four artworks selected for their distinct concepts and execution, generating a draft codebook that they then applied to three additional pieces, discussing the state of the codebook with the larger research team. At this point, two additional coders joined the team, and all four coders reached consensus on codes for seven additional artworks. The four researchers then independently coded 15 artworks from our sample, meeting as a full team after every five artworks to discuss new codes and themes. At that point, we moved to a split-coding approach where these four researchers worked in rotating pairs, independently coding each artwork. Each pair met to discuss and resolve disagreements after every five pieces, while the full research team (including faculty in both the arts and computer science) also met regularly to review the state of the codebook.

We continued this process until no new codes were introduced for five artworks in a row per pair of coders. This occurred after 73 artworks. Our full codebook can be found in Appendix C, and an example of a coded work can be found in Appendix D. Due to the subjectivity of and vastness of creative works, we focus on reaching a stable understanding of components, mechanisms, and their affective aspects, rather than conventional saturation of knowledge. Though artworks with unique mechanisms may exist beyond our sample, our aim is not to enumerate all possible mechanisms; rather, we examine those common among multiple artworks, so we may compare and contrast how these are used.

3.4 Study Team Composition and Positionality

Our interdisciplinary team's expertise spans both the art and computer science domains. All four coders are students at various levels focusing on computer science, but with additional academic experience (e.g., double majors/minors in media arts) or prior experiences publicly exhibiting art. Our broader study team includes faculty members in computer science (specializing in security and privacy), the arts, and media studies. All faculty members have taught academic courses that discuss surveillance art. This combination of artistic understanding and technical privacy knowledge enabled our team to interpret artworks through both lenses, facilitating nuanced analysis that bridges the gap between artistic expression and applications in privacy research.

3.5 Limitations

Our work has a number of limitations, many of which are common in qualitative analysis.

Scope. Though our database of privacy art is by far the largest to date, it is likely impossible to create one that is comprehensive. While we relied on web searches, suggestions from practicing privacy artists, and multiple other methods, it is near certain that we missed works. For example, our keyword searches included terms related to *surveillance art*, which was characterized in the 2000s and 2010s alongside the rise in surveillance technologies [40, 182]. This may bias our database towards more recent works and those that include these technologies (e.g., surveillance cameras). Some privacy artworks are likely to remain inaccessible—not archived online, lost to time, or lacking documentation. Furthermore, while our research team is multilingual and includes multiple cultural backgrounds, we are all affiliated with universities in a single country. There are likely works that we cannot access based on either language barriers or different cultural interpretations of privacy. Due to our methods, though, it is likely that we covered many of the most notable privacy artworks. That said, we intend for our database's website to be a living document; as such, it includes a form with which others can submit artworks for possible inclusion.

Weighted Sampling. Since we intentionally biased our sampling process toward the Foundation Set, we potentially overrepresent well-known artists and more recent works in our selection. While this may limit our analysis of less-well-known artists and older works, we seek to map common techniques in the space in our analysis rather than evaluating every topic or mechanism. Additionally, these works have expectation to be public and to be analyzed.

Formal Arts Institutions. While privacy communications can employ multiple media [226], visual elements, such as those present in formally exhibited artworks (Section 3.2), are most prevalent. However, formal art institutions may be skewed towards Western perspectives and built upon colonialism [19, 115], often excluding independent artworks such as grassroots art, graffiti, protest art, and memes. These abundant artistic practices have distinct modes of interaction and creation warranting further in-depth exploration in future studies. Even if posted online, independent artists may not expect their work to be analyzed in academic contexts [85]. Researchers should collaborate with communities and artists when studying these works [55, 185]. To conduct a large-scale analysis, we focus on formally exhibited artworks that have an expectation of being viewed by large crowds and being the subject of critical discourse. Formal venues have more consistent documentation and accessibility, making them better suited for our analysis.

Subjectivity. Art is subjective, creating interpretive challenges. Our team viewed works through a technical privacy lens. While we used consensus coding on available statements by artists themselves and/or art critics, we cannot capture all possible interpretations. Similarly, selection criteria boundaries are inherently debatable. Our team debated selection criteria over months and spent extra time deliberating over edge cases. Though our criteria are certainly not the only basis for evaluating privacy artworks, we chose them based on applicability to usable privacy research.

Perspective. We characterize our interpretations and those suggested by the artists (or critics), not viewers of the artwork, differing from actual experiences of art. It is unreasonable to assume that an artwork will have the same effect on every viewer. Our team viewed most artworks outside their original context (i.e., online or in photographs, rather than in a gallery or in-person exhibition). We also relied heavily on artist statements, which are often a secondary or tertiary artifact in a gallery setting. We attempted to standardize formats and consulted direct sources (e.g., quotes or artist statements), if possible. Nonetheless, our approach may have missed notable nuances of these artworks.

4 Results: Components in Privacy Art

In this section, we provide an overarching look at what privacy artists are saying in their art. Section 4.1 describes our database and sample set composition and Section 4.2 details audiovisual components (e.g., symbols, objects). After discussing topics present in the works (Section 4.3), we discuss how artworks emphasize different subjects of privacy invasion and data collection (Section 4.4).

4.1 Database Characteristics (RQ 1)

As of this writing, our database includes 859 artworks by 332 unique artists, 78 of whom collaborated with others. Our database spans over 350 years of privacy art: the earliest work is *Las Meninas*, painted by Diego Velázquez in 1656; the latest pieces are either ongoing or are currently exhibited at an artistic venue.

Sample Set Composition. Our sample set includes 73 works (see Appendix B). While many works are collaborative, all artists appear only once in the sample set. Artists came from national backgrounds spanning 32 countries; most artists are Europe-based (49%), followed by the Americas (37%, 31% US-based), and Asia (11%).

The earliest work our team coded was painted in 1657-1659, and the most recent works were pieces ongoing or exhibited in 2024. The most common decade (N=36) in our sample are pieces from 2010-2019. The least represented (N=5) era is pre-2000s. Half those from 2010-2019 (N=18) deal with data access and agency, mirroring increases in consumer technology use and rise of social media. Beyond this connection, works from different time frames use diverse methods and explore myriad topics.

Privacy artworks in our sample set employ a wide spectrum of media, some even employing multiple media (see Appendix B). There are 27 digital pieces, including 23 software-controlled systems (i.e., using code to drive or manipulate the installation), a virtual reality experience (A25), and a video game (A30). Ten pieces use electronic hardware, such as computers. We also saw 11 video-based artworks. Six others included animated images (e.g., GIFs). Still images are in 19 pieces, including eight photographs, and two (A41, A55) paintings. Seven pieces take on tangible forms through textiles and wearables. Another seven pieces are three-dimensional sculptures using raw materials or manufactured products. Beyond discrete media, nine pieces use immersive exhibits that collapse the distance between artwork and audience. Seven live performances further engage real-time dynamics through human or machine agents. Finally, eight architectural installations use preexisting or constructed spaces (e.g., buildings or rooms) to explore privacy in physical environments.

4.2 Sensory Vocabulary of Privacy Art (RQ 2)

Artworks following our criteria are constructed from audiovisual components, which set tone, create a visual shorthand, or indicate symbolism. *Visual components* are items or symbols appearing visually in an artwork.

Familiarity as an Anchor in Reality. Thirty-three artworks turn to familiar settings (Section 4.3), human forms, and objects to develop comfort or conduct satirical critique. Thirteen pieces use imagery from familiar settings—for example, offices (A6, A40, A59) or airports (A50)—showing how innocuous locations may be part of the surveillance apparatus (see also Section 4.3). Fifteen pieces include human forms both real (N=11) or digital (N=5), inviting the viewer to relate to the subject or face the uncanny. Commonplace objects also play a role in centering privacy experiences in daily life. Five pieces feature smartphones; three (A11, A13, A30) display text messages on a phone in the piece and two (A6, A44) provide interaction on a viewer's device. Two pieces comment on the security from (A32) or embedded into (A20) clothing. For example, Doringer's *The Hoodie* (A32) uses AI-generated images of a hoodie as commentary on how it might be the only counter-surveillance tactic an individual has at their disposal (see Figure 2b).

Transforming the Abstract Digital into the Tactile Physical. Some artists translate digital information into familiar tangible forms using materials that emulate touch, comfort, and daily life. Five works use paper to ground digitized information in a more traditional format, including printed screenshots of text messages (A6) and NSA documents (A55). Two pieces (A33, A53) transform fleeting, intangible data into a permanent print form. For example, a simple robotic arm in MSCHF's *Eavesdropper* (A53) writes out overheard words of viewers in Sharpie (see Figure 2e), turning casual speech into an enduring artifact. Three pieces (A7, A59, A70) embed digital information into textiles, such as cross-stitch depicting surveillance footage (A70), a word cloud of common passwords sewn into a quilt (A7), and carpet tiles with color patterns correlated with the frequency of email exchanges (A59). Through these tactile materials, digital surveillance becomes something viewers can literally feel—a reminder of how deeply it threads through daily life.

Cameras and Microphones. Twenty pieces include visuals of surveillance devices, drawing attention to objects viewers may typically ignore due to familiarity. Cameras were visible in 17 pieces, types including eight bullet, five dome, two (A39, A49) web, two (A60, A67) video, and a smartphone (A13). While some cameras are functional (see Section 4.4), cameras in eight pieces are non-functional or are even presented in a novel medium—in photos (A9), VR (A25), or marble sculpture (A12) (see Figure 2c). Though nonfunctional cameras do not capture data, they imply observation and act as a proxy for surveillance. Some pieces contain visible audio equipment to record (A22, A53) or play audio (N=5), including microphones (A22, A53), speakers (N=5), and megaphones (A3, A47). Together, these visual cues of monitoring equipment evoke an atmosphere where observation feels ubiquitous.

Linguistic and auditory content. Many artists turn to language and sound to shape how viewers engage with surveillance, with 35 works incorporating written or auditory communication. Plaintext is an important component in 26 pieces, filling a role beyond supplementary statements or descriptive text for the piece. For example, ten works use labels for data visualizations, six provide additional context, and two (A33, A42) give instructions (e.g., prompts in an app (A42)). In 13 pieces, plaintext even features as a central subject: social media posts (A39, A45, A59), text messages (A6, A11), transcripts (A16, A53), and browser history (A33, A59). Fifteen pieces include music (N=9) or narration (N=7). Music (N=9) may help set a mood (see Section 5.4). Robotic voices lend technology a voice in four pieces for communication with viewers (A3, A5, A43) or for narration (A1). In contrast, three pieces (A8, A62, A73) use human voices to highlight humanity behind technology. In Coupe's *Sanctum* (A73), a human voice narrates the text of an online post, mapping the individual being viewed to a specific identity and age.

4.3 Privacy Concepts Explored in Art (RQ 2)

We determined topics in privacy artworks by consulting artists' statements and documentation concerning the works. The most common topic (N=33) in our sampled dataset was organized surveillance of individuals, commonly in conjunction with resisting surveillance (N=23). Other common topics include identity in context of privacy invasions (N=27), relationship between public and private space (N=15), and exposure of personal data (N=9).

Organized Surveillance and Data Collection. Thirty-three pieces comment on organized surveillance by entities like governments or

WHY DON'T PEOPLE
A
REVOLT?

(a) Mariam Ghani's *Security Blanket* restages a familiar childhood bedroom setting [101]. ©Mariam Ghani

(b) Bogomir Doringer's *The Hoodie* presents an everyday item of clothing [cropped] [73]. ©Nieuwe Instituut

(c) Ai Weiwei's *Surveillance Camera*: A camera sculpture carved from marble [5]. ©Phillips Auctioneers

(d) Plaintext in Surveillance Camera Players' *The Mass Psychology of Fascism* [209]. ©NOT BORED!

(e) MSCHF's *Eavesdropper* (41×67 inch) uses a robot arm to write what viewers say [184]. ©Galerie Emmanuel Perrotin

Figure 2: Examples of the visual and auditory components of privacy art.

corporations, often portraying these forces as intrusive, inequitable, or quietly omnipresent. Twenty-nine comment on pervasive government and large-scale surveillance of citizens and the resulting power disparity. For example, Luo's *If This Is a Global Surveillance Center* (A23) accesses video feeds of public surveillance cameras, equating control of data to "dominance over physical space" [160]. Other works address government surveillance even more directly, such as the US National Security Agency (NSA) (e.g., A55). Ten artworks focus on corporate-driven privacy invasions, with three (A33, A71, A73) exploring data collection within specific companies like Facebook, illustrating how private information can be mined within everyday platforms on which people routinely rely.

Resisting surveillance. Twenty-three pieces additionally focus on resisting surveillance, with 15 exposing surveillance and four offering direct interventions. Four pieces (A1, A17, A24, A32) also explore this concept abstractly, such as repurposing surveillance equipment to monitor air pollution instead of people (A24).

Fifteen pieces expose surveillance practices, which can point out omnipresent observation and encourage reflection on surveillance apathy. By revealing practices that often fade into the background of daily life, artists encourage viewers to confront the extent to which constant observation has become normalized. Six glamorize surveillance, drawing attention to the practice by ornamentation or idolization (see Section 5.4, Figure 3a). Five pieces expose existing CCTV cameras, showcasing the prevalence of surveillance in public settings, with three (A35, A42, A46) exposing specific locations. In The Institute for Applied Autonomy's *iSee* (A35), CCTV cameras in New York City are collected on a map, so viewers can identify and avoid their specific locations (see Figure 3b). Two pieces (A9, A23) explore the prevalence of cameras ambiguous from location, such as repeated images of different CCTV cameras in London (A9) (see Figure 1f). Five pieces expose government surveillance tactics (A31, A36, A55) and the web of individuals behind these systems of control (A36, A37, A58). Lavigne's *3 Degrees of Separation* (A37) uses a network graph to expose individuals with surveillance skills publicly posted on LinkedIn. One piece (A66) exposes the environmental cost of cookie tracking—an unseen expense of surveillance.

Beyond exposure, several artists imagine direct countermeasures. Four pieces (A2, A31, A44, A71) show direct interventions that could be used to hide from surveillance. Two (A31, A71) use obfuscation. In Elahi's *Citizen* (A31), part of *Tracking Transience* (2003-Ongoing), Elahi floods the FBI with mundane photos of his life (e.g., meals, toilets) to combat profiling with radical transparency (see Figure 3c) [80, 132]. Differently, Grosser's downloadable tool *GoRando* (A71) obfuscates users' reactions on Facebook by randomization. Two pieces serve as proof of concept, showing inventive possibilities of directly combating surveillance: Burtch's *Mic Jammer* (A44) mutes phone microphones, and Harvey's *HyperFace* (A2) cloak tricks a specific facial recognition system (see Figure 1d).

Privacy-Invading Technology, Algorithms, and Identity. Twenty-seven works cover the interplay between personal identity and privacy invasions. Eleven pieces comment on how algorithmic systems construct, distort, or conceal assumptions about who a person is, revealing the gap between lived identity and computational shortcuts used to define it. For example, Ọnụọha's *Classification.01* (A21) hides an algorithm and its calculations from viewers, flagging viewers as "similar" through hidden sensors, pointing to opaque judgments embedded in machine classification. Three pieces (A1, A31, A36) highlight profiling and the use of assumptions about identity as an excuse to surveil marginalized groups, such as Boundaoui's documentary *The Feeling of Being Watched* (A36) exposing FBI tactics used to surveil her Arab American community.

Relationship Between Public and Private Space. Similar to architectural literature [119, 128], several works probe shifting boundaries between public and private spaces. Eight use public infrastructure to spotlight or draw attention to surveillance of public spaces. Three of these (A45, A46, A73) seamlessly integrate with existing infrastructure, such as glamorously decorating public surveillance cameras (A46) or projecting videos onto a building (A73). Four pieces simulate more personal locations like homes (A41) or bedrooms (A8, A29, A69) (see Figure 2a) to emphasize how normally safe, private spaces may still be invaded. Although many works focus on physical spaces, four (A39, A45, A52, A59) explore how increased data collection blurs the line between public and private in digital space. Lowe's *You Saw Me?* (A45) projects Facebook status updates on the side of a building in a public area, showing how seemingly private or personal online activity may be seen by unexpected viewers.

(a) Giles Walker's *Peepshow* installation exposes surveillance with glamorous pole dancing CCTV cameras [186, 270, 273]. ©Wieden+Kennedy

(b) The IAA's interactive map, *iSee*, exposes surveillance camera locations, indicated by red squares [202, 268]. ©Rich Pell

(c) Hasan Elahi's *Citizen* obfuscates surveillance by collaging mundane photographs (e.g., meals, toilets) [78, 79]. ©Hasan Elahi

Figure 3: Examples of resisting surveillance in privacy art (see Section 4.3).

4.4 Subjects of Privacy Invasion (RQ 2)

Artists play with different collection sources and subjects of privacy invasions (the public, the artist, and the viewer). Pieces collect data through a variety of channels, including cameras (N=17), public datasets (N=10), tech-mediated communication[2] (N=10), microphones (A8, A16, A53), and a viewer's personal device (A6).

Invading Privacy of the Public (Aggregated and Individual). Seventeen pieces focus on invading the privacy of the aggregated public, showing the limitations of privacy in any number of private spaces (both physically and digitally). Twelve pieces draw on public datasets, including publicly available city datasets (A24, A34, A54, A66) (e.g., traffic), location data (A24, A35, A54), social media posts (A39, A73), and leaked passwords (A7). Similarly, four (A23, A38, A68, A70) works aggregate and obscure—such as through generative AI (A38)—camera footage of the unknowing public. Giasson's *VOX* (A16) features secretly-overheard conversations transcribed onto transparent panels; this aggregated data gives little insight into subjects' identities. These works illuminate how anonymity in masses can be less secure than it appears, revealing structural vulnerabilities that affect populations rather than isolated individuals.

While 17 pieces focus on the public in aggregated format, six focus on public individuals. Three (A15, A39, A67) highlight specific individuals, which may show how publicly accessible information can be used against any person. For example, Riekstins's *Back to the Light* (A15) restores deleted files from secondhand hard drives, showing that data persists on physical devices. Two works (A37, A58) focus on individuals' part of the surveillance apparatus (see Section 4.3). Hovers's *The Right to be Forgotten* (A18) uniquely focuses on a very specific subject, the first man to successfully claim his "Right to be Forgotten" in Europe. Hovers creates a series of multimedia images based on a digitally accessible image of the man, illustrating that one can have a digital footprint despite attempting to erase it. Using specific individuals' data demonstrates that breaches of privacy are not abstract phenomena, but direct incursions into real lives and identities.

Invading the Personal Privacy of Artists and Performers. Artists may invade the privacy of themselves (N=11), performers (A4, A10, A27), or study participants (A44) to act as a viewer proxy, showcasing intimate privacy invasions.

In 11 pieces, artists invade their own privacy in a more intrusive way than they could that of a viewer. Six pieces display artists' personal data. Two (A59, A64) contrast dense and specific data displayed in different formats, showing how small segments of data can be more personal. Mattes and Mattes's *My Little Big Data* (A59) shares over 13 years of the artists' digital information in a video essay and installation with data visualizations and schematics of their apartments (see Figure 1g). In contrast, Goni's *Deletion Process* (A33) presents the artist's search queries one at a time, which may showcase the information derived from even a small piece of data. Three pieces (A4, A10, A44) transform a viewer's perception of "normal" observational contexts (e.g., performances) into surveillance with computer vision (A10) and other means.

Invading the Privacy of the Viewer. Sixteen pieces invade the viewer's privacy *non-consensually*. By viewing or experiencing the artwork, viewers inherently become part of the piece. This can potentially draw a stronger, more personal reaction, as the act of experiencing the piece becomes inseparable from the experience of being observed. Viewers' data is typically collected through cameras (N=13); two works employ (A8, A53) microphones (see Figure 2e). Six pieces process video data before it is displayed to the viewer, three (A21, A57, A67) use computer vision visuals (see Section 5.2), and one converts video data into a different medium (A3). For example, in Depoorter's *Surveillance Speaker* (A3), a camera captures gallery visitors' actions, which are run through a computer vision algorithm and narrated out loud with a robotic voice (see Fig 1c). Two (A49, A73) pieces simply present the viewer with a video of themselves without modification, emphasizing the immediate feeling of being observed. Using the viewer as a data source forces them to confront how easily their personal behaviors, movements, and voices can be captured, analyzed, and displayed, transforming passive observation into a deeply personal experience.

5 Results: Mechanisms to Present Components

In this section, we provide an overview of mechanisms used to showcase the topics presented in Section 4. We examine how artworks influence the viewer's gaze (Section 5.1) and control the

[2] Tech-mediated communication may include SMS (A6, A11, A30), browsing history (A33, A59), or social media (A39, A71, A73).

viewer's perspective (Section 5.2), concluding with viewer interaction (Section 5.3). Finally, we examine various tonal portrayals of privacy violations in Section 5.4.

5.1 Directing Viewer Attention (RQ 3)

Artworks can direct attention toward important elements through techniques of emphasis but also reveal elements through techniques of obscurement. Common techniques include lighting, collages, or even obscuring information.

Alerting Viewers at the Moment of Privacy Invasion. Three pieces (A39, A42, A56) alert viewers to an invasion of privacy the moment it happens. By providing real-time notifications, these works may show the frequency of surveillance and allow viewers the opportunity to recognize and potentially avoid future intrusions. Blinder's *Dark Side of the Prism* (A56), a downloadable tool, plays a snippet of Pink Floyd's *Dark Side of the Moon*[3] each time the NSA's PRISM[4] invades a user's privacy. Wunderling's *Audience* (A39) displays a public image from Flickr and takes a photo of the viewer, then immediately notifies the owner of the public image that it has been viewed by commenting a blurred version of the viewer's photo on the image. The viewer in turn sees the publicly posted comment. In-the-moment alerts expose the immediacy of privacy invasions while prompting viewers to consider their own vulnerability.

Exposing Those Surveilled and Surveillance with Lighting. Eight pieces use lighting to indicate surveillance and direct viewer attention. Lighting can be an analogy for visibility, paralleling the implied spotlight of being under surveillance. Five pieces use lights to direct viewer attention to a specific area of a piece, where two (A4, A25) highlight surveilled subjects. In Huang's *The Eye and I* (A25), a central lighthouse emits a rotating spotlight, illuminating cells within a VR panopticon. Two pieces use light to indicate that surveillance devices are active (A21, A57), such as a subtle white bounding box framing the viewer's face in a mirror (A57). Instead of using light to explicitly direct a viewer's attention, Ådahl's *The Exhibited* (A4) uses contrasting bright and dark spaces where performers can move between to "escape" the spotlight, though they remain visible in every location (see Figure 4b).

Showing Connections and Scope with Collages of Information. Twenty-seven pieces use a collage effect for display. In these pieces, viewer attention is directed to *multiple* visual components (e.g., images, videos), which may show the vastness of surveillance and data collection. Six pieces showcase still images in grids (see Figure 4a), ranging from photos of surveillance cameras (A9) to objects (e.g., food, toilets) from an artist's personal life (A31), both exposing and obfuscating surveillance. Five pieces display video surveillance footage in grids, showcasing the vast amount of data collected by CCTVs. Two pieces use grids to display non-photographic content such as identification (A48) and leaked government documents (A55). One (A7) uses overlapping collage to display a colorful word cloud of common passwords.

Obscuring Information with Composite. Six pieces used composites i.e., combinations of multiple overlaid images that create a new image. Using composites could illustrate how a specific individual can be lost when part of an aggregate. Over 1,000 individuals' faces are obscured in Riekstins's *Back to the Light* (A15) as they are overlaid on top of one another, making a single hazy and unidentifiable face (see Figure 4c). Similarly, Tarar's *Landsat.Earth* (A26) showcases low-resolution images of earth for monitoring of the atmosphere stitched together. Though this technology is part of the surveillance apparatus, in this form it is unable to be used for the direct surveillance of individuals.

5.2 Viewer Perspective (RQ 3)

The relationship between observer and subject is a common theme in privacy art [40, 182, 271]. Attention drawn to surveillance may be fetishistic in nature (A46, A47). In Vermeer's *A Girl Reading a Letter by an Open Window*, the viewer peers into a young woman's private moment (featuring symbolic elements such as window blinds thrown open, suggesting an affair) [260] (see Figure 5a). In other cases, the viewer is the subject of a voyeuristic gaze—watched by a giant eye (A25) or being in a space with large windows leaving nowhere to hide (A69). In two (A4, A8) pieces, viewers are both the observer and the observed. In Ådahl's *The Exhibited* (A4), the performers watch back, inspired by historical "Human Zoo[s]" [291]. In Ghani's *Security Blanket* (A8), initial viewers whisper secrets into a wall; future viewers listen.

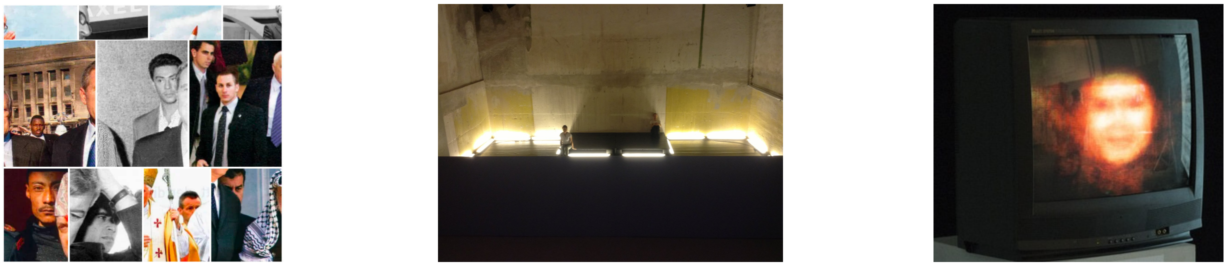
Camera POV. Thirteen pieces used a camera point of view (POV), immersing viewers in the perspective of surveillance (see Figures 5b–5c). Ten pieces specifically focus on surveillance systems which look down on subjects from a bird's-eye-view, allowing viewers to explore what surveillance cameras "see" and feel the inescapability of being in view (see Figure 5b). This POV is commonly (N=11) displayed as videos on monitors such as flat screen televisions (A39, A50, A73), cathode ray-style televisions (A14, A15 A60), CCTVs (A29, A67), or computer monitors (A49). Uniquely, Leclercq's *Embroidered Surveillance* (A70) displays "1/24 second" stills of surveillance footage in cross-stitch, creating a frozen, permanent contrast to the fleeting nature of a moment. Six pieces make use of livestream video, with three (A14, A49, A73) directly surveilling the viewer (see Section 4.4) and one (A67) surveilling members of the public nearby. Viewers hold the objectifying gaze of the surveillant and may question their role in systems of observation.

Visualizing AI. Seven pieces use a camera POV in conjunction with bounding boxes and image distortion to display how cameras "see" with AI and computer vision. Five works use bounding boxes to outline faces (A2, A10, A57, A61) or bodies (A67) and two (A2, A10) comment on possible facial recognition errors (see Figure 5b), drawing attention to the assumptions embedded in algorithms. Two pieces (A32, A38) feature morphed bodies and environments as a result of small datasets being fed into a GAN (generative adversarial network) (see Figure 2b), creating an eerie stitching of images. These visualizations reveal the interpretive power and the potential misjudgments inherent in AI-driven surveillance.

[3] The iconic album cover of Pink Floyd's *Dark Side of the Moon* (1973) prominently features a triangular prism on a black background.

[4] PRISM is an online surveillance program run by the US NSA that collects user data from websites and services like YouTube, Facebook, and Yahoo, among others.

[5] Gemäldegalerie Alte Meister, Staatliche Kunstsammlungen Dresden

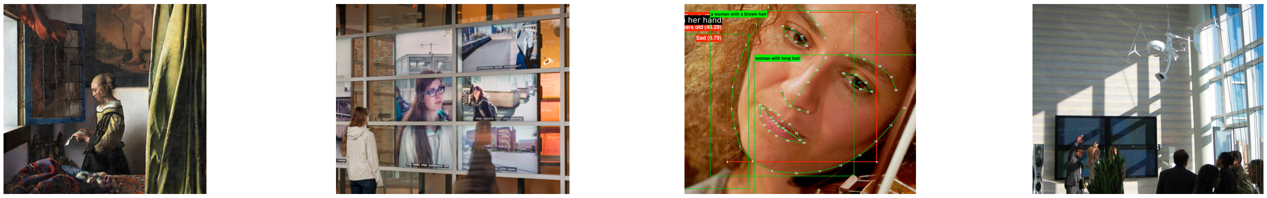


(a) Viktoria Binschtok's *Suspicious Minds* uses collage to show multiple cropped photographs [30]. ©Viktoria Binschtok

(b) Anna Ådahl's *The Exhibited* employs lighting to show more private and less private spaces [291] ©Anna Ådahl

(c) Peters Riekstins's *Back to the Light* layers different faces into a composite, unidentifiable face [162, 218]. ©Kristine Madjare

Figure 4: Different mechanisms for directing gaze including collage, lighting, and composite (see Section 5.1).



(a) Johannes Vermeer's *A Girl Reading a Letter* [cropped] shows a voyeuristic perspective [64, 260, 267]. ©Hans Peter Klut/Elke Estel[5]

(b) James Coupe's *Sanctum* shows the viewers looking up at the camera POV from the devices that surveil them [61]. ©James Coupe

(c) Trevor Paglen's video *Image Operations* visualizes computer vision through bounding boxes with correct and incorrect labels [198]. ©Trevor Paglen

(d) Björn Schülke's *Drone #4* looms above viewers in the gallery, who must look up to see the hanging sculpture [230]. ©Björn Schülke

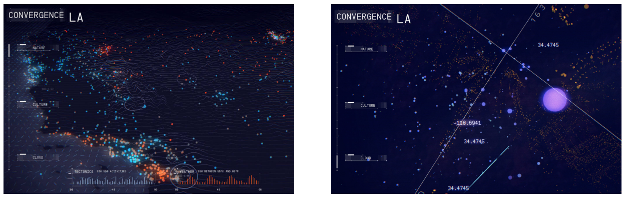
Figure 5: Examples of different viewer perspectives in privacy art (see Section 5.2).

Surveillance Infrastructure Looms Above Viewers. Seven works situate surveillance tools looming over viewers, such that they must physically look up to experience the work (N=6). A looming perspective can imply observation and allude to tools of surveillance being beyond reach or control. Three pieces (A3, A5, A22) are displayed above a viewer in a gallery setting, two of which hang from the ceiling (A5, A22). Schülke's *Drone #4* (A22) is a monochrome conglomerate of surveillance equipment hung by a string above viewers, with parts swooping downwards (see Figure 5d). Two pieces (A45, A54) are projected onto skyscrapers, potentially reinforcing the idea that surveillance towers over everyday life. Differently, Bridle's *Every CCTV Camera* (A9) features photos of surveillance cameras shot from a worm's-eye-view (see Figure 1f).

5.3 Viewer Agency and Interactivity (RQ 3)

In 16 pieces, viewers are active agents rather than passive subjects, which may create a more visceral experience of surveilling and being surveilled. Viewers can interact without being surveilled (N=10), as a countersurveillance intervention (A35, A42, A56, A71) (see also Section 4.3), or under surveillance (A6, A8, A14, A60).

Viewer Exploration in Absence of Being Surveilled. Eight works let viewers directly explore the piece with the agency of the surveillant, making decisions on interpreting and scaling the presented data. This shifts the viewer from passive subject to active participant of the surveillance apparatus, highlighting the mechanics of surveillance and the potential for control or resistance. Five include web-based interactive data visualizations. Anadol's web version of *Convergence LA* (A54) allows viewers to directly interact with scale by zooming in and out from a typographic map of Los Angeles into a "molecular" level of data transfer (see Figure 6). Differently, other works offer tools designed to counteract surveillance rather than replicate it: two pieces (A56, A71) are downloadable tools to combat surveillance online through alerts and obfuscation. In Vasiliev's *Netless2* (A17), viewers may engage with the work (which details a new data transfer system) by sending messages through a network integrated into a model train system (see Figure 7).



(a) Zoomed-out view showing a map of LA and weather data [8].

(b) Zoomed in with coordinates and digital data transport [8].

Figure 6: Refik Anadol's *Convergence LA* (web-version) viewers explore a map of LA by zooming from natural (Figure 6a) to digital (Figure 6b) data [8]. ©Refik Anadol

Compulsory Participation. Viewers who are observed (N=9) (see Section 4.4) have some agency to move out of view of the camera or remain in silence to avoid recording, but they have still been

Figure 7: Danja Vasiliev's *Netless2* allows viewers to interactively send secure messages through a model train [266]. ©Danja Vasiliev

surveilled. Works that force viewer participation highlight the tension between agency and surveillance, showing that seemingly innocuous participation can serve the surveillance apparatus. Two pieces directly ask for viewer participation—like telling a secret (A8)—or texting a viewer's device with an action—like "I left you something on the printer" (A6). In these cases, information is taken from a viewer (e.g., secret, cell information). Sometimes, the interaction control is more subtle, e.g., viewer distance (A14, A39, A60), where a video of a dog barks louder as the viewer approaches (A60).

Info Withheld About Surveillance. Six pieces have information deliberately censored, which could make a statement on the limited information available about the everyday surveillance apparatus. Viewers are directed to consider what is *absent* as much as what is *present*, prompting reflection on the unseen forces that shape observation. Two pieces (A21, A57) use hidden cameras and indirectly show the viewer the outcome of the observation. Information may also be withheld by censoring or caricaturing dataset contents. Treister's *Camouflage* (A55) obscures segments of leaked NSA documents concerning surveillance and data mining with geometric paintings mimicking shapes in the documents, warping their original meanings. These works reveal the gaps of information inherent in surveillance. What is purposefully hidden can be as revealing about power and control as the data that is openly displayed.

5.4 Ambiance (RQ 3)

What is shown, and *how* it is shown, contribute to the atmosphere of a piece and the viewer's emotional response to it. In our sample set, we found four common tones to privacy invasions: *mundane*, *overly formal*, *unsettling*, or *fun*.

Mundanity of Surveillance. In seven pieces, surveillance blends into ordinary settings such that it becomes seemingly uneventful, normalized, or overlooked. Ghani's *Security Blanket* (A8) recreates the setting of a cozy childhood bedroom in soft, neutral colors where visitors whisper secrets into a hidden wall, which is recorded without viewers' knowledge. Its success collecting intimate, private answers from viewers demonstrates how the nostalgic comfort and security of childhood may lower people's defenses against surveillance and privacy invasion. Three pieces (A68, A69, A70) comment on the existing surveillance infrastructure. Three (A4, A31, 68) use mundane contents as the data subject. For example, Sidén's *Sticky Floors* (A68) documents the full daily cycle of a pub through its own security cameras, making constant observation feel like part of the venue's natural rhythm (see Figure 8a).

Ostentatious Formality. Ten artworks are framed as serious or formal to emulate and critique formal structures of power. Three pieces (A11, A18, A55) feature framed images of text messages (A11), images (A18), and government documents (A11, A18) to emphasize their importance and subvert expectations about what belongs in a frame. Two pieces (A12, A51) use marble to mimic the formality of government regulation. For example, Kraft's *Twelve Nodes* (A51) uses marble as a backdrop to display imagined rules for protecting privacy; the choice draws on marble's legacy in the first written legal code of ancient Rome, imbuing the proposed rules with stately significance [141] (see Figure 8b). Ai's *Surveillance Camera* (A12) monumentalizes surveillance: a marble CCTV camera as an anti-monument, the material drawing on cultural traditions of commemoration and past political symbols to emphasize the longevity of government surveillance [5] (see Figure 2c).

Unsettling Invasions of Privacy. Eighteen pieces induce viewer anxiety about privacy invasions. Six pieces convey the constant, inescapable sense of surveillance, similar to the "Panopticon" [25] (see Figure 8c). Four pieces (A25, A38, A43, A72) describe eerie and dystopian futures of technological control and surveillance. Other works may induce disorientation (A5, A14, A38, A49). Nauman's *Live-Taped Video Corridor* (A14) confronts visitors with an unsettling split image: the viewer's live reflection shrinking away in one monitor and complete absence in the other.

Thirteen pieces feature exposed wires or raw components, and seven pieces feature industrial styling (e.g., concrete, exposed pipes). These visual styles may emphasize intrusions of technology into private life. For example, Scher's *Papa Bed* (A29) has a mass of wiring and technology sprawling around a plain bedframe. Eleven pieces distort familiar objects into uncanny new forms. Six pieces include modified human visuals such as digital avatars (A1, A25), AI-distorted figures (A32, A38), or blocky facial features to trick AI (A2). Digital representations draw on both familiarity and a sense of detachment, creating a sense of tension for the viewer.

Making Privacy Violations Fun. Sixteen artworks created fun or playful atmospheres for the viewer, potentially for engagement or as juxtaposition to the underlying privacy violation messaging. For example, in Larios's *Surveillance Cutie* (A49), pink reflective foil and warm colors create a bubbly, cutesy tone, in contrast to the stark message of control under surveillance (see Figure 8d). Five pieces also use familiar music. Some music acts as jokes: for example, Stevie Wonder's *I Just Called to Say I Love You* plays during a mysterious phone call to viewers' phones (A6). Six pieces make surveillance glamorous. This can sometimes be literal, with four pieces (A34, A46, A47, A49) decorating or idealizing surveillance infrastructure. Walker both glamorizes and fetishizes surveillance in *Peepshow* (A47), where anthropomorphic robots with security cameras for heads perform a pole dancing routine in a club setting (see Figure 3a). The viewer is enticed to stare at the display; they then confront the visual of the surveillance camera as it stares back.

Ten works are framed as humorous or satirical. In five pieces, the surveillance apparatus itself is parodied. For example, Bunting's *The Status Project* (A72) does a satirical take of the class system to comment on surveillance and the power of corporations (classified as artificial humans). Five pieces use exaggerated, over-the-top humor. While this technique may underscore absurdities of surveillance

(a) Ann-Sofi Sidén's *Sticky Floors* frames a mundane tone by showing daily surveillance footage at a pub [238]. ©Ann-Sofi Sidén

(b) Egor Kraft's *Twelve Nodes* presents proposed Fair Data rules on marble blocks in a serious, formal tone [141]. ©Egor Kraft

(c) Hsin-Chien Huang's *The Eye and I* creates unsettling VR panopticon with the eye and surrounding cells [124]. ©Hsin-Chien Huang

(d) Fabiola Larios's *Surveillance Cutie* adds fun to surveillance with pink bedazzled vintage TVs [144]. ©Fabiola Larios

Figure 8: Examples of pieces that feature different ambiances such as mundane, formal, unsettling, and fun (see Section 5.4).

systems (A6, A27, A42), some pieces highlighted fatuous measures to protect personal security in a highly surveilled world (A1, A20). For example, Mann's *EXISTech* (A20) promotes merchandise such as bags and bras retrofitted with large security cameras designed to deter crime. Two pieces create parodies of existing media (A1, A28). For example, Steyerl's *How Not to Be Seen* (A1) is a satirical documentary based on a Monty Python skit[6] describing silly ways to avoid detection, such as "being female and over fifty" [250].

6 Discussion

In this work, we conducted the first large-scale, qualitative analysis of topics and mechanisms in privacy art. While prior work discussed a few dozen artworks at most, we constructed a database of 859 pieces and performed rich qualitative analysis of a sample of 73, mapping novel approaches for provocative privacy communication. We find that privacy artworks engage with topics like speculating on the future, provide metaphors for privacy, and offer mechanisms like performative privacy invasion with varied ambiance.

Here, we offer early-stage design opportunities for provoking end-user privacy reflection. Paralleling previous provocative design research inspired by science fiction [279], we drew from privacy art. We situate these opportunities within usable privacy research (e.g., pro-privacy tools, education) and interaction design. We also present suggestions for pro-privacy companies (e.g., Mozilla, Brave). Provoking privacy reflection may have conflicting goals or constraints depending on context. Researchers may promote user agency and maintain neutrality [1, 208, 289]. Companies may use persuasive design [24, 87, 108] to influence user choice. Differently, privacy art is often subversive, polarizing, or up-to-interpretation.

Moreover, usable privacy communications rarely center marginalized or repressed populations [86] and at-risk users. While some privacy art explores intimate privacy invasions of the artist or their community, illuminating surveillance impacts and biases (Section 4.3), these techniques and those discussed above may conflict with HCI *standards* and corporate *regulations* due to limited frameworks for privacy and consent in art (Section 2.2). Those adapting these techniques for usable privacy should utilize existing trauma-informed frameworks in HCI research [55, 231], such as SAMHSA trauma-informed guidelines [125], to minimize retraumatization and exhibit ethical data usage (Section 6.5).

We build upon usable privacy and interaction design research to present design opportunities as examples of how privacy art might uniquely apply to these diverging contexts. Future work, however, is necessary to evaluate strategies' actual effectiveness for end users. These theoretical approaches seek primarily to provoke *privacy reflection* with artistic mechanisms, rather than enforcing changes in habit or providing purely educational material. Evaluating effectiveness might follow similar strategies to Plaut et al. to evaluate participants' reactions and reflections on privacy in context of the specific approach [208]. We discuss future speculation, novel metaphors, performative privacy invasions, and physical representations. We end by further discussing ethical implementation.

6.1 Speculating on Society's Future

Most usable privacy tools and communications are situated in the moment [86] and rarely explore societal values [276, 277]. Similarly, people often visualize privacy through small-scale personal settings and interpersonal dynamics [190]. Despite this, experts and users express concerns at a broader scale (e.g., *sale and sharing* of data) that does not appear frequently in privacy visualizations [20], offering an opportunity for usable privacy researchers as explored previously by Wong et al. [277]. Similar to speculative design, some privacy artworks speculate on the consequences of government and corporate surveillance at a societal level (Section 4.3). Future privacy tools in educational and research settings could speculate on the *long-term* impacts of anti-privacy practices. One could imagine a pro-privacy tool offering speculative "what-ifs" [76] on the use of data collected online (Section 5.4), prompting users to reflect. For example, what if this data were sent to your local government? What if this data was used to predict your credit score? Future designs could even present fully fleshed-out future scenarios with stories or imagery. These questions should be developed in conjunction with trauma-informed experts to mitigate potential harms and empower participants to opt out (Section 6.5). While such tools may decrease usability (e.g., increasing pop-ups), they may foster deeper reflection on values and implications of online tracking.

Resistance to Surveillance. Countersurveillance is an important, yet underexplored, aspect of usable privacy [158, 166]. Similarly, speculative designs in HCI often focus on the future of inescapable surveillance technologies *themselves* [88, 259, 279]. However, both our qualitative analyses and the academic literature in media arts [54,

[6] Monty Python is a comedy troupe formed in Britain in the 1960s that was known for their absurdist television sketches.

132, 181] highlight how art can offer speculative takes on *counter-surveillance* (Section 4.3). For instance, some artworks anonymize viewers through speculative designs employing camouflage or obfuscation. One could imagine speculative designs and prototypes that *counter* surveillance infrastructure and empower participants, such as a visor that displays a different face depending on who or what (e.g., a camera) is looking. Researchers could use such designs in interviews and workshops to prompt reflection on how participants can *fight against* surveillance. Given the serious risks that *ineffective* countersurveillance measures pose to at-risk users, researchers should be explicit about the limitations of speculative design, similar to warnings on Harvey's *HyperFace* [117].

6.2 More Expansive Metaphors for Privacy

Privacy art, design, and usable privacy communications all use imagery like microphones, cameras [183], and everyday objects [183, 190, 285, 289] (Section 4.2), though with differing framing. Prior work argues that "icons for privacy choices should be rooted in simple and familiar concepts" [112] and "visualizations based on metaphors or analogies are perceived as more suitable to depict complex concepts" [289], such as privacy [289].

One could imagine interactive worksheets [50, 222] employing metaphors to facilitate concrete communication of participants' privacy preferences. Some privacy art uses (sometimes literal) spotlighting to direct viewer attention (Section 5.1). While illumination can refer to the view of a surveillance camera [207], lighting could provide a visually distinct metaphor for directing attention in educational privacy tools. This could manifest as a visual drag-sort for privacy preferences, moving information into and out of the light to indicate users' desired exposure levels. Differently, researchers could design a worksheet with a flashlight metaphor exposing opaque privacy policies, highlighting key sections with a "beam of light" while dimming extraneous information. Spatial metaphors drawn from domestic or public environments offer another avenue for exploring privacy interpretations (Section 4.2, 4.3). Domestic spaces, often bedrooms, commonly serve as metaphors for real (or perceived) privacy in end-user interpretations [190], privacy education [289], critical design [259], and privacy art. *Public* space may also serve as a metaphor for exposure in privacy art, which we expand upon in Section 6.3.2. One could imagine a similar drag-sort tool moving information into a private "home" and out of a crowd. Previous work suggests that artistic aesthetics could offer design benefits, like increased user satisfaction, beyond usability [4]. Pro-privacy companies could consider metaphorical approaches for users choosing privacy settings, though differing interpretations may necessitate supplementary descriptive text.

6.3 Performative Privacy Invasion

Existing privacy communications usually convey privacy concepts through static text [171, 172, 214, 228] or abstract icons [112]. In some privacy artworks, however, these topics are conveyed through scripted privacy *invasions* with different subjects (Section 4.4). In some, the viewer experiences performative surveillance. In others they are the surveillant (e.g., viewing artist's data, other people). Such provocative simulations of privacy invasion may offer a more concrete way of communicating privacy concepts than abstract usable privacy communications outside of artistic contexts. This echoes Plaut et al.'s suggestion to "[use] problematic technology to teach about problematic technology" [208] and uses of surveillance technology to critique said technology in media arts [11, 18, 246].

6.3.1 *Invading a Viewer's Privacy.*

Most usable privacy tools do not show a user's own data, instead highlighting data collection with icons [112, 183] or sounds (e.g., camera shutters) [63, 226]. Even those that do—most notably privacy dashboards [84, 233]—focus on types of information that apply to most users [71, 216, 272], rather than what makes a user's data unique [217]. Some artworks simulate privacy violations of the viewer (Section 4.4), like using cameras and microphones to echo users' data back to them. Privacy art violates a viewer's sense of *control* [20, 226], which may cause discomfort [22] and demonstrate how users give up control to engage with real-world technologies (Section 5.3). Artworks typically use arguably public (if unsettling) information about the viewer. While this may be adequate for some, at-risk users may face factors that make this invasion *unsafe*. Researchers should collaborate with the at-risk communities (or their proxies) and trauma-informed experts to mitigate harm (Section 6.5). We find that invasions in privacy art have creepy or playful ambiances (Section 5.4).

"Creepy" Privacy Invasions. Creepy and uncomfortable designs focus on technology subverting social norms [22, 143, 258]. In usable privacy, this discomfort often stems from data visualizations leveraging the creepiness of personalization and data inference [217]. Similarly, privacy art often intensifies this through panoptic immersion and unsettling imagery (Section 5.4). Applications for this mechanism would perhaps be most suited for educational tools to prompt reflection on privacy invasions; conversely, creepiness by subverting control may not work well when user trust or autonomy is essential. One could imagine employing users' personal data to build virtual dossiers [217] with a creepy aesthetic (e.g., distorted imagery, unsettling music). Similarly, one could imagine a private browser that locally tracks data similar to that of a less privacy-respecting competitor. Creepy parts of competitor data could be displayed to users to show the disadvantages of switching tools. Such designs raise ethical concerns: provoking discomfort requires clear opt-out options, adherence to differing ethical guidelines [22], and recognition that perceptions of "creepiness" vary widely across users [203, 212, 217].

"Playful" Privacy Invasions. While we had expected privacy artworks to adopt a "creepy" aesthetic [22, 217], we found that some privacy artworks glamorize surveillance satirically (Section 5.4), like placing rhinestones on surveillance equipment [144] or cameras on the heads of pole-dancing robots [186, 270] (Section 5.4). Some previous design research has explored using "positive advertising in framing invasive products" [88, 279]. Future research might consider how a more *playful* or *sensual* aesthetic could be applied to privacy dashboards [84, 233]. One could imagine gilded and glittery notifications when privacy is invaded, such as collecting cute cartoon awards in a trophy case each time the user's data is collected. Researchers should take care to ensure that satirical notifications are interpreted as such (rather than promoting surveillance) before recommending wider adoption. Future usable privacy research could compare the effects of employing creepy and

unsettling visual elements (e.g., distorted figures) with providing surveillance warnings that are cute (e.g., glittery, colorful), where the latter uses juxtaposition to frame user reactions.

6.3.2 Invading Others' Privacy. One could imagine similar aesthetics applied to surveillance camera livestream (Section 5.2), exposing a broader lack of privacy. Research has explored use of surveillance cameras in a museum setting [208], though exploring the data of others could present opportunities in *research settings* to elicit responses about privacy [91]. In privacy art, *public spaces* (e.g., cities, offices) can represent privacy invasion—for example, surveillance camera POV overlooking streets (Section 4.2, 4.4)—contrasting the privacy of bathrooms [190] and homes [190, 289]. Crowded spaces (like the vast sea of online information [85]) can create an expectation of anonymity, though individuals can be singled out. Some privacy artworks violate the privacy of a single (typically unaware) individual observed in "public" (Section 4.4). Other artworks let viewers interactively *surveil* other people's public data in aggregate (Section 5.3). In both cases, viewers experience being the surveillant, looking from a surveillance camera's POV or "seeing" the world as an AI (Section 5.2). While viewer-as-surveillant approaches offer potential for future study, this technique may be best suited for isolated research settings as prompts for provocation and reflection, rather than mass distributed techniques (see Section 6.5.) One could imagine a workshop where participants browse data logs to see what information they can infer, which may allow participants to reflect on what may be gleaned from their own data. Since real data logs are often not human-readable, it may be worth providing parsed versions so users may understand which types of data are collected. Researchers may also consider donated data (Section 6.5) from consenting users, aggregated and deidentified for this purpose.

6.4 Physical Media

Previous work has explored how physical forms can make "abstract concepts more tangible and illustrative" [259] [2, 129, 140, 178, 206, 225, 259], particularly for tactile on and off buttons versus abstract LED indicators [2, 140, 207, 259]. Similarly, some privacy artworks transform digital concepts into tactile everyday objects like printed materials, blankets [62, 101], and carpets [168] (Section 4.2). This can include collages of information (e.g., printed government documents) meant overwhelm viewers and expose surveillance's ubiquity (Section 5.1). Corporate advertisements could consider alternative tangible media to communicate about digital privacy. One could imagine a pro-privacy company (e.g., Mozilla, Brave, DuckDuckGo) plastering a competitor's privacy policy across billboards. Displaying this policy in its full text could visually expose the policy's vastness [171]. It is possible a wall of text could induce similar apathy to that towards scrolling privacy policies [138, 178]. Companies should explore what additional information is needed to make such displays effective, such as explicitly comparing the pro-privacy company's and competitor's policies.

6.5 Privacy and Consent Ethics in Provocations

Here, we elaborate on how trauma-informed HCI frameworks [55, 231] apply to elements of our early-stage design opportunities. We outline minimizing retraumatization and then discuss data usage.

Minimizing Retraumatization. Researchers creating provocations should seek to limit retraumatization [55, 125] for those with personal or cultural surveillance experiences. At-risk users (e.g., immigrants, people with disabilities, historically marginalized communities), may experience more limited privacy [29, 169] and undue surveillance by governments [43, 110, 211, 232]. When considering a tool that prompts participants with questions (Section 6.1), it is important to understand how questions may be understood. To gain perspective [3, 65, 208], researchers should collaborate with trauma-informed experts [55, 286] and communities impacted by the intervention (or proxies like stakeholders with deep knowledge of the population). Interventions should provide trauma resources for viewers/users [55] and allow them to opt-out with proper content warnings [55]. Also, researchers could develop scenarios to explore the possibilities of how interventions could be experienced [286].

Ethics of Data Collection For Privacy Interventions. Information displayed in privacy art is often (technically) public, and to our knowledge, no sampled artwork sells data to third parties. However, viewers may perceive it as private, particularly for social media data [85]. Harms like location leakage may exist, particularly for at-risk users [169]. Additionally, data deletion and security practices have yet to be standardized in interactive art [210, 246], leaving security vulnerabilities that researchers should consider and mitigate. Collaboration with communities can help identify suitable data collection methods [208]. When collecting user data is not appropriate, researchers could solicit data donations [105, 193, 240, 286] from informed participants; this has previously been used for sensitive topics, such as menstrual data [105] and sexual violence [286]. Zheng et al. provide a framework for ethical data donation [286]. To account for "different data donation journeys" [286], interfaces should facilitate choices about which data is shared [286].

Finally, depending on context (e.g., personally identifiable information, non-aggregated data, at-risk users), researchers should consider *stand-ins.* For example, artists visualize their *own* data in detailed, concrete ways to critique corporations and governments (Section 4.4). Specific personal stories may be uniquely persuasive [37]. In research settings, synthetic data [114] or personas [150, 224], in a similar format to user data, could demonstrate privacy violations without risking the violation of a specific user. Personas, already a tool to prompt reflection in HCI research [90], could likewise be synthetic subjects of privacy-art-inspired interventions.

7 Conclusion

We brought together an interdisciplinary team to perform a novel analysis of approaches to end-user provocation and reflection being used in privacy artworks. We constructed a database of 859 privacy artworks and qualitatively coded a sample of 73 works. We found that privacy artworks often highlighted government and corporate surveillance, resistance, and identity-surveillance dynamics, drawing on a shared visual language of familiar surveillance objects and domestic metaphors. Many works also grounded commentary in artists' personal data or lived experiences, as well as data collected from the public or artwork viewers. Artworks employed mechanisms like spotlighting, data aggregation, surveillance-system viewpoints, interactive experiences (sometimes with constrained user agency), and performative privacy invasions to convey privacy concepts. These mechanisms evoked affective responses via tones ranging from unsettling to playful, revealing opportunities for provocative privacy communication. Finally, we discussed how future privacy communications might adopt some of the techniques we observed to prompt privacy reflection.

Acknowledgments

We thank everyone who helped contribute to our database, especially students in *CMSC 23218/SAIC 5007: Surveillance Aesthetics* (Fall 2024) and Nick Briz. We would also like to thank our anonymous reviewers for their insightful feedback and suggestions. This material is based upon work supported by the National Science Foundation under Grants No. CNS-2047827 and CNS-2149680.

References

[1] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for privacy and security: understanding and assisting users' choices online. *Comput. Surveys* 50, 3 (2017). doi:10.1145/3054926

[2] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. 2020. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020). doi:10.1145/3415187

[3] Naseem Ahmadpour, Lian Loke, Carl Gray, Yidan Cao, Chloe Macdonald, and Rebecca Hart. 2023. Understanding how technology can support social-emotional learning of children: A dyadic trauma-informed participatory design with proxies. In *Proceedings of the 2023 SIGCHI Conference on Human Factors in Computing Systems*. doi:10.1145/3544548.3581032

[4] Salah Uddin Ahmed, Abdullah Al Mahmud, and Kristin Bergaust. 2009. Aesthetics in human-computer interaction: Views and reviews. In *International Conference on Human-Computer Interaction*. doi:10.1007/978-3-642-02574-7_63

[5] Weiwei Ai. 2010. Surveillance camera. https://www.phillips.com/detail/ai-weiwei/NY010620/46

[6] Amy Alexander. 2006/2007. SVEN. https://amy-alexander.com/live-performance/sven/

[7] Meriţ Algŭn Ringborg. 2012. Which no one will ever see. https://www.mericalgun.com/works.html#Which%20No%20One%20Will%20Ever%20See

[8] Refik Anadol. 2017. Convergence LA. https://refikanadol.com/works/convergence-la/

[9] Burak Arıkan. 2008. MyPocket. https://burak-arikan.com/mypocket/

[10] Jackie Armstrong. 2024. Content warnings in museums and galleries: Taking a proactive approach. https://www.aam-us.org/2024/07/26/content-warnings-in-museums-and-galleries-taking-a-proactive-approach/

[11] Simone Ashby, Julian Hanna, and Ricardo Rodrigues. 2017. Using BLE beacons to simulate proxemic surveillance for an interactive art installation. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. doi:10.1145/3027063.3053096

[12] James Auger. 2013. Speculative design: Crafting the speculation. *Digital Creativity* 24, 1 (2013), 11–35. doi:10.1080/14626268.2013.767276

[13] Larry Catá Backer. 2008. Global panopticism: States, corporations, and the governance effects of monitoring regimes. *Indiana Journal of Global Legal Studies* 15, 1 (2008), 101–148. doi:10.2979/gls.2008.15.1.101

[14] Jeffrey Bardzell. 2011. Interaction criticism: An introduction to the practice. *Interacting with Computers* 23, 6 (2011), 604–621. doi:10.1016/j.intcom.2011.07.001

[15] Jeffrey Bardzell and Shaowen Bardzell. 2013. What is "critical" about critical design?. In *Proceedings of the 2013 SIGCHI Conference on Human Factors in Computing Systems*. doi:10.1145/2470654.2466451

[16] Jeffrey Bardzell, Shaowen Bardzell, Carl DiSalvo, William Gaver, and Phoebe Sengers. 2012. The humanities and/in HCI. In *Proceedings of the 2012 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. doi:10.1145/2212776.2212405

[17] Shaowen Bardzell, Jeffrey Bardzell, Jodi Forlizzi, John Zimmerman, and John Antanitis. 2012. Critical design and critical theory: The challenge of designing for provocation. In *Proceedings of the 2012 Designing Interactive Systems Conference*. doi:10.1145/2317956.2318001

[18] Katherine Barnard-Wills and David Barnard-Wills. 2012. Invisible surveillance in visual art. *Surveillance & Society* 10 (2012), 204–214. doi:10.24908/ss.v10i3/4.4328

[19] Tim Barringer and Tom Flynn. 2012. *Colonialism and the object: Empire, material culture and the museum.* Routledge.

[20] Susanne Barth, Dan Ionita, and Pieter Hartel. 2022. Understanding online privacy—A systematic review of privacy visualizations and privacy by design guidelines. *Comput. Surveys* 55, 3 (2022). doi:10.1145/3502288

[21] Aram Bartholl. 2024. Choir of missed connections. https://arambartholl.com/choir-of-missed-connections/

[22] Steve Benford, Chris Greenhalgh, Gabriella Giannachi, Brendan Walker, Joe Marshall, and Tom Rodden. 2012. Uncomfortable interactions. In *Proceedings of the 2012 SIGCHI Conference on Human Factors in Computing Systems*. doi:10.1145/2207676.2208347

[23] Walter Benjamin. 1969. The work of art in the age of mechanical reproduction. In *Illuminations*, Hannah Arendt (Ed.). Schocken Books, New York. (Original work published 1935), translated by Harry Zohn.

[24] Dennis Benner, Sofia Schöbel, Andreas Janson, and Jan Marco Leimeister. 2022. How to achieve ethical persuasive design: A review and theoretical propositions for information systems. *AIS Transactions on Human-Computer Interaction* 14, 4 (2022). doi:10.17705/1thci.00179

[25] Jeremy Bentham. 1791. *Panopticon or the inspection house.* T. Payne.

[26] Jenny Berkholz, Aniqa Rahman, and Gunnar Stevens. 2025. Playing with privacy: Exploring the social construction of privacy norms through a card game. *Proceedings of the ACM on Human-Computer Interaction* 9, 1 (2025). doi:10.1145/3701202

[27] Charles Bernheimer. 1987. Degas's brothels: Voyeurism and ideology. *Representations, Special Issue: Misogyny, Misandry, and Misanthropy* 20 (1987), 158–186. doi:10.2307/2928506

[28] Ann-Christin Bertrand and James Bridle. 2016. *WATCHED! Surveillance, art and photography.* Verlag der Buchhandlung Walther König.

[29] Rasika Bhalerao, Vaughn Hamilton, Allison McDonald, Elissa M. Redmiles, and Angelika Strohmayer. 2022. Ethical practices for security research with at-risk populations. In *2022 IEEE European Symposium on Security and Privacy Workshops*. doi:10.1109/EuroSPW55150.2022.00065

[30] Viktoria Binschtok. 2009. Suspicious minds. https://viktoriabinschtok.wordpress.com/work-3/suspicious-minds/

[31] Justin Blinder. 2013. Dark side of the prism. https://justin.work/dark-side-of-the-prism/

[32] Mark Blythe. 2014. Research through design fiction: Narrative in real and imaginary abstracts. In *Proceedings of the 2014 SIGCHI Conference on Human Factors in Computing Systems*. doi:10.1145/2556288.2557098

[33] Mark Blythe, Kristina Andersen, Rachel Clarke, and Peter Wright. 2016. Anti-solutionist strategies: Seriously silly design fiction. In *Proceedings of the 2016 SIGCHI Conference on Human Factors in Computing Systems*. doi:10.1145/2858036.2858482

[34] Mark Blythe, Enrique Encinas, Jofish Kaye, Miriam Lueck Avery, Rob McCabe, and Kristina Andersen. 2018. Imaginary design workbooks: Constructive criticism and practical provocation. In *Proceedings of the 2018 SIGCHI Conference on Human Factors in Computing Systems*. doi:10.1145/3173574.3173807

[35] Natalie Bobrowska. 2024. Art Institute of Chicago: Visitors' privacy. *World Libraries* 28, 1 (2024). https://worldlibraries.dom.edu/index.php/worldlib/article/view/605/696

[36] Assia Boundaoui. 2018. The feeling of being watched. https://www.feelingofbeingwatched.com/

[37] Julia Braverman. 2008. Testimonials versus informational persuasive messages: The moderating effect of delivery mode and personal involvement. *Communication research* 35, 5 (2008), 666–694. doi:10.1177/0093650208321785

[38] James Bridle. 2017. Every CCTV camera (CC). https://jamesbridle.com/works/every-cctv-camera-cc

[39] Pam Briggs and Lisa Thomas. 2015. An inclusive, value sensitive design perspective on future identity technologies. *ACM Transactions on Computer-Human Interaction* 22, 5 (Aug. 2015). doi:10.1145/2778972

[40] Andrea Mubi Brighenti. 2010. Artveillance: At the crossroad of art and surveillance. *Surveillance & Society* 7, 2 (2010), 137–148. doi:10.24908/ss.v7i2.4142

[41] Jeffery Brown. 2018. In a world full of surveillance, artist Trevor Paglen stares back. https://www.pbs.org/newshour/show/in-a-world-full-of-surveillance-artist-trevor-paglen-stares-back

[42] Kathryn Brown. 2010. The aesthetics of presence: Looking at Degas's bathers. *The Journal of Aesthetics and Art Criticism* 68 (2010), 331–341. Issue 4. doi:10.1111/j.1540-6245.2010.01428.x

[43] Simone Browne. 2015. *Dark matters: On the surveillance of Blackness.* Duke University Press.

[44] Jonah Brucker-Cohen. 2022. Human error: Demand ware (2022). https://www.coin-operated.com/2022/07/27/human-error-demand-ware-2022/

[45] Jason Bruges. 2012. Platform 5. https://www.jasonbruges.com/platform-5

[46] Heath Bunting. c. 2012. The status project. https://irational.org/cgi-bin/cv2/temp.pl

[47] Allison Burtch. 2017. Mic jammer. https://github.com/allisonburtch/micjammer

[48] Susan Cahill, Morgan Campbell, and Stéphanie McKnight. 2025. Art and surveillance project. Website. http://www.artandsurveillance.com/

[49] Daniel Canogar. 2014. CMYK. https://www.danielcanogar.com/work/cmyk

[50] Jiashuo Cao, Samantha W. T. Chan, Dawn L. Garbett, Paul Denny, Alaeddin Nassani, Philipp M. Scholl, and Suranga Nanayakkara. 2021. Sensor-based interactive worksheets to support guided scientific inquiry. In *Proceedings of the 20th Annual ACM Interaction Design and Children Conference.* doi:10.1145/3459990.3460716

[51] Dashiel Carrera, Gitanjali Bhattacharjee, and Robert Soden. 2023. "We're not decorators": Fostering interdisciplinary exchange in STEM–artist collaborations. In *Proceedings of the 2023 Designing Interactive Systems Conference.* doi:10.1145/3563657.3595973

[52] Mary Cassatt. 1891. The bath.

[53] Ann Cavoukian. 2012. Privacy by design and user interfaces. https://gpsbydesigncentre.com/wp-content/uploads/2021/09/pbd-user-interfaces_Yahoo.pdf

[54] Claudio Celis. 2020. Critical surveillance art in the age of machine vision and algorithmic governmentality: Three case studies. *Surveillance & Society* 18, 3 (2020), 295–311. doi:10.24908/ss.v18i3.13410

[55] Janet X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A. Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-informed computing: Towards safer technology experiences for all. In *Proceedings of the 2022 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3491102.3517475

[56] Joana Chicau, Sarah Fdili Alaoui, Anne Lee Steele, Hazel Ryan, Yadira Sánchez, Romayne Gadelrab, Caroline Sinders, Mukul Patel, Gavin Starks, John Fass, and Rebecca Fiebrink. 2025. Designing counter-choreographies: embodied choreographic approaches for critical examination of online tracking. In *Proceedings of the 2025 Conference on Creativity and Cognition.* doi:10.1145/3698061.3726928

[57] Shruthi Sai Chivukula, Colin M. Gray, and Jason A. Brier. 2019. Analyzing value discovery in design decisions through ethicography. In *Proceedings of the 2019 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3290605.3300307

[58] C/O Berlin. 2017. Watched! Surveillance, art & photography. https://co-berlin.org/en/program/exhibitions/watched-surveillance-art-photography

[59] Beatriz da Costa. 2006-2008. Pigeonblog. https://nideffer.net/shaniweb/pigeonblog.php

[60] National Research Council. 2003. *Beyond productivity: Information technology, innovation, and creativity.* The National Academies Press. 96–115 pages. doi:10.17226/10671

[61] James Coupe. 2015. Sanctum. http://jamescoupe.com/?p=1740

[62] Lorrie Cranor. 2013. Security blanket. https://lorrie.cranor.org/blog/2013/08/12/security-blanket/

[63] Lorrie Faith Cranor, Praveen Guduru, and Manjula Arjula. 2006. User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction* 13, 2 (2006), 135–178. doi:10.1145/1165734.1165735

[64] Google Arts & Culture. [n. d.]. Girl reading a letter by an open window. https://artsandculture.google.com/asset/girl-reading-a-letter-by-an-open-window/3wFQaidzxA5mqg?hl=en

[65] Jiamin Dai and Karyn Moffatt. 2021. Surfacing the voices of people with dementia: Strategies for effective inclusion of proxy stakeholders in qualitative research. In *Proceedings of the 2021 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3411764.3445756

[66] Fabio de Almeida and Sónia Rafael. 2025. Data sins: Exploring data colonialism through storytelling-based speculative design practices. In *Proceedings of the 2025 Conference on Creativity and Cognition.* doi:10.1145/3698061.3726961

[67] Sander de Jong and Dayana Spagnuelo. 2020. Iconified representations of privacy policies: A GDPR perspective. In *World Conference on Information Systems and Technologies.* doi:10.1007/978-3-030-45691-7_75

[68] Dries Depoorter. 2018-2024. Surveillance speaker. https://driesdepoorter.be/surveillancespeaker/

[69] Pieter M. A. Desmet, Rick Porcelijn, and M. B. van Dijk. 2007. Emotional design; application of a research-based design approach. *Knowledge, Technology & Policy* 20 (2007), 141–155. doi:10.1007/s12130-007-9018-4

[70] Rod Dickinson, Nathan Semertzidis, and Florian Floyd Mueller. 2022. Machine in the middle: Exploring dark patterns of emotional human-computer integration through media art. In *Proceedings of the 2022 CHI Conference Extended Abstracts on Human Factors in Computing Systems.* doi:10.1145/3491101.3503555

[71] Claire Dolin, Ben Weinshel, Shawn Shan, Chang Min Hahn, Euirim Choi, Michelle L. Mazurek, and Blase Ur. 2018. Unpacking perceptions of data-driven inferences underlying online targeting and personalization. In *Proceedings of the 2018 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3173574.3174067

[72] Mimi Ọnụọha. 2017. Classification.01. https://mimionuoha.com/classification01

[73] Bogomir Doringer. 2008. The hoodie. https://nieuweinstituut.nl/en/projects/the-hoodie/bogomir-doringer

[74] Emanuel Felipe Duarte, Luiz Ernesto Merkle, and M. Cecília C. Baranauskas. 2019. The interface between interactive art and human-computer interaction: Exploring dialogue genres and evaluative practices. *Journal on Interactive Systems* 10, 2 (2019), 20–34. doi:10.5753/jis.2019.551

[75] Kellie Dunn, Irina Shklovski, and Pernille Bjørn. 2024. What research through art can bring to CSCW: Exploring ambiguous futures of work. *i-com* 23, 1 (2024), 33–55. doi:10.1515/icom-2023-0038

[76] Anthony Dunne and Fiona Raby. 2013. *Speculative everything: Design, fiction, and social dreaming.* MIT press.

[77] Myk Eff. 2025. The top 10 works of surveillance art. Medium. https://medium.com/spy-novel-research/the-top-10-works-of-surveillance-art-15a39bcdb2ce

[78] Hasan Elahi. 2006. Citizen. https://elahi.wayne.edu/citizen.php

[79] Hasan Elahi. 2006. Recap: Hiding in plain sight by Hasan Elahi. https://www.objectifs.com.sg/recap-hasan-elahi/

[80] Hasan Elahi. 2011. FBI, here I am! https://www.ted.com/talks/hasan_elahi_fbi_here_i_am

[81] Chris Elsden, David Chatting, Michael Duggan, Andrew Carl Dwyer, and Pip Thornton. 2022. Zoom obscura: Counterfunctional design for video-conferencing. In *Proceedings of the 2022 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3491102.3501973

[82] Chris Elsden, David Chatting, Abigail C. Durrant, Andrew Garbett, Bettina Nissen, John Vines, and David S. Kirk. 2017. On speculative enactments. In *Proceedings of the 2017 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3025453.3025503

[83] David England, Celine Latulipe, Nick Bryan-Kinns, Ernest Edmonds, and Sean Clark. 2016. Art.CHI II: Digital art in a post-digital world. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems.* doi:10.1145/2851581.2856474

[84] Florian M. Farke, David G. Balash, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv. 2021. Are privacy dashboards good for end users? Evaluating user perceptions and reactions to Google's My Activity. In *Proceedings of the 30th USENIX Security Symposium.* https://www.usenix.org/conference/usenixsecurity21/presentation/farke

[85] Casey Fiesler and Nicholas Proferes. 2018. "Participant" perceptions of Twitter research ethics. *Social Media + Society* 4, 1 (2018). doi:10.1177/2056305118763366

[86] Simone Fischer-Hübner and Farzaneh Karegar. 2024. Overview of usable privacy research: Major themes and research directions. *The Curious Case of Usable Privacy: Challenges, Solutions, and Prospects* (2024), 43–102. doi:10.1007/978-3-031-54158-2_3

[87] B. J. Fogg. 1998. Persuasive computers: Perspectives and research directions. In *Proceedings of the 1998 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/274644.274677

[88] Sarah Fox, Noura Howell, Richmond Wong, and Franchesca Spektor. 2019. Vivewell: Speculating near-future menstrual tracking through current data practices. In *Proceedings of the 2019 Designing Interactive Systems Conference.* doi:10.1145/3322276.3323695

[89] Batya Friedman, Edward Felten, and Lynette I. Millett. 2000. Informed consent online: A conceptual model and design principles. *University of Washington Computer Science & Engineering Technical Report 00–12–2* 8 (2000).

[90] Batya Friedman, Peter H. Kahn Jr., Alan Borning, and Alina Huldtgren. 2013. Value sensitive design and information systems. (2013), 55–95. doi:10.1007/978-94-007-7844-3_4

[91] Batya Friedman, Peter H. Kahn Jr., Jennifer Hagman, Rachel L. Severson, and Brian Gill. 2006. The watcher and the watched: Social judgments about privacy in a public place. *Human–Computer Interaction* 21, 2 (2006), 235–272. doi:10.1207/s15327051hci2102_3

[92] Kelsey R. Fulton, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L. Mazurek. 2019. The effect of entertainment media on mental models of computer security. In *Proceedings of the 15th Symposium on Usable Privacy and Security.* doi:10.5555/3361476.3361483

[93] Anirudh Ganesh, Chinenye Ndulue, and Rita Orji. 2021. PERMARUN–A persuasive game to improve user awareness and self-efficacy towards secure smartphone behaviour. In *Proceedings of the 2021 CHI Conference Extended Abstracts on Human Factors in Computing Systems.* doi:10.1145/3411763.3451781

[94] Anirudh Ganesh, Chinenye Ndulue, and Rita Orji. 2022. Smartphone security and privacy–A gamified persuasive approach with protection motivation theory. In *International Conference on Persuasive Technology.* doi:10.1007/978-3-030-98438-0_7

[95] Anirudh Ganesh, Chinenye Ndulue, and Rita Orji. 2023. Tailoring a persuasive game to promote secure smartphone behaviour. In *Proceedings of the 2023 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3544548.3581038

[96] Zhimin Gao and Jiaxi Huang. 2022. Human-computer interaction emotional design and innovative cultural and creative product design. *Frontiers in Psychology* 13 (2022). doi:10.3389/fpsyg.2022.982303

[97] Paul Garrin. 1989. Yuppie ghetto with watchdog. https://zkm.de/en/artwork/yuppie-ghetto-with-watchdog

[98] Bill Gaver and Heather Martin. 2000. Alternatives: Exploring information appliances through conceptual design proposals. In *Proceedings of the 2000 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/332040.332433

[99] William Gaver. 2011. Making spaces: How design workbooks work. In *Proceedings of the 2011 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/1978942.1979169

[100] Jakub Geltner. 2015. Nest. http://www.geltner.cz/2009/nest-05/

[101] Mariam Ghani. 2005. Security blanket. https://www.mariamghani.com/work/195

[102] Ghostery. 2025. Free tracker & ad blocker extension. Version 4.4.25. https://www.ghostery.com/ghostery-ad-blocker

[103] Steve Giasson. 2015-2016. VOX. http://www.artandsurveillance.com/artists-artworks-exhibits/

[104] Kentaro Go and John M. Carroll. 2004. The blind men and the elephant: Views of scenario-based system design. *Interactions* 11, 6 (2004), 44–53. doi:10.1145/1029036.1029037

[105] Alejandra Gomez Ortega, Jacky Bourgeois, and Gerd Kortuem. 2022. Reconstructing intimate contexts through data donation: A case study in menstrual tracking technologies. In *Proceedings of the Nordic Human-Computer Interaction Conference.* doi:10.1145/3546155.3546646

[106] Kyriaki Goni. 2013, 2015, 2019. Deletion process. https://kyriakigoni.com/projects/deletion-process

[107] Kyriaki Goni. 2016. Deletion process_only you can see my history: Investigating digital privacy, digital oblivion, and control on personal data through an interactive art installation. In *ACM SIGGRAPH 2016 Art Gallery.* doi:10.1145/2897843.2915187

[108] Colin M. Gray, Cristiana Teixeira Santos, Nataliia Bielova, and Thomas Mildner. 2024. An ontology of dark patterns knowledge: Foundations, definitions, and a pathway for shared knowledge-building. In *Proceedings of the 2024 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3613904.3642436

[109] Ben Grosser. 2021. Go rando. https://bengrosser.com/projects/go-rando/

[110] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a low profile? Technology, risk and privacy among undocumented immigrants. In *Proceedings of the 2018 SIGCHI conference on human factors in computing systems.* doi:10.1145/3173574.3173688

[111] Mengyao Guo, Kexin Nie, Jinda Han, Guan Wang, Xin Wang, zhishun Chi, Jie Fu, and Ze Gao. 2025. Visual storytelling in HCI: A workshop on narrative development through sequential art. In *Proceedings of the 2025 Conference on Creativity and Cognition.* doi:10.1145/3698061.3728391

[112] Hana Habib, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Joel Reidenberg, Norman Sadeh, and Florian Schaub. 2021. Toggles, dollar signs, and triangles: How to (in)effectively convey privacy choices with icons and link texts. In *Proceedings of the 2021 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3411764.3445387

[113] Helen Halbert and Lisa P. Nathan. 2015. Designing for discomfort: Supporting critical reflection through interactive tools. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing.* doi:10.1145/2675133.2675162

[114] Perttu Hämäläinen, Mikke Tavast, and Anton Kunnari. 2023. Evaluating large language models in generating synthetic HCI research data: A case study. In *Proceedings of the 2023 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3544548.3580688

[115] Elizabeth Harney and Ruth B. Phillips. 2018. *Mapping modernisms: Art, indigeneity, colonialism.* Duke University Press.

[116] Hugh Hart. 2007. The art of surveillance. https://www.wired.com/2007/11/the-art-of-surveillance/

[117] Adam Harvey. 2017. Hyperface. https://adam.harvey.studio/hyperface/

[118] Drew Hemment, Morgan Currie, SJ Bennett, Jake Elwes, Anna Ridler, Caroline Sinders, Matjaz Vidmar, Robin Hill, and Holly Warner. 2023. AI in the public eye: Investigating public AI literacy through AI art. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency.* doi:10.1145/3593013.3594052

[119] Lefebvre Henri and Nicholson-Smith Donald. 1991. *The production of space.* Blackwell, Oxford.

[120] Dan Hett. 2018. Sorry to bother you. https://danhett.itch.io/sorry

[121] Kashmir Hill. 2022. This surveillance artist knows how you got that perfect Instagram photo. https://www.nytimes.com/2022/09/24/technology/surveillance-footage-instagram.html

[122] Leif-Erik Holtz, Katharina Nocun, and Marit Hansen. 2010. Towards displaying privacy information with icons. In *Privacy and Identity Management for Life.* Vol. 352. 338–348. doi:10.1007/978-3-642-20769-3_27

[123] Esther Hovers. 2021-2024. The right to be forgotten. https://estherhovers.com/works-main

[124] Hsin-Chien Huang. 2023. The eye and I. https://hsinchienhuang.com/pix/_3artworks/i_theEyeAndI/p0.php?lang=en

[125] Larke N. Huang, Rebecca Flatow, Tenly Biggs, Sara Afayee, Kelley Smith, Thomas Clark, and Mary Blake. 2014. SAMHSA's concept of trauma and guidance for a trauma-informed approach. https://www.health.ny.gov/health_care/medicaid/program/medicaid_health_homes/docs/samhsa_trauma_concept_paper.pdf

[126] International Association of Privacy Professionals. 2025. Privacy art gallery. IAPP Resource Center. https://iapp.org/resources/privacy-art-gallery/

[127] Aki Ishida and Noritaka Minami. 2022. Obsolescent masculinity: Nakagin Capsule Tower demolition (Tokyo). https://disegnojournal.com/newsfeed/obsolescent-masculinity-nakagin-capsule-tower-demolition-tokyo

[128] Jane Jacobs. 1992. *Death and life of great American cities, 1961.* Knopf Doubleday Publishing Group.

[129] Mirabelle Jones, Christina Neumayer, and Irina Shklovski. 2023. Embodying the algorithm: Exploring relationships with large language models through artistic performance. In *Proceedings of the 2023 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3544548.3580885

[130] Patrick W. Jordan. 2000. *Designing pleasurable products: An introduction to the new human factors.* CRC press. doi:10.4324/9780203305683

[131] Frederike Jung, Jonah-Noël Kaiser, Kai Von Holdt, Wilko Heuten, and Jochen Meyer. 2023. The art of privacy – A theatrical privacy installation in virtual reality. In *Proceedings of the 2023 CHI Conference Extended Abstracts on Human Factors in Computing Systems.* doi:10.1145/3544549.3583893

[132] Gary Kafer. 2016. Reimagining resistance: Performing transparency and anonymity in surveillance art. *Surveillance & Society* 14, 2 (2016), 227–239. doi:10.24908/ss.v14i2.6005

[133] KairUs. 2018. Found footage stalkers. https://kairus.org/portfolio/forensic-fantasies-trilogy/

[134] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security.* doi:10.1145/1572532.1572538

[135] Dave Kemp. 2010. Data collection. https://davekemp.ca/projects/data-collection/

[136] Ars Electronica Linz GmbH & Co KG. [n. d.]. *Archive - Prix.* https://archive.aec.at/prix/

[137] David Kirby. 2010. The future is now: Diegetic prototypes and the role of popular films in generating real-world technological development. *Social Studies of Science* 40, 1 (2010), 41–70. doi:10.1177/0306312709338325

[138] Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A. Martucci. 2020. Enhancing privacy through the visual design of privacy notices: Exploring the interplay of curiosity, control and affect. In *Proceedings of the 16th Symposium on Usable Privacy and Security.* doi:10.5555/3488905.3488928

[139] Cory Knobel and Geoffrey C. Bowker. 2011. Values in design. *Commun. ACM* 54, 7 (2011), 26–28. doi:10.1145/1965724.1965735

[140] Marion Koelle, Katrin Wolf, and Susanne Boll. 2018. Beyond LED status lights - Design requirements of privacy notices for body-worn cameras. In *Proceedings of the Twelfth International Conference on Tangible, Embedded, and Embodied Interaction.* doi:10.1145/3173225.3173234

[141] Egor Kraft. 2019. Twelve nodes. https://kraft.studio/twelve-nodes/

[142] Kisho Kurokawa. 1972. Nakagin Capsule Tower.

[143] Markus Langer and Cornelius J. König. 2018. Introducing and testing the creepiness of situation scale (CRoSS). *Frontiers in Psychology* 9 (2018). doi:10.3389/fpsyg.2018.02220

[144] Fabiola Larios. 2024. Surveillance cutie. https://fabiola.io/portfolio/works/surveillance_cutie.html

[145] Sam Lavigne. 2015. 3 degrees of separation from the military-industrial-prison-data-surveillance state. https://lav.io/projects/3-degrees-of-separation/

[146] Francine Leclercq. 2024. Embroidered surveillance. https://www.designboom.com/art/hand-embroidered-artworks-francine-leclercq-surveillance-cameras-footage-03-20-2024/

[147] Kiljae Lee, Jungsil Choi, George M. Marakas, and Surendra N. Singh. 2019. Two distinct routes for inducing emotions in HCI design. *International Journal of Human-Computer Studies* 124 (2019), 67–80. doi:10.1016/j.ijhcs.2018.11.012

[148] Makayla Lewis and Lizzie Coles-Kemp. 2014. A tactile visual library to support user experience storytelling. *Proceedings of NordDesign 2014* (2014). https://www.designsociety.org/publication/36283/a_tactile_visual_library_to_support_user_experience_storytelling

[149] Makayla Lewis, Miriam Sturdee, Denise Lengyel, Mauro Toselli, John Miers, Violet Owen, Josh Urban Davis, Swen E. Gaudl, Lanxi Xiao, Ernesto Priego, Kim Snooks, Laia Turmo Vidal, Eli Blevis, Nicola Privato, Patricia Piedade, Corey Ford, Nick Bryan-Kinns, Beatriz Severes, Kirsikka Kaipainen, Caroline Claisse, Raksanda Mehnaz Huq, Mirjam Palosaari Eladhari, Anna Troisi, Ana O. Henriques, Ar Grek, Gareth Mcmurchy, Ray Lc, Sara Nabil, Jacinta Jardine, Robert Collins, Andrey Vlasov, Yana Knight, Michele Cremaschi, Silvia Carderelli-Gronau, Claudia Núñez Pacheco, Gisela Reyes-Cruz, and Jean-Philippe Riviere. 2024. Traveling arts x HCI sketchbook: Exploring the intersection between artistic expression and human-computer interaction. In *Proceedings of the 2024 CHI Conference Extended Abstracts on Human Factors in Computing Systems.* doi:10.1145/3613905.3644069

[150] Makayla M. Lewis and Lizzie Coles-Kemp. 2014. Who says personas can't dance? The use of comic strips to design information security personas. In *Proceedings of the 2014 CHI Conference Extended Abstracts on Human Factors in Computing Systems.* doi:10.1145/2559206.2581323

[151] Smithsonian Libraries and Archives. [n. d.]. *Art and artist files.* https://library.si.edu/art-and-artist-files

[152] Kathryn Lichlyter, Urvashi Kishnani, Kate Hollenbach, and Sanchari Das. 2024. Understanding professional needs to create privacy-preserving and secure emergent digital artworks. arXiv:2407.05450

[153] Junsu Lim, Hyeonggeun Yun, Auejin Ham, and Sunjun Kim. 2022. Mine yourself!: A role-playing privacy tutorial in virtual reality environment. In *Proceedings of the 2022 CHI Conference Extended Abstracts on Human Factors in Computing Systems.* doi:10.1145/3491101.3519773

[154] Joseph Lindley and Paul Coulton. 2015. Back to the future: 10 years of design fiction. In *Proceedings of the 2015 British HCI Conference.* doi:10.1145/2783446.2783592

[155] Joseph Lindley and Paul Coulton. 2016. Pushing the limits of design fiction: The case for fictional research papers. In *Proceedings of the 2016 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/2858036.2858446

[156] Machine Listening. 2018. Always learning. https://machinelistening.exposed/site-map/works/always-learning

[157] Melanie Lowe. 2008. You saw me? http://www.artandsurveillance.com/artists-artworks-exhibits/

[158] Alex Jiahong Lu. 2022. Toward everyday negotiation and resistance under data-driven surveillance. *Interactions* 29, 2 (2022). doi:10.1145/3516427

[159] Louis Lumière. 1895. Workers leaving the Lumière Factory.

[160] He-Lin Luo. 2019. If this is a global surveillance center. https://www.digiarts.org.tw/DigiArts/DataBasePage/1_147254841059061/En

[161] Nic Lupfer, Bill Hamilton, Andrew Webb, Rhema Linder, Ernest Edmonds, and Andruid Kerne. 2015. The Art.CHI gallery: An embodied iterative curation experience. In *Proceedings of the 2015 CHI Conference Extended Abstracts on Human Factors in Computing Systems.* doi:10.1145/2702613.2725457

[162] Kristine Madjare and rixcriga. 2016. [RIXC Gallery] Trihars exhibition "RAM" opening. https://www.flickr.com/photos/rixcriga/albums/72157669540894514/with/29083597595

[163] Jill Magid. 2002. System Azure security ornamentation. https://www.jillmagid.com/projects/system-azure-security-ornamentation

[164] Emanuel Maiberg. 2025. 'FuckLAPD.com' lets anyone use facial recognition to instantly identify cops. https://www.404media.co/fucklapd-com-lets-anyone-use-facial-recognition-to-instantly-identify-cops/

[165] Steve Mann. 2001. EXISTech Corp. http://wearcam.org/domewear/

[166] Steve Mann. 2004. "Sousveillance": Inverse surveillance in multimedia imaging. In *Proceedings of the 12th Annual ACM International Conference on Multimedia.* doi:10.1145/1027527.1027673

[167] Ivan Manokha. 2018. Surveillance, panopticism, and self-discipline in the digital age. *Surveillance & Society* 16, 2 (2018), 219–237. doi:10.24908/ss.v16i2.8346

[168] Eva Mattes and Franco Mattes. 2019. My little big data. https://0100101110101101.org/my-little-big-data/

[169] Tara Matthews, Elie Bursztein, Patrick Gage Kelley, Lea Kissner, Andreas Kramm, Andrew Oplinger, Andreas Schou, Manya Sleeper, Stephan Somogyi, Dalila Szostak, Kurt Thomas, Anna Turner, Jill Palzkill Woelfer, Lawrence L. You, Izzie Zahorian, and Sunny Consolvo. 2025. Supporting the digital safety of at-risk users: Lessons learned from 9+ years of research and training. *ACM Transactions on Computer-Human Interaction* 32, 3 (June 2025). doi:10.1145/3716382

[170] Lauren Lee McCarthy. 2017. MWITM. https://get-lauren.net/MWITM-Man-Woman-In-The-Middle

[171] Aleecia M. McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* 4 (2008).

[172] Aleecia M. McDonald, Robert W. Reeder, Patrick Gage Kelley, and Lorrie Faith Cranor. 2009. A comparative study of online privacy policies and formats. In *Proceedings of the 5th Symposium on Usable Privacy and Security.* doi:10.1145/1572532.157258

[173] Kyle McDonald. 2018, 2025. ICESPY. https://icespy.org/

[174] Carolyn McKay. 2013. Covert: The artist as voyeur. *Surveillance & Society* 3 (2013), 334–353. doi:10.24908/ss.v11i3.4504

[175] Shaun McNiff. 1998. *Art-based research.* Jessica Kingsley Publishers.

[176] Vice Media. [n. d.]. Surveillance art. https://www.vice.com/en/tag/surveillance-art/

[177] Jessica Megarry, Peta Mitchell, Markus Rittenbruch, Yu Kao, Bryce Christensen, and Marcus Foth. 2023. Probing for privacy: A digital design method to support reflection of situated geoprivacy and trust. *Digital Society* 2, 3 (2023). doi:10.1007/s44206-023-00083-x

[178] Vikram Mehta, Daniel Gooch, Arosha Bandara, Blaine Price, and Bashar Nuseibeh. 2021. Privacy care: A tangible interaction framework for privacy management. *ACM Transactions on Internet Technology* 21, 1 (2021). doi:10.1145/3430506

[179] Melissa Miles. 2015. Photography, privacy and the public. *Law, Culture and the Humanities* 11, 2 (2015), 270–293. doi:10.1177/1743872111430277

[180] Joana Moll. 2022. Carbolytics. https://www.janavirgin.com/carbolytics.html

[181] Torin Monahan. 2015. The right to hide? Anti-surveillance camouflage and the aestheticization of resistance. *Communication and Critical/Cultural Studies* 12, 2 (2015), 159–178. doi:10.1080/14791420.2015.1006646

[182] Torin Monahan. 2018. Ways of being seen: Surveillance art and the interpellation of viewing subjects. *Cultural Studies* 32, 4 (2018), 560–581. doi:10.1080/09502386.2017.1374424

[183] Vivian Genaro Motti and Kelly Caine. 2016. Towards a visual vocabulary for privacy concepts. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 60. 1078–1082. doi:10.1177/1541931213601249

[184] MSCHF. 2022. Eavesdropper 1. https://leaflet.perrotin.com/view/338/no-more-tears-im-lovin-it

[185] Maria Murray, Nadia Pantidi, and John McCarthy. 2023. Agency, power and confrontation: The role for socially engaged art in CSCW with rurban communities in support of inclusion. *Computer Supported Cooperative Work* 33, 3 (2023), 435–472. doi:10.1007/s10606-023-09482-7

[186] mwvisser. [n. d.]. Peepshow - Art & Electronic Media Online Companion. https://artelectronicmedia.com/en/artwork/peepshow/

[187] Bruce Nauman. 1967, 1968. Live-taped video corridor. https://www.guggenheim.org/artwork/3153

[188] Ana Ndumu, Diana E. Marsh, Victoria Van Hyning, and Sydney Triola. 2022. Panopticism and complicity: The state of surveillance and everyday oppression in libraries, archives, and museums. *Journal of Critical Library and Information Studies* 4, 1 (2022). doi:10.24242/jclis.v4i1.166

[189] Don Norman. 2007. *Emotional design: Why we love (or hate) everyday things.* Basic books.

[190] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. 2018. Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration. *Proceedings on Privacy Enhancing Technologies* (2018). Issue 4. doi:10.1515/popets-2018-0029

[191] Museum of Modern Art. [n. d.]. *MoMA archives, library, and research collections.* https://research.moma.org/home

[192] ACLU of the District of Columbia. 2025. If stopped for photographing in public. https://www.acludc.org/know-your-rights/if-stopped-photographing-public/

[193] Jakob Ohme, Theo Araujo, Claes H. de Vreese, and Jessica Taylor Piotrowski. 2021. Mobile data donations: Assessing self-report accuracy and sample biases with the iOS Screen Time function. *Mobile Media & Communication* 9, 2 (2021), 293–313. doi:10.1177/2050157920959106

[194] Julian Oliver. 2015. Stealth cell tower. https://julianoliver.com/projects/stealth-cell-tower/

[195] Opera on Tap. [n. d.]. *Looking at you: A new techno-noir opera.* https://operaontap.org/looking-at-you/

[196] George Orwell. 2008. *1984* (reprint ed.). Signet Classics. (Original work published 1949).

[197] Trevor Paglen. 2006. Black sites. https://paglen.studio/2020/04/24/black-sites/

[198] Trevor Paglen. 2018. Image operations. https://paglen.studio/2020/04/23/image-operations/

[199] Nam June Paik. 1984. Good Morning Mr. Orwell. https://www.eai.org/titles/good-morning-mr-orwell

[200] Andrew S. Patrick and Steve Kenny. 2003. From privacy legislation to interface design: Implementing information privacy in human-computer interactions. In *International Workshop on Privacy Enhancing Technologies.* doi:10.1007/978-3-540-40956-4_8

[201] Yuri Pattison. 2017. Yuri Pattison at Kunst Halle Sankt Gallen. https://artviewer.org/yuri-pattison-at-kunst-halle-sankt-gallen/

[202] Rich Pell and The Institute for Applied Autonomy. 2009. iSee - The Institute for Applied Autonomy (2004). https://vimeo.com/6163268

[203] Chanda Phelan, Cliff Lampe, and Paul Resnick. 2016. It's creepy, but it doesn't bother me. In *Proceedings of the 2016 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/2858036.2858381

[204] James Pierce. 2014. On the presentation and production of design research artifacts in HCI. In *Proceedings of the 2014 Designing Interactive Systems Conference.* doi:10.1145/2598510.2598525

[205] James Pierce. 2019. Smart home security cameras and shifting lines of creepiness: A design-led inquiry. In *Proceedings of the 2019 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3290605.3300275

[206] James Pierce. 2020. Roomba+Clips Cam: Exploring unpredictable autonomy in everyday smart systems. In *Companion Publication of the 2020 Designing Interactive Systems Conference.* doi:10.1145/3393914.3395816

[207] James Pierce, Richmond Y. Wong, and Nick Merrill. 2020. Sensor illumination: Exploring design qualities and ethical implications of smart cameras and image/video analytics. In *Proceedings of the 2020 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3313831.3376347

[208] Ethan Plaut, Kiri West, Fabio Morreale, Maya Gibson, Grace Thompson, Kara Woodward, and Danielle Lottridge. 2025. Surveillance on exhibit: Using problematic technology to teach about problematic technology. In *Proceedings of the 2025 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3706598.3713710

[209] Surveillance Camera Players. 1999, 2000. The mass psychology of fascism. https://notbored.org/reich.html

[210] Barbara Pollack. 2014. When does surveillance art cross the line? https://www.artnews.com/art-news/news/privacy-and-surveillance-art-2628/

[211] Craig Proulx. 2014. Colonizing surveillance: Canada constructs an Indigenous terror threat. *Anthropologica* 56 (2014), 83–100. Issue 1. https://www.jstor.org/

stable/24469643

[212] Argenis Ramirez Gomez, Carolina Fuentes Toro, Samuelson Atiba, Nervo Verdezoto Dias, and Katarzyna Stawarz. 2025. Understanding #creepytech: Exploring the context of creepiness of emerging technology. In *Proceedings of 38th International BCS Human-Computer Interaction Conference.* doi:10.14236/ewic/BCSHCI2025.11

[213] Argenis Ramirez Gomez and Katarzyna Stawarz. 2025. Exploring creepy futures: Reflecting on the value of creepiness as design fiction. In *Proceedings of 38th International BCS Human-Computer Interaction Conference.* doi:10.14236/ewic/BCSHCI2025.25

[214] Joel R. Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T. Graves, Fei Liu, Aleecia McDonald, Thomas B. Norton, Rohan Ramanath, N. Cameron Russell, Norman Sadeh, and Florian Schaub. 2015. Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Technology Law Journal* 30 (2015). doi:10.2139/ssrn.2418297

[215] Daniel Reinhardt, Johannes Borchard, and Jörn Hurtienne. 2021. Visual interactive privacy policy: The better choice?. In *Proceedings of the 2021 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3411764.3445465

[216] Nathan Reitinger, Bruce Wen, Michelle L. Mazurek, and Blase Ur. 2023. Analysis of Google ads settings over time: Updated, individualized, accurate, and filtered. In *Proceedings of the 22nd Workshop on Privacy in the Electronic Society.* doi:10.1145/3603216.3624968

[217] Nathan Reitinger, Bruce Wen, Michelle L. Mazurek, and Blase Ur. 2024. What does it mean to be creepy? Responses to visualizations of personal browsing activity, online tracking, and targeted ads. In *Proceedings on Privacy Enhancing Technologies.* doi:10.56553/popets-2024-0101

[218] Peters Riekstins. 2016. Back to the Light. https://we-make-money-not-art.com/back-to-the-light/

[219] Daniel Romm, Hongyu Zhang, Priyanka Verma, Grant McKenzie, and Emily Chen. 2021. "Data horror": Mapping (spatial) data privacy violations onto a cognitive account of horror. In *Proceedings of the Spatial Data Science Symposium 2021 Short Paper Proceedings.* doi:10.25436/E23S3T

[220] Arianna Rossi and Monica Palmirani. 2017. A visualization approach for adaptive consent in the European data protection framework. In *Proceedings of the 2017 Conference for E-Democracy and Open Government.* doi:10.1109/CeDEM.2017.23

[221] Manuel Rudolph, Denis Feth, and Svenja Polst. 2018. Why users ignore privacy policies–A survey and intention model for explaining user privacy behavior. In *International Conference on Human-Computer Interaction.* doi:10.1007/978-3-319-91238-7_45

[222] Alaa Sadik. 2008. Digital storytelling: A meaningful technology-integrated approach for engaged student learning. *Educational technology research and development* 56, 4 (2008), 487–506. doi:10.1007/s11423-008-9091-8

[223] Johnny Saldaña. 2021. *The coding manual for qualitative researchers.* SAGE publications Ltd. 1–440 pages.

[224] Joni Salminen, Kathleen Wenyun Guan, Soon-Gyo Jung, and Bernard Jansen. 2022. Use cases for design personas: A systematic review and new frontiers. In *Proceedings of the 2022 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3491102.3517589

[225] Anup Sathya and Ken Nakagaki. 2024. Attention receipts: Utilizing the materiality of receipts to improve screen-time reflection on YouTube. In *Proceedings of the 2024 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3613904.3642505

[226] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In *Proceedings of the 11th Symposium on Usable Privacy and Security.* doi:10.5555/3235866.3235868

[227] Julia Scher. 2003. Papa bed. https://www.estherschipper.com/artists/51-julia-scher/works/1292-julia-scher-papa-bed-2003/

[228] Roman Schlegel, Apu Kapadia, and Adam J. Lee. 2011. Eyeing your exposure: Quantifying and controlling information sharing for improved privacy. In *Proceedings of the 7th Symposium on Usable Privacy and Security.* doi:10.1145/2078827.2078846

[229] Angela Schöpke-Gonzalez, Kellie Dunn, Shaowen Bardzell, Makayla Lewis, Maria Murray, and Catherine Wieczorek. 2025. Computing and the arts: Establishing theoretical and methodological foundations for cross-disciplinary collaboration. In *Companion Publication of the 2025 Conference on Computer-Supported Cooperative Work and Social Computing.* doi:10.1145/3715070.3748283

[230] Björn Schülke. 2005. Drone #4. http://www.schuelke.org/drone-4.html

[231] Carol F. Scott, Gabriela Marcu, Riana Elyse Anderson, Mark W. Newman, and Sarita Schoenebeck. 2023. Trauma-informed social media: Towards solutions for reducing and healing online harm. In *Proceedings of the 2023 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3544548.3581512

[232] Saher Selod. 2018. *Forever suspect: Racialized surveillance of Muslim Americans in the war on terror.* Rutgers University Press.

[233] Vandit Sharma and Mainack Mondal. 2022. Understanding and improving usability of data dashboards for simplified privacy control of voice assistant data. In *Proceedings of the 31st USENIX Security Symposium.* https://www.usenix.org/conference/usenixsecurity22/presentation/sharma-vandit

[234] Mehdi Sheikhi Nashalji and Fatemeh Mehdizadeh Saradj. 2025. Measuring visual privacy: A systematic review of evaluation methods, conceptual definitions, and design strategies. *Buildings* 15, 10 (2025). doi:10.3390/buildings15101606

[235] Mark Shepard. 2012. Minor urbanism. https://www.andinc.org/site/minor-urbanism/

[236] Katie Shilton. 2013. Values levers: Building ethics into design. *Science, Technology, & Human Values* 38, 3 (2013), 374–397. doi:10.1177/0162243912436985

[237] Irina Shklovski and Erik Grönvall. 2020. CreepyLeaks: Participatory speculation through demos. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction.* doi:10.1145/3419249.3420168

[238] Ann-Sofi Sidén. 2014. Sticky floors. https://www.annsofisiden.com/index.html#detail-sticky

[239] SIGCHI. 2025. SIGCHI policies. Version 4.4.25. https://programs.sigchi.org/policies#sigchi-acm-privacy-policy

[240] Anya Skatova and James Goulding. 2019. Psychology of personal data donation. *PloS one* 14, 11 (2019). doi:10.1371/journal.pone.0224240

[241] Michael Skirpan, Maggie Oates, Daragh Byrne, Robert Cunningham, and Lorrie Faith Cranor. 2022. Is a privacy crisis experienced, a privacy crisis avoided? *Commun. ACM* 65 (2022), 26–29. Issue 3. doi:10.1145/3512325

[242] Michael Warren Skirpan, Jacqueline Cameron, and Tom Yeh. 2018. More than a show: Using personalized immersive theater to educate and engage the public in technology ethics. In *Proceedings of the 2018 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3173574.3174038

[243] Garrett Smith, Sarah Carson, Rhea G. Vengurlekar, Stephanie Morales, Yun-Chieh Tsai, Rachel George, Josh Bedwell, Trevor Jones, Mainack Mondal, Brian Smith, Norman Makoto Su, Bart Knijnenburg, and Xinru Page. 2024. "I know I'm being observed:" Video interventions to educate users about targeted advertising on Facebook. In *Proceedings of the 2024 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3613904.3642885

[244] Marie Louise Juul Søndergaard and Lone Koefoed Hansen. 2018. Intimate futures: Staying with the trouble of digital personal assistants through design fiction. In *Proceedings of the 2018 Designing Interactive Systems Conference.* doi:10.1145/3196709.3196766

[245] Stanza. 2023. The nemesis machine: Manifestation. https://www.stanza.co.uk/Nemesis_Manifestation/index.html

[246] Luke Stark and Kate Crawford. 2019. The work of art in the age of artificial intelligence: What artists can teach us about the ethics of data practice. *Surveillance & Society* 17, 3/4 (2019), 442–455. doi:10.24908/ss.v17i3/4.10821

[247] Dan Stavy. 2017. Selfie stick. https://stavdan.com/selfie-stick/

[248] Katarzyna Stawarz, Alison Burrows, and Argenis Ramirez Gomez. 2025. Leveraging creepiness to facilitate ethical design: Lessons learned from a design workshop. In *38th International BCS Human-Computer Interaction Conference.* doi:10.14236/ewic/BCSHCI2025.49

[249] Bruce Sterling. 2005. *Shaping things.* MIT Press.

[250] Hito Steyerl. 2013. How not to be seen: A fucking didactic educational .MOV file. https://www.moma.org/collection/works/181784?artist_id=43752&page=1&sov_referrer=artist

[251] Miriam Sturdee, Paul Coulton, Joseph G. Lindley, Mike Stead, Haider Ali, and Andy Hudson-Smith. 2016. Design fiction: How to build a Voight-Kampff machine. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems.* doi:10.1145/2851581.2892574

[252] Miriam Sturdee, Makayla Lewis, Mafalda Gamboa, Thuong Hoang, John Miers, Ilja Šmorgun, Pranjal Jain, Angelika Strohmayer, Sarah Fdili Alaoui, and Christina R. Wodtke. 2022. The state of the (CHI)Art. In *Proceedings of the 2022 CHI Conference Extended Abstracts on Human Factors in Computing Systems.* doi:10.1145/3491101.3503722

[253] Miriam Sturdee, Makayla Lewis, Angelika Strohmayer, Katta Spiel, Nantia Koulidou, Sarah Fdili Alaoui, and Josh Urban Davis. 2021. A plurality of practices: Artistic narratives in HCI research. In *Proceedings of the 2021 Conference on Creativity and Cognition.* doi:10.1145/3450741.3466771

[254] Arne Svenson. 2023. The neighbors. https://www.danzigergallery.com/exhibitions/arne-svenson-1

[255] Madiha Tabassum, Abdulmajeed Alqhatani, Marran Aldossari, and Heather Richter Lipford. 2018. Increasing user attention with a comic-based policy. In *Proceedings of the 2018 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3173574.3173774

[256] Theresa Jean Tanenbaum, Marcel Pufal, and Karen Tanenbaum. 2016. The limits of our imagination: Design fiction as a strategy for engaging with dystopian futures. In *Proceedings of the Second Workshop on Computing within Limits.* doi:10.1145/2926676.2926687

[257] Shaheer Tarar. 2023. LANDSAT.EARTH. https://shaheer.info/

[258] Omer Tene and Jules Polonetsky. 2013. A theory of creepy: Technology, privacy and shifting social norms. *Yale JL & Tech.* 16 (2013), 59.

[259] Marc Teyssier, Marion Koelle, Paul Strohmeier, Bruno Fruchard, and Jürgen Steimle. 2021. Eyecam: Revealing relations between humans and sensing devices through an anthropomorphic webcam. In *Proceedings of the 2021 SIGCHI Conference on Human Factors in Computing Systems.* doi:10.1145/3411764.3445491

[260] Lucy Thompson. 2017. Vermeer's curtain: Privacy, slut-shaming and surveillance in 'A Girl Reading a Letter'. *Surveillance & Society* 15, 2 (2017), 326. doi:10.24908/ss.v15i2.6100

[261] Nye Thompson. 2021. Uninvited. https://nyethompson.net/works/UNINVITED.html

[262] Timo Toots. 2017, 2023. Reality TV. https://www.timo.ee/reality-tv/

[263] Suzanne Treister. 2013. Camouflage. https://www.suzannetreister.net/Camouflage/Camouflage.html

[264] Ben Van den Berghe. 2022. Backspace. https://benvandenberghe.com/

[265] Danja Vasiliev. 2012. Netless. https://k0a1a.net/netless/netless-abstract.pdf

[266] Danja Vasiliev. 2012. Netless2. https://k0a1a.net/danja/netless2

[267] Johannes Vermeer. c. 1657—1659. A girl reading a letter by an open window.

[268] Ian Wagner. 2016. iSee. https://www.digiart21.org/art/isee

[269] R. L. Wakkary, W. T. Odom, Sabrina Hauser, Garnet Hertz, and Henry Lin. 2016. Material speculation: Actual artifacts for critical inquiry. In *5th Decennial Aarhus Conference on Critical Alternatives*. doi:10.7146/aahcc.v1i1.21299

[270] Giles Walker. 2022. Kinetic sculpture. https://www.gileswalker.org/kinetic-sculpture

[271] Zhixuan Wang. 2021. Watch me watching: Surveillance art and the politics of observation. *Aspectus* 3 (2021). doi:doi.org/10.15124/yao-kdgx-a713

[272] Ben Weinshel, Miranda Wei, Mainack Mondal, Euirim Choi, Shawn Shan, Claire Dolin, Michelle L. Mazurek, and Blase Ur. 2019. Oh, the places you've been! User reactions to longitudinal transparency about third-party web tracking and inferencing. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. doi:10.1145/3319535.3363200

[273] Wieden+Kennedy. 2019. Giles Walker brings PEEPSHOW to W+K London.

[274] Lauren Wissot. 2018. "Do not be daunted by the magnitude of the challenge in front of you": Assia Boundaoui on her surveillance doc, The feeling of being watched. https://filmmakermagazine.com/105231-do-not-be-daunted-by-the-magnitude-of-the-challenge-in-front-of-you-assia-boundaoui-on-her-surveillance-doc-the-feeling-of-being-watched/

[275] Richmond Y. Wong and Deirdre K. Mulligan. 2016. When a product is still fictional: Anticipating and speculating futures through concept videos. In *Proceedings of the 2016 Designing Interactive Systems Conference*. doi:10.1145/2901790.2901801

[276] Richmond Y. Wong and Deirdre K. Mulligan. 2019. Bringing design to the privacy table: Broadening "design" in "privacy by design" through the lens of HCI. In *Proceedings of the 2019 SIGCHI Conference on Human Factors in Computing Systems*. doi:10.1145/3290605.3300492

[277] Richmond Y. Wong, Deirdre K. Mulligan, Ellen Van Wyk, James Pierce, and John Chuang. 2017. Eliciting values reflections by engaging privacy futures using design workbooks. In *Proceedings of the ACM on Human-Computer Interaction*, Vol. 1. doi:10.1145/3134746

[278] Richmond Y. Wong, Jason Caleb Valdez, Ashten Alexander, Ariel Chiang, Olivia Quesada, and James Pierce. 2023. Broadening privacy and surveillance: Eliciting interconnected values with a scenarios workbook on smart home cameras. In *Proceedings of the 2023 Designing Interactive Systems Conference*. doi:10.1145/3563657.3596012

[279] Richmond Y. Wong, Ellen Van Wyk, and James Pierce. 2017. Real-fictional entanglements: Using science fiction and design fiction to interrogate sensing technologies. In *Proceedings of the 2017 Designing Interactive Systems Conference*. doi:10.1145/3064663.3064682

[280] Justin Wooley. 2025. Aesthetic disruptions: Critical surveillance art and the unsettling of surveillance. *Surveillance & Society* 23, 2 (2025), 218–229. doi:10.24908/ss.v23i2.17532

[281] Paweł W. Woźniak, Jakob Karolus, Florian Lang, Caroline Eckerth, Johannes Schöning, Yvonne Rogers, and Jasmin Niess. 2021. Creepy technology: What is it and how do you measure it?. In *Proceedings of the 2021 SIGCHI Conference on Human Factors in Computing Systems*. doi:10.1145/3411764.3445299

[282] WTTDOTM. 2024. Traffic cam photobooth. https://trafficcamphotobooth.com/

[283] Jens Wunderling. 2010. Audience. http://jenswunderling.com/works/audience/

[284] Susan Fillin Yeh. 1976. Mary Cassatt's images of women. *Art Journal* 35 (1976), 359–363. Issue 4. doi:10.2307/776228

[285] Leah Zhang-Kennedy and Sonia Chiasson. 2021. A systematic review of multimedia tools for cybersecurity awareness and education. *Comput. Surveys* 54, 1 (2021). doi:10.1145/3427920

[286] Wenqi Zheng, Emma Walquist, Isha Datey, Xiangyu Zhou, Kelly Berishaj, Melissa Mcdonald, Michele Parkhill, Dongxiao Zhu, and Douglas Zytko. 2024. "It's not what we were trying to get at, but I think maybe it should be": Learning how to do trauma-informed design with a data donation platform for online dating sexual violence. In *Proceedings of the 2024 SIGCHI Conference on Human Factors in Computing Systems*. doi:10.1145/3613904.3642045

[287] Catherine Zimmer. 2015. *Surveillance cinema*. New York University Press.

[288] John Zimmerman, Jodi Forlizzi, and Shelley Evenson. 2007. Research through design as a method for interaction design research in HCI. In *Proceedings of the 2007 SIGCHI Conference on Human Factors in Computing Systems*. doi:10.1145/1240624.1240704

[289] Verena Zimmermann, Adrienn Toth, Hannah Sievers, Linda Fanconi, Yanis Isenring, Mona Henz, Alina Stöver, and Nina Gerber. 2025. Let's get visual - Testing visual analogies and metaphors for conveying privacy policies and data handling information. In *2025 IEEE Symposium on Security and Privacy*. doi:10.1109/SP61157.2025.00240

[290] Shoshana Zuboff. 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.

[291] Anna Ådahl. 2013. The exhibited. https://www.annaadahl.com/works/the-exhibited-2013

A Depiction of Artwork-Discovery Process

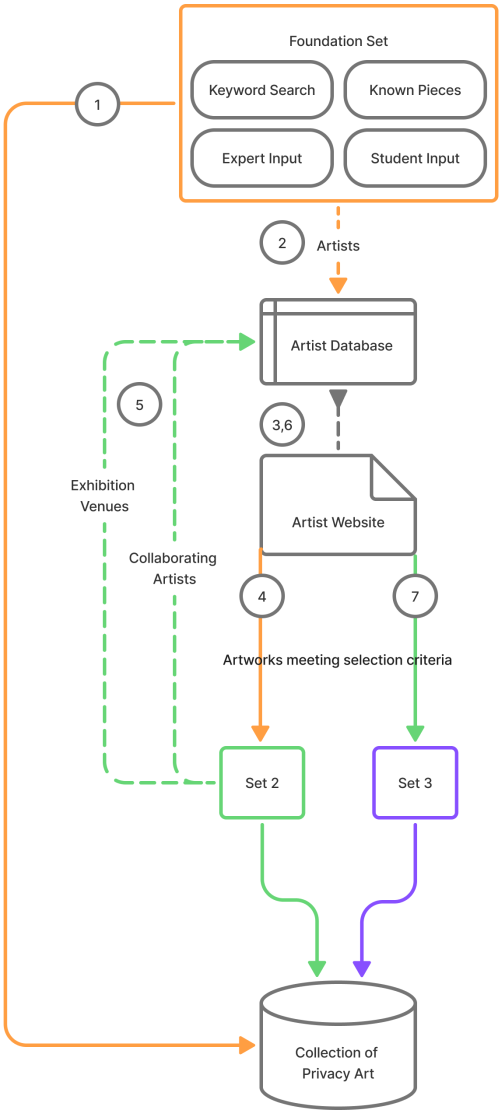


Figure 9: A graphical summary of our process for discovering privacy artworks. We first add artworks to our Foundation Set (1). Artists are added to a database (2) and we visit their websites (3), adding the first round of works to Set 2 (4). We then search exhibition venues and collaborating artists associated with Set 2 for more artists, adding them to the artist database (5). We repeat the process to add to Set 3 (6,7).

B Artworks in Our Sample

Table 1: The sample of artworks from our larger database that we qualitatively coded and the numbers (*A-#*) that reference them in the text. Nationality was determined based on public information on where an artist lives/works and their citizenship.

A-#	Title	Artist	Year	Medium	Venue	Artist's Nationality
1	How Not to Be Seen: A Fucking Didactic Educational .MOV File [250]	Hito Steyerl	2013	Video	Gallery	Germany
2	Hyperface [117]	Adam Harvey	2017	Textile, Wearable	Festival	Germany, USA
3	Surveillance Speaker [68]	Dries Depoorter	2018-2024	Hardware	Gallery, Public Art	Belgium
4	The Exhibited [291]	Anna Ådahl	2013	Live Performance, Multimedia Installation	Gallery	Sweden
5	Choir of Missed Connections [21]	Aram Bartholl	2024	Sculpture	Festival/Pop-up	Germany
6	Stealth Cell Tower [194]	Julian Oliver	2015	Sculpture	Public Art	New Zealand
7	Security Blanket [62]	Lorrie Cranor	2013	Textile	Festival/Pop-up	USA
8	Security Blanket [101]	Mariam Ghani	2005	Architectural Space, Multimedia Installation	Festival/Pop-up	Afghanistan, Lebanon, USA
9	Every CCTV Camera (CC) [38]	James Bridle	2017	Photographs	Gallery	Greece, UK
10	Image Operations [198]	Trevor Paglen	2018	Video	Gallery	USA, Germany
11	MWITM [170]	Lauren Lee McCarthy, Kyle McDonald	2017	Software, Still Image	Gallery	China, USA
12	Surveillance Camera [5]	Ai Weiwei	2010	Sculpture	Gallery	China, Portugal
13	Selfie Stick [247]	Dan Stavy	2017	Sculpture, Software	Public Art	Israel, USA
14	Live-Taped Video Corridor [187]	Bruce Nauman	1967, 1968	Architectural Space, Multimedia Installation	Gallery	USA
15	Back to the Light [218]	Peters Riekstins	2016	Multimedia Installation	Gallery	Latvia
16	VOX [103]	Steve Giasson	2015-2016	Still Image	Festival/Pop-up	Canada
17	Netless2 [265, 266]	Danja Vasiliev	2012	Software	Public Art	Germany, Russia
18	The Right to be Forgotten [123]	Esther Hovers	2021-2024	Photographs	Gallery	Netherlands
19	Found Footage Stalkers [133]	KairUs	2018	Photographs	Gallery	Austria, Finland
20	EXISTech Corp. [165]	Steve Mann	c. 2001	Hardware, Wearable	Public Art	Canada
21	Classification.01 [72]	Mimi Onuoha	2017	Sculpture	Gallery	Nigeria, USA
22	Drone #4 [230]	Björn Schülke	2005	Sculpture	Gallery	Germany
23	If This is a Global Surveillance Center [160]	He-Lin Luo	2019	Multimedia Installation	Gallery	Taiwan
24	Pigeonblog [59]	Beatriz da Costa, Cina Hazegh, Kevin Ponto	2006-2008	Wearable, Multimedia Installation	Festival/Pop-up	Germany
25	The Eye and I [124]	Hsin-Chien Huang	2023	Multimedia Installation	Festival/Pop-up	Taiwan
26	LANDSAT.EARTH [257]	Shaheer Tarar	2023	Digital	Online	UK
27	The Mass Psychology of Fascism [209]	Surveillance Camera Players	1999, 2000	Live Performance	Public Art	USA
28	Good Morning Mr. Orwell [199]	Nam June Paik	1984	Live Performance, Livestream	Mass Media	South Korea, USA
29	Papa Bed [227]	Julia Scher	2003	Sculpture	Gallery	USA
30	Sorry to Bother You [120]	Dan Hett	2018	Video Game	Online	Turkey, UK
31	Citizen [78, 79]	Hasan Elahi	2006	Photographs	Online	Bangladesh, USA
32	The Hoodie_ [73]	Bogomir Doringer	2008	Still Image	Gallery	Serbia, Netherlands
33	Deletion Process [106, 107]	Kyriaki Goni	2013, 2015, 2019	Hardware, Multimedia Installation	Gallery	Greece
34	The Nemesis Machine: Manifestation [245]	Stanza	2023	Hardware, Multimedia Installation	Gallery	UK, USA
35	iSee [202, 268]	The Institute for Applied Autonomy	2004	Digital, Software	Online	USA
36	The Feeling of Being Watched [36, 274]	Assia Boundaoui	2018	Video	Festival/Pop-up	Algeria, USA
37	3 Degrees of Separation from the Military-Industrial-Prison-Data-Surveillance State [145]	Sam Lavigne	2015	Digital	Online	USA
38	Uninvited [261]	Nye Thompson	2021	Video	Gallery	Austria, Switzerland, UK, USA
39	Audience [283]	Jens Wunderling	2010	Digital	Gallery	Germany
40	CMYK [49]	Daniel Canogar	2014	Sculpture, Video	Gallery	Spain, USA
41	A Girl Reading a Letter by an Open Window [260, 267]	Johannes Vermeer	c. 1657-1659	Painting	Gallery	Netherlands
42	Traffic Cam Photobooth [282]	WTTDOTM	2024	Digital, Software	Online	USA
43	Always Learning [156]	Machine Listening	2018	Video	Gallery, Festival/Pop-up	Australia
44	Mic Jammer [47]	Allison Burtch	2015	Hardware, Software	Gallery	USA
45	You Saw Me? [157]	Melanie Lowe	2008	Digital, Multimedia Installation	Public Art, Gallery	Canada
46	System Azure Security Ornamentation [163]	Jill Magid	2002	Live Performance	Public Art	USA
47	Peepshow [186, 270]	Giles Walker	2007	Live Performance, Multimedia Installation	Festival/Pop-up	UK, Canada
48	Data Collection [135]	Dave Kemp	2010	Photographs, Video, Multimedia Installation	Gallery	Canada
49	Surveillance Cutie [144]	Fabiola Larios	2024	Multimedia Installation	Festival/Pop-up	Mexico, USA
50	Trusted Traveller [201]	Yuri Pattison	2017	Architectural Space, Digital, Multimedia Installation	Gallery	Ireland, UK
51	Twelve Nodes [141]	Egor Kraft	2019	Hardware, Software, Multimedia Installation	Gallery	Austria, Germany, Japan, Russia
52	Backspace [264]	Ben Van den Berghe	2022	Architectural Space	Gallery	Belgium
53	Eavesdropper 1 [184]	Mschf	2022	Hardware	Gallery	USA
54	Convergence LA [8]	Refik Anadol	2017	Digital, Multimedia Installation	Public Art	Turkey, USA
55	Camouflage [263]	Suzanne Treister	2013	Painting, Still Image	Gallery	UK
56	Dark Side of the Prism [31]	Justin Blinder	2013	Digital, Software	Online	USA
57	Reality TV [262]	Timo Toots	2017, 2023	Hardware, Software	Gallery, Public Art	Estonia
58	Suspicious Minds [30]	Viktoria Binschtok	2009	Photographs	Gallery	Russia, Germany
59	My Little Big Data [168]	Eva and Franco Mattes	2019	Video, Architectural Space, Multimedia Installation	Gallery	Italy, USA
60	Yuppie Ghetto with Watchdog [97]	Paul Garrin	1989	Architectural Space, Video, Multimedia Installation	Gallery	USA
61	Minor Urbanism [235]	Mark Shepard	2012	Video	Online	USA
62	Which no one will ever see [7]	Meriç Algün Ringborg	2012	Multimedia Installation	Gallery	Turkey, Sweden
63	Nest [100]	Jakub Geltner	2015	Sculpture	Public Art	Czechia
64	MyPocket [9]	Burak Arikan	2008	Software, Multimedia Installation	Gallery	Turkey
65	Demand Ware [44]	Jonah Brucker-Cohen	2022	Digital, Software	Festival/Pop-up	Ireland, USA
66	Carbolytics [180]	Joana Moll	2022	Digital, Software, Multimedia Installation	Gallery, Online	Spain, Germany
67	SVEN [6]	Amy Alexander	2006-2007	Digital, Multimedia Installation	Gallery, Public Art	USA
68	Sticky Floors [238]	Ann-Sofi Sidén	2014	Video, Multimedia Installation	Festival/Pop-up	Sweden
69	Nakagin Capsule Tower [127, 142]	Kisho Kurokawa	1972	Architectural Space	Building	Japan
70	Embroidered Surveillance [146]	Francine Leclercq	2024	Textile	Festival/Pop-up	France, USA
71	Go Rando [109]	Ben Grosser	2021	Digital, Software	Gallery	USA
72	The Status Project [46]	Heath Bunting	c. 2012	Digital	Gallery, Festival/Pop-up	UK
73	Sanctum [61]	James Coupe	2015	Hardware, Software	Gallery, Public Art	UK, USA

C Codebook

Table 2: Our codebook and the artworks in our sample to which we applied each code (part 1 of 2).

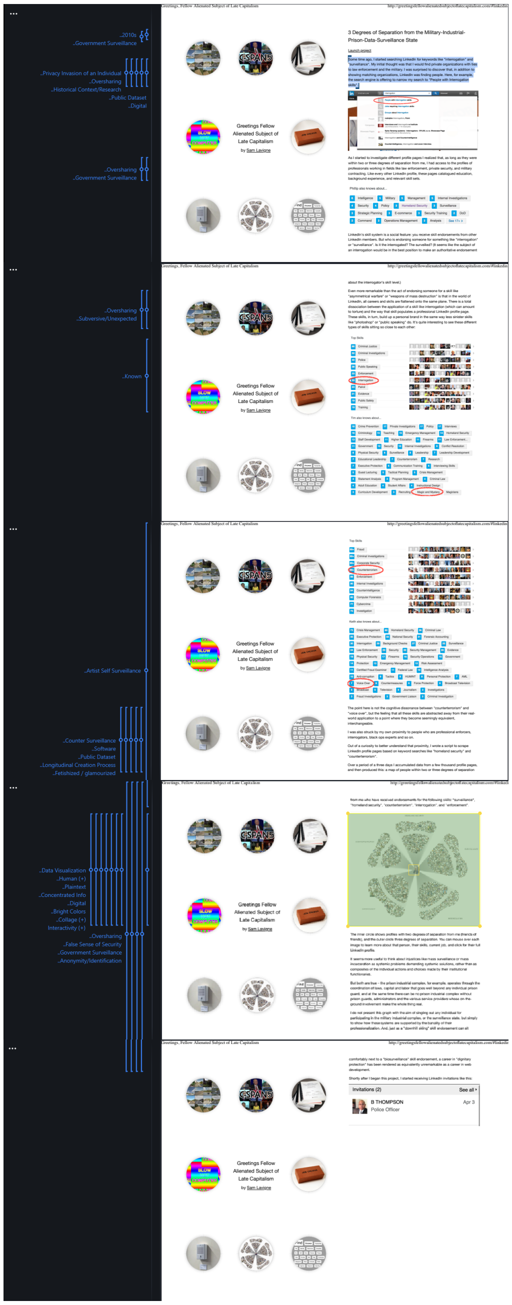
Code	Definition	Artworks (A-#)
Elements & Principles of Design	Arrangement, shape, and composition	
Colors		
↪ Bright Colors	Whites, yellows, hot pink, etc.	7, 10, 13, 15, 21, 25, 28, 31, 32, 34, 35, 37, 38, 40, 42, 44, 45, 47, 49, 52, 55, 56, 58, 59, 60, 64, 67, 72
↪ Dark Colors	Blacks, dark greys, etc.	3, 4, 10, 11, 15, 18, 20, 23, 25, 26, 28, 29, 32, 33, 35, 38, 39, 40, 42, 44, 48, 51, 54, 59, 60, 64, 67
↪ Monochrome	One color with different tones, or black and white	1, 6, 12, 14, 15, 18, 20, 22, 25, 26, 27, 38, 47, 53, 55, 58, 59, 62, 64, 68, 70
↪ Contrasting Colors	Uses strongly opposing colors, such as red and green	1, 2, 4, 11, 17, 26, 29, 33, 34, 51, 52, 54, 55
Distortion	Alters the perception of visual or auditory components	2, 4, 14, 15, 16, 18, 25, 26, 28, 32, 38, 39, 55, 59, 71
↪ Tactile/Analog Representation of Digital	Digital object is represented through physical media	6, 7, 33, 53, 55, 57, 59, 62, 70, 73
↪ Digitized	Pixelated, synthetic, or screen-mediated aesthetics	1, 10, 18, 25, 26, 50, 52, 66, 70
Scale	Emphasizes size in respect to space	4, 7, 9, 11, 13, 14, 15, 16, 17, 19, 20, 21, 25, 26, 29, 31, 32, 34, 35, 37, 48, 51, 52, 53, 54, 55, 57, 58, 59, 64, 66, 72, 73
Collage	Piecing together many smaller works or elements, often using repetition and variation	4, 5, 7, 9, 13, 15, 18, 19, 23, 26, 28, 31, 32, 37, 38, 42, 48, 49, 52, 55, 58, 61, 63, 67, 68, 69, 73
↪ Composite	Overlapping or merging multiple elements into the same space	15, 26, 28, 32, 38
Perspective	Position the artwork is viewed from	
↪ Voyeuristic	Viewer in the watcher, camera POV	4, 14, 23, 25, 27, 33, 38, 39, 41, 42, 47, 61, 67, 68, 69, 70, 73
↪ Surveillance is Looming	Situated above the viewer or subject	3, 9, 22, 26, 54, 67
↪ Shifts	Literal viewpoint shifts across the artwork	4, 8, 10, 38, 50, 58
Motion	Visible movement, physically or visually	1, 3, 36, 38, 49, 45, 47, 49, 50, 53, 54, 59, 61, 62, 66, 67, 68
Lighting	Lights are used to direct attention	4, 5, 13, 21, 25, 28, 34, 43, 45, 50, 54, 57
Visual and auditory lexicon	The sensory vocabulary that the artist uses as components to build from	
Plaintext	Words, source code	1, 6, 7, 10, 11, 15, 16, 18, 27, 33, 34, 37, 38, 39, 45, 48, 51, 53, 54, 59, 61, 62, 64, 70, 72, 73
Everyday Object	Common objects in daily life (e.g., smartphones, bedding)	5, 6, 8, 11, 13, 17, 20, 25, 29, 30, 32, 39, 40, 41, 44, 49, 50, 57, 59, 60, 67, 68, 69, 73
Human	Human form (e.g., bodies, faces)	1, 2, 4, 10, 13, 15, 18, 25, 27, 28, 32, 36, 37, 38, 39, 41, 57, 58, 59, 60, 61, 67, 70
Camera (object)	Visible camera	3, 5, 9, 12, 14, 20, 22, 25, 29, 39, 46, 47, 49, 50, 60, 62, 63, 73
Audio	Audio or sound plays	38, 54, 60
↪ Music	Music is used within the artwork or is the artwork itself	6, 10, 25, 28, 47, 56, 62, 67
↪ Robotic Voice	A robotic or synthetic voice can be heard in the artwork	1, 3, 5, 43
↪ Human Voice	A human voice can be heard in the artwork	8, 62, 73
Public Infrastructure	Human-built public infrastructure (e.g., buildings, streets)	9, 17, 23, 24, 34, 36, 45, 46, 50, 52, 59, 60, 61, 70, 73
Common Symbols	A shape or object that is representative of another object or idea	1, 27, 41, 51, 62, 66, 71
Microphone (object)	Visible microphone	22, 44, 53
Display	The modes in which the artwork is presented or output to viewers	
Data Visualization	Network graphs, bar charts, interactive interfaces	24, 33, 34, 35, 37, 54, 59, 61, 64, 66, 72
↪ Bounding Boxes	Rectangles displayed around objects (e.g., faces) to suggest detection	2, 10, 54, 57, 61, 67
Livestream	Video plays in real time	4, 14, 23, 49, 67, 73
Framed Image	Parts of the artwork are framed for display	11, 18, 52, 55

Table 3: Our codebook and the artworks in our sample to which we applied each code (part 2 of 2).

Code	Definition	Artworks (A-#)
Techniques	Strategies and methods artist utilizes to construct, critique, or reframe surveillance and privacy invasion	
Interactivity	The viewer can interact directly with the artwork	3, 4, 6, 8, 14, 17, 21, 25, 26, 30, 33, 34, 35, 37, 42, 48, 53, 57, 60, 66, 71, 73
Speculative	Imagines future possibilities	17, 20, 21, 23, 24, 25, 28, 38, 43, 51, 65, 67, 72
↪ Proof of Concept	Demonstrates feasibility through a functional prototype	2, 6, 17, 24, 35, 44, 64, 65, 66, 67
Counter-Surveillance Interventions	Direct methods to resist or evade surveillance (e.g., camouflaging, obfuscation)	1, 2, 11, 17, 23, 24, 26, 31, 32, 35, 37, 44, 46, 55, 56, 59, 62, 71
Exposing Surveillance	Reveals hidden or often ignored surveillance	9, 12, 20, 22, 23, 24, 25, 29, 35, 36, 39, 42, 43, 46, 55, 56, 58, 66
Imitation	Mimics or exaggerates an existing object, topic, or cultural form, often as satire or parody	5, 6, 12, 13, 20, 22, 31, 34, 40, 47, 50, 55, 60, 62, 3, 67, 69
Information Withheld From Viewer	Restricts what the viewer knows	11, 14, 21, 31, 48, 55, 57, 59, 65
Observation	Dynamics of watching and being watched (visual and data collection)	
Data Source/Subject	Whose data is collected/privacy invaded	
↪ Specific Individual (public)	Specific individual from the public is highlighted	1, 6, 8, 15, 16, 18, 19, 23, 30, 37, 39, 41, 45, 48, 58, 67, 68, 69, 70
↪ Viewer	The viewer is the subject of surveillance/privacy invasion	3, 4, 6, 8, 13, 21, 25, 34, 39, 42, 49, 53, 57, 60, 67, 69, 71, 73
↪ The Public	The general public in an aggregate form	3, 6, 16, 17, 19, 23, 24, 34, 54, 61, 66, 67, 68, 70, 73
↪ Artist Self-Surveillance	Artist uses their own data or personal experiences	11, 14, 27, 28, 30, 31, 33, 37, 59, 64, 72
↪ Performers	Those hired by an artist or part of a collective art group	4, 10
Data Collection Method	How data used in the artwork is collected	
↪ Camera	Uses cameras	3, 10, 13, 14, 21, 23, 25, 38, 39, 42, 49, 57, 60, 67, 68, 70, 73
↪ Text-mediated Communications	Uses text or social media data	6, 11, 15, 30, 39, 59, 71, 72, 73
↪ Microphone	Uses microphones	8, 16, 53
↪ Viewer Device	Uses the viewer’s personal device	42, 45
Duration of Data Collection	The artwork emphasizes the length of time data is collected, or comments on the persistence of data traces	6, 8, 13, 15, 17, 18, 19, 21, 33, 35, 39, 45, 48, 54, 59, 61, 64, 68, 73
Implied Observation	Suggests that the viewer is being watched, e.g. non-functioning cameras	4, 5, 20, 21, 22, 47, 50, 56, 57, 63, 69
Tone	Atmosphere that frames how the artwork is experienced	
Unsettling	Discomfort or eeriness	5, 6, 12, 14, 15, 18, 19, 23, 25, 29, 30, 32, 36, 38, 39, 48, 49, 60, 65, 66, 69, 73
↪ Industrial	Utilitarian or cyberpunk (e.g., pipes, wires, metal)	3, 4, 13, 15, 20, 21, 25, 29, 34, 38, 39, 40, 47, 49, 50, 51, 53, 54, 59, 60, 69
↪ Panopticon	Constant sense of overwhelming surveillance	12, 20, 23, 34, 41, 69
Fun and Playful	Light-hearted and whimsical in tone	3, 8, 28, 31, 42, 46, 47, 49, 67
Glamourized / Fetishized	Glamorous or pleasurable to view	9, 34, 37, 41, 46, 47, 49
Mundane	Ordinary, everyday life	4, 8, 31, 49, 68, 69, 70
Ornate	Refined, elegant, or high-class	12, 46, 52
Topics	The ideas and themes the artwork engages or critiques	
Privacy-invading Technology, Algorithms, and Identity	Technological systems that invade privacy and their implications	
↪ Personal Identity	How a person is defined by themselves or others	2, 4, 11, 13, 15, 18, 19, 21, 25, 32, 33, 36, 40, 41, 45, 50, 59, 62, 64, 67, 71, 72
↪ Artificial Intelligence	Classification algorithms, computer vision	2, 3, 10, 13, 21, 32, 34, 38, 39, 43, 54, 57, 61, 64, 67, 72, 73
↪ Algorithmic Assumption	Inferences made by algorithms	10, 21, 32, 64, 71
Organized Surveillance / Data Collection	Surveillance and data collection by an organization	
↪ Government Surveillance	Law enforcement, intelligence agencies	1, 6, 9, 12, 17, 18, 23, 24, 25, 26, 28, 33, 34, 35, 36, 37, 42, 46, 47, 50, 54, 55, 56, 58, 61, 62, 66, 67, 70, 71, 72
↪ Corporate Surveillance	Social media companies, browsers	33, 35, 43, 44, 55, 56, 66, 71, 72, 73
Public vs. Private Space	Questions which digital / physical spaces are private or public	1, 4, 5, 16, 23, 31, 40, 41, 45, 52, 54, 59, 60, 62, 69

D Example Coded Piece

To begin coding, the coder reads through the document to become familiar with overall content. Codes pertaining to the visual content of the document are applied to a bounding box drawn around images (see the fourth panel in Figure 10). In this example, the consistent images on the left are ignored, since these refer to other artworks by the artist. The fourth panel contains an image of the artwork; other images contain information about the process. Process images typically contain information about mechanisms or more subjective, interpretive elements. In the artwork image, our sample contains the codes "Data Visualization" (display mode), "Human" (visual object), and "Collage" (design element), among others. Codes pertaining to the textual content of the document are applied to a highlighted paragraph (see the first panel in Figure 10). Each paragraph is considered one unit of text for consistency in coder analysis. Codes applied to text have a broader scope, since text may contain both information about the mechanisms of the artwork and themes or topics the artist addresses.


..2010s
..Government Surveillance
..Privacy Invasion of an Individual
..Oversharing
..Historical Context/Research
..Public Dataset
..Digital
..Oversharing
..Government Surveillance
..Oversharing
..Subversive/Unexpected
..Known
..Artist Self Surveillance
..Counter Surveillance
..Software
..Public Dataset
..Longitudinal Creation Process
..Fetishized / glamourized
..Data Visualization
..Human (+)
..Plaintext
..Concentrated Info
..Digital
..Bright Colors
..Collage (+)
Interactivity (+)
..Oversharing
..False Sense of Security
..Government Surveillance
..Anonymity/Identification
Greetings, Fellow Alienated Subject of Late Capitalism
http://greetingsfellowalienatedsubjectoflatecapitalism.com/#linkedin
Greetings Fellow Alienated Subject of Late Capitalism
by Sam Lavigne

3 Degrees of Separation from the Military-Industrial-Prison-Data-Surveillance State

Launch project

Some time ago, I started searching LinkedIn for keywords like "interrogation" and "surveillance". My initial thought was that I would find private organizations with ties to law enforcement and the military. I was surprised to discover that, in addition to showing matching organizations, LinkedIn was finding people. Here, for example, the search engine is offering to narrow my search to "People with Interrogation skills".

As I started to investigate different profile pages I realized that, as long as they were within two or three degrees of separation from me, I had access to the profiles of professionals working in fields like law enforcement, private security, and military contracting. Like every other LinkedIn profile, these pages catalogued education, background experience, and relevant skill sets.

Phillip also knows about...

6 Intelligence · 5 Military · 5 Management · 5 Internal Investigations
4 Security · 4 Policy · 3 Homeland Security · 3 Surveillance
3 Strategic Planning · 3 E-commerce · 3 Security Training · 2 DoD
2 Command · 2 Operations Management · 2 Analysis · See 17+ ›

LinkedIn's skill system is a social feature: you receive skill endorsements from other LinkedIn members. But who is endorsing someone for something like "interrogation" or "surveillance". Is it the interrogated? The surveilled? (It seems like the subject of an interrogation would be in the best position to make an authoritative endorsement about the interrogator's skill level.)

Even more remarkable than the act of endorsing someone for a skill like "asymmetrical warfare" or "weapons of mass destruction" is that in the world of LinkedIn, all careers and skills are flattened onto the same plane. There is a total dissociation between the application of a skill like interrogation (which can amount to torture) and the way that skill populates a professional LinkedIn profile page. These skills, in turn, build up a personal brand in the same way less sinister skills like "photoshop" or "public speaking" do. It's quite interesting to see these different types of skills sitting so close to each other:

Top Skills

66 Criminal Justice
50 Criminal Investigations
40 Police
38 Public Speaking
33 Enforcement
33 Interrogation
23 Patrol
21 Evidence
19 Public Safety
19 Training

Tim also knows about...

18 Crime Prevention · 17 Private Investigations · 17 Policy · 17 Interviews
16 Criminology · 15 Teaching · 15 Emergency Management · 14 Homeland Security
13 Staff Development · 11 Higher Education · 11 Firearms · 11 Law Enforcement...
11 Government · 10 Security · 10 Internal Investigations · 9 Conflict Resolution
8 Physical Security · 8 Surveillance · 8 Leadership · 7 Leadership Development
7 Educational Leadership · 7 Counterterrorism · 7 Research
7 Executive Protection · 6 Communication Training · 6 Interviewing Skills
5 Guest Lecturing · 5 Tactical Planning · 5 Crisis Management
4 Statement Analysis · 4 Program Management · 4 Criminal Law
4 Adult Education · 4 Student Affairs · 4 Instructional Design
3 Curriculum Development · 3 Recruiting · Magic and Mystery · Magicians

Top Skills

99+ Fraud
99+ Criminal Investigations
99+ Corporate Security
99+ Counterterrorism
99 Enforcement
90 Internal Investigations
84 Counterintelligence
80 Computer Forensics
77 Cybercrime
75 Investigation

Keith also knows about...

72 Crisis Management · 60 Homeland Security · 36 Criminal Law
35 Executive Protection · 33 National Security · 31 Forensic Accounting
30 Interrogation · 29 Background Checks · 27 Criminal Justice · 25 Surveillance
24 Law Enforcement · 23 Security · 22 Security Management · 20 Evidence
19 Physical Security · 17 Firearms · 16 Security Operations · 15 Government
14 Protection · 13 Emergency Management · 12 Risk Assessment
11 Certified Fraud Examiner · 11 Federal Law · 10 Intelligence Analysis
10 Anti-corruption · 9 Tactics · 8 HUMINT · 8 Personal Protection · 7 AML
7 Voice Over · 6 Countermeasures · 6 Force Protection · 6 Broadcast Television
5 Broadcast · 5 Television · 5 Journalism · 3 Investigations
3 Fraud Investigations · 3 Government Liaison · 3 Criminal Investigation

The point here is not the cognitive dissonance between "counterterrorism" and "voice over", but the feeling that all these skills are abstracted away from their real-world application to a point where they become seemingly equivalent, interchangeable.

I was also struck by my own proximity to people who are professional enforcers, interrogators, black ops experts and so on.

Out of a curiosity to better understand that proximity, I wrote a script to scrape LinkedIn profile pages based on keyword searches like "homeland security" and "counterterrorism".

Over a period of a three days I accumulated data from a few thousand profile pages, and then produced this: a map of people within two or three degrees of separation from me who have received endorsements for the following skills: "surveillance", "homeland security", "counterterrorism", "interrogation", and "enforcement".

The inner circle shows profiles with two degrees of separation from me (friends of friends), and the outer circle three degrees of separation. You can mouse over each image to learn more about that person, their skills, current job, and click for their full LinkedIn profile.

It seems more useful to think about injustices like mass surveillance or mass incarceration as systemic problems demanding systemic solutions, rather than as composites of the individual actions and choices made by their institutional functionaries.

But both are true – the prison industrial complex, for example, operates through the coordination of laws, capital and labor that goes well beyond any individual prison guard, and at the same time there can be no prison industrial complex without prison guards, administrators and the various service providers whose on-the-ground involvement make the whole thing real.

I do not present this graph with the aim of singling out any individual for participating in the military industrial complex, or the surveillance state, but simply to show how these systems are supported by the banality of their professionalization. And, just as a "downhill skiing" skill endorsement can sit comfortably next to a "biosurveillance" skill endorsement, a career in "dignitary protection" has been rendered as equivalently unremarkable as a career in web development.

Shortly after I began this project, I started receiving LinkedIn invitations like this:

Invitations (2) See all ›
B THOMPSON Apr 3
Police Officer

Figure 10: An example of a coded artwork, *3 Degrees of Separation* [145] (©Sam Lavigne), in the coder window of MAXQDA.