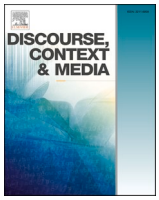
Surveillance at the (inter)face: a nexus analysis

Discourse, Context & Media 62 (2024) 100832

Contents lists available at ScienceDirect

Discourse, Context & Media

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



Surveillance at the (inter)face: A nexus analysis

Rodney H. Jones *

University of Reading, United Kingdom

ARTICLE INFO

Keywords:
Facial recognition
Interfaces
Mediated discourse analysis
Nexus analysis
Surveillance

ABSTRACT

This paper discusses how facial recognition technology is changing the way interfaces are designed for digital surveillance. Drawing on work in mediated discourse analysis, it argues that interfaces for surveillance (as well as digital interfaces more generally) should be understood as *sites of engagement* where particular texts, bodies, social relationships, and social practices come together to make surveillance possible. To illustrate this framework, I analyse the controversial facial recognition service PimEyes, exploring how the 'discourses in place' on the PimEyes website, the 'interaction orders' it makes possible, and the 'historical bodies' that users bring to the site work together to lure users into using the service and contribute to the normalisation of digital surveillance using facial recognition. This paper contributes not just to our understanding of surveillance, but also to our understanding of digital interfaces more generally by showing how they function to enable new kinds of social identities, social relationships and social practices.

1. The interface and the face

The intersection south of Changhong Bridge in the city of Xiangyang used to be a nightmare. Cars drove fast and jaywalkers darted into the street.

Then last summer, the police put up cameras linked to facial recognition technology and a big, outdoor screen. Photos of lawbreakers were displayed alongside their names and government I.D. numbers. People were initially excited to see their faces on the board, said Guan Yue, a spokeswoman, until propaganda outlets told them it was punishment.

'If you are captured by the system and you don't see it, your neighbors or colleagues will, and they will gossip about it,' she said. 'That's too embarrassing for people to take.'

— *New York Times,* July 8, 2018, 'Inside China's Dystopian Dreams: A.I., Shame, and Lots of Cameras' (Mozur, 2018)

When we think of digital surveillance, we are most likely to think of websites gathering data about us through our clicks, site visits and search queries — what Clarke (1988) has called 'dataveillance'. This special issue's invitation to consider digital media 'at the interface,' however, provides an opportunity to consider ways in which the digital interfaces that collect information about us (along with the kind of information that they collect) are rapidly changing. The example above, for instance, illustrates how facial recognition technologies are transforming digital surveillance. Indeed, tracking individuals through these technologies has become almost as pervasive as more conventional forms of digital surveillance not just in places like China, but across the globe. These technologies are put to a range of different uses from catching traffic violators, to creating entertaining experiences for social media users, to getting passers-by to engage with outdoor advertising, and the more pervasive these technologies become, the more the new kinds of surveillance they enable are normalised (Norval and Prasopoulou, 2017).

Another thing this example demonstrates is how *interactive* people's encounters with these technologies can sometimes be. While much of the scholarship on facial recognition distinguishes it from other forms of digital surveillance based on the fact that users do not have to *do* anything in order to produce data (Andrejevic and Selwyn, 2022; Introna and Wood, 2002), much of the surveillance that is performed using it (in places like airports, banks, and schools) is not just overt but often *requires* people to interact with interfaces (such as cameras and screens) in rather deliberate ways. In many cases, these interactions and the kinds of social relationships and social identities they create are as important a part of the practice of surveillance as the gathering of data, serving as they do, to elicit performances of compliance from those who are being monitored.

Most importantly, this example compels us to reconsider what we mean by the term 'interface' itself when it comes to digital surveillance. Usually, when we think of interfaces, we think about 'equipment' such as keyboards, computer screens, cameras and microphones. But what

* Address: University of Reading, Rm 212, Edith Morley Building, Shinfield Road, Whiteknights, Reading, Berkshire RG6 6EL, United Kingdom.
E-mail address: r.h.jones@reading.ac.uk.

https://doi.org/10.1016/j.dcm.2024.100832
Received 2 May 2024; Received in revised form 7 August 2024; Accepted 14 September 2024
Available online 24 October 2024

else in the situation described above also constitutes part of the 'interface'? Is it limited to the cameras and the screens upon which the faces of jaywalkers are projected, or should we also count the traffic lights, the zebra crossing, the street signs, and even the vehicles and other pedestrians, all of which are equally important parts of people's 'interfacing' with traffic crossings?

In this paper I will argue, drawing on work in mediated discourse analysis (Norris and Jones, 2005; Scollon, 2001), that to understand interfaces for surveillance we need to go beyond a focus on technologies like keyboards, computer screens and surveillance cameras, and see interfaces as *nexuses* of technologies, texts, bodies, social relationships, and social practices which come together at particular moments to make surveillance possible. To test this approach, I will apply it to analysing a controversial web service known as PimEyes, which enables people to use facial recognition technology to find images of individuals online based on a sample picture they provide. What I aim to show through my analysis is how this broader understanding of digital interfaces can help us understand not just how technology companies and governments transform people into compliant objects of surveillance, but also how interfaces contribute to normalising new kinds of social practices, social relationships and social identities.

2. What is an interface?

Most of the work in the interdisciplinary field of 'interface studies' over the past four decades has defined digital interfaces as the software and hardware that shape the interaction between computers and their users by 'translating' between them and 'making one sensible to the other' (Johnson, 1997: 14). Among scholars working within this definition there has been considerable attention to the ways the semiotics of interfaces affect users' understanding not just of the computer, but also of the world as it is increasingly mediated through digital media. (see e.g. Manovich, 2001). Not surprisingly, it is this cultural/semiotic orientation that has most influenced discourse analytical work on interfaces, especially by multimodal and critical discourse analysts concerned with the way interfaces work to reinforce ideologies and relationships of power (see e.g. Kvåle, 2016). As far back as 1994, Selfe and Selfe described interfaces as perpetuating asymmetrical power relations of class, race and gender by promoting the 'values of rationality, hierarchy and logocentrism' (p. 482). More recently, Djonov and van Leeuwen (2017: 571) have argued that digital interfaces are defined both by the 'semiotic resources' they make available to users, and the 'semiotic regimes' they *impose* on them, which lock them into normative ways of making meaning.

Other scholars of interfaces, however, have concerned themselves less with their semiotic dimensions and more with their spatial and material dimensions. This is especially true of those interested in mobile interfaces (e.g. Farman, 2021), who have focused on the ways interfaces mediate not just 'entities' or 'social actors', but also social contexts, acting as the threshold between different spaces, times and social situations. As digital interfaces increasingly become part of our everyday lives, writes De Souza and Silva (2006: 261), they come to 'define our perceptions of the space we inhabit, as well as the type of interaction with other people with whom we might connect' in that space.

Meanwhile, scholars with a posthuman orientation towards digital media have focused more on the embodied dimensions of interfaces, seeing them as points where the organic and inorganic join to form cybernetic organisms (Haraway, 1991). It is through attending to interfaces as technologies that 'enmesh humans into integrated circuits,' says Hayles (1999: 46–47), that we come to understand how the coupling of human and machine is sometimes so 'intense and multifaceted that it is no longer possible to distinguish meaningfully between the biological organism and the informational circuits in which the organism is enmeshed.'

All of these different orientations towards interfaces: the interface as semiotic mediator, as shaper of physical and social space, and as embodied experience, are relevant to the model of the interface that I will be developing here, which sees it not just in terms of semiosis, spatiality or embodiment, but as a dynamic collection of social and material *relationships* that involves all of these dimensions. This processual and relational view of interfaces is not entirely foreign to studies of digital media. Galloway (2012), for instance, has argued that interfaces are not stable objects, but rather sets of processes that create a certain 'effect' on social and material life, and Hookway (2014: 4) insists that interfaces are best thought of not as things but as 'form(s) of relation that obtain between two or more entities'.

Like most scholars interested in interfaces, mediated discourse analysts are interested in how social actors interact with tools in ways that make various kinds of social actions possible. These 'mediated actions' (Scollon, 2001: 5), however, do not occur in social vacuums in which tools and tool users can be abstracted from their material and social environments. Rather, they are 'irreversible, one-time-only' actions that are made possible when particular *combinations* of tools, bodies and social relationships come together at a'site of engagement', which Scollon (2001:4) defines as 'the real-time window that is opened through an intersection of social practices and mediational means (cultural tools) that make that action the focal point of attention of the relevant participants.' From this perspective, the 'interface' between tools and tool users cannot be located in the tool, or in the user, or in the environment in which the tool is used. Rather, the interface *is the site of engagement itself* where all three of these things intersect. When particular configurations of tools, texts, people and practices are regularly repeated, they come to constitute what the Scollons (2004: 28) call a 'nexus of practice', and the analysis of these recurring sites of engagement is known as *nexus analysis* (Scollon and Scollon, 2004).

This understanding of interfaces which insists that we look beyond technologies and 'semiotic surfaces' resonates with recent work in surveillance studies, which has struggled with the inadequacy of conceptions of surveillance that reduce it to instances of monitoring made possible by particular kinds of 'equipment' such as CCTV cameras or computers. Most contemporary approaches to surveillance view surveillant interfaces not as specific pieces of equipment, but rather as *assemblages,* 'emergent and unstable' configurations of technologies, institutions, people and practices which often 'lack discernible boundaries or responsible parties' (Haggerty and Ericson, 2000: 609). To see Foucault's (1975) panopticon, for instance, as simply a matter of Bentham's architectural design of a prison very much misses Foucault's point. It is not just the 'equipment' through which prisoners and guards interface with each other, but also the *social relationships* that the prison walls and watchtower help to create and the *psychological and embodied dispositions* that develop within the prisoners themselves which result in a form of 'discipline' in which the gaze of the guards becomes irrelevant and the prisoners' *consciousness* of being watched keeps them 'imprisoned'. Indeed, Foucult's main point in using the panopticon as a metaphor for modern surveillance societies is that, even when you take away the physical interface, the panopticon still works because of the way it has come to be *distributed* throughout society in the *bodies* of citizens, in the *discourses* that circulate through institutions, and in the *relationships* people have with figures like physicians, psychiatrists, school teachers and bureaucrats.

3. Discourses, interaction orders and historical bodies

For Scollon and Scollon (2004), sites of engagement similarly occur at the intersection of *discourses* (which they call 'discourses in place'), social *relationships* (which they call 'interaction orders'), and people's physical *bodies* (which they call 'historical bodies'). Discourses in place consist of all of the texts and technologies present or 'circulating through' (p. 19) particular moments of action, each introducing different affordances and constraints regarding what kinds of actions can occur. Interaction orders are the relationships between the different people and institutions present or circulating through the site, including

their respective 'rights' and 'responsibilities'. And historical bodies consist of the memories, habits, goals and dispositions that social actors bring to the site.

To illustrate how the intersection of these three elements comes to constitute an 'interface' for the social actor to accomplish an action, the Scollons (2003: 198–202) use the example of crossing the street. Discursive objects like traffic lights, crossing signals, street signs and zebra crossings direct pedestrians as to where and when to cross. People also commonly interact with traffic crossings through the behaviour of other pedestrians — parents might, for example, take the hand of a young child while crossing, and people frequently take their cues from the people around them when deciding when to cross. Finally, people 'interface' with traffic crossings through their own embodied practices of crossing the street, which might be different for people with different experiences of urban traffic or different purposes for crossing the street.

So how do the facial recognition cameras and computer screens installed at the intersection mentioned at the beginning of this paper change this site of engagement and consequently alter the practice of crossing the street? What a nexus analysis helps to highlight is that this change does not come from the presence of these technologies alone, but from the way they function to alter how the reoccurring discourses in place, interaction orders, and historical bodies of traffic crossings interact. The most obvious way they alter the discourses in place is by introducing a screen on which pictures of those who are crossing the street are projected, essentially transforming the bodies of jaywalkers into discourses in place to be 'read' by others. In fact, such processes of 'entextualization' (Bauman and Briggs, 1990) – turning the body into a text– are common features of surveillant interfaces. The process of entextualisation that is occurring here, however, involves not just the transformation of the face into an image on a screen, but also into *code*, turning it into information that can be linked to other kinds of information such as identity cards and police records.

Through these processes of entextualization, the technologies also bring about a change in the interaction order. Whereas pedestrians normally look to one another when crossing the street in order to figure out what to do, here they are directed to gaze at the offending pedestrian on the screen to figure out what *not* to do. In other words, the relationship between the offending pedestrian and the others changes from what Golfman (1963) calls a *with*, a group of people perceived to be together, to what Scollon (1998: 16) calls a *watch*, a group of people in which one or more come to be separated out from the others to become a spectacle offered up for appreciation or inspection. This shift does not just change the status of the jaywalker, but also the other pedestrians, who are suddenly recruited into the surveillant assemblage as 'watchers'.

Perhaps the most important change, however, occurs in the jaywalker, whose embodied experience of being held up as an 'object' for the inspection of the others causes 'embarrassment', which is designed to bring about changes in their historical body that will compel them to avoid similar situations in the future.

This analysis demonstrates the importance of seeing the interface as an *assemblage* of mutually articulating parts, none of which are able to operate independently with the same effect. The capture and extextualization of the jaywalker's face alone is not sufficient to cause shame without the gaze of the other pedestrians, and the self-consciousness caused by the jaywalker witnessing themselves is not sufficient without being experienced by a historical body conditioned to respond to shame. At the same time this analysis is still incomplete. One of the main principles of nexus analysis is the acknowledgement that discourses, interaction orders, and historical bodies do not just 'appear' at sites of engagement, but are themselves the result of historical trajectories of discourse and action that have led up to this particular moment, including the history of jaywalking at this particular intersection, the history of decisions by authorities leading to them placing the cameras there, and the histories of individual pedestrians, including their experiences of crossing as the street and their shared cultural understandings of shame. It is when we consider the site of engagement not just as a meeting point of texts, technologies, people and social relationships, but as a point at which multiple *histories* of street crossing, traffic enforcement, government surveillance and public shaming come together that we begin to see how the interface operates as a *nexus of practice*. In other words, we begin to see that what is mediating people's experience of this traffic crossing involves not just the discourses, interaction orders and historical bodies, but also broader *Discourses* (with a capital D) (Gee, 2014) about things like digital technologies, public order, state surveillance and shame that are 'circulating through' this moment.

This point is dramatically illustrated by Ariane Ollier-Malaterre, who, for her book *Living with Digital Surveillance in China* (2023), interviewed Chinese citizens about their experiences with digitally enhanced traffic crossings like this one. What she discovered is that the way people 'interface' with such sites depends on far more than the cameras and computer screens, or the power of the police, or even the embarrassing interactions that such technologies give rise to, but also on broader 'narratives' of safety, civility and nationalism. Among the most common narratives she encountered were 'anguishing' narratives of the lack of 'moral quality' (素质) among Chinese citizens which make such forms of punishment necessary, and 'redeeming' narratives of technology as a source of pride for the country, evidence of China's growing technological dominance over the West. Along with these narratives, her participants also talked about their emotional reactions to state surveillance, which ranged from feelings of anxiety that came from knowing that they were constantly being watched, to feelings of gratitude for the convenience such technologies brought, to feelings of delighted enchantment with these 'magical' technologies (de Seta, 2021).

The purpose of this detour into Ollier-Malaterre's research has been, on one hand, to provide a more nuanced picture of the situation at the intersection south of Chonghong Bridge than the 'dystopian' framing provided by the New York Times in the quote at the beginning of this paper, and on the other, to demonstrate that such 'framings' matter to how we analyse surveillant interfaces and how people experience them. Technologies, practices and social relationships at sites of engagement are always framed by broader social, political and economic Discourses, practices and relationships.

In the remainder of this paper I will apply this approach to digital interfaces to the controversial consumer facial recognition service PimEyes, based on an analysis of PimEye's website, the sequence of (inter)actions that users are guided through as they use it, the broader Discourses associated with the technology, and reactions to the service by users on social media sites like TikTok and Reddit. My aim is to understand what the website, the service it provides and the cast of social identities and social practices assembled around it can tell us about how consumers become entangled in this surveillant assemblage as both objects and agents of digital surveillance.

4. 'Googling' faces

One use of facial recognition technology that has attracted particularly negative attention from the media, politicians and privacy advocates is the development of 'facial recognition search engines' which are able to find photos of an individual that have been posted online based on a biometric pattern created from a sample photo of that person. In their recent overview of the privacy implications of facial recognition technologies, Andrejevic and Selwyn (2022) argue that the problem with such services is not just that they often violate laws on the collection of personal data, but that they normalise the use of facial recognition in ways that are likely to fundamentally alter norms around privacy. One example of such services that they single out as a 'cautionary tale' (p. 69) is the Polish start-up, PimEyes (as of this writing registered in Belize). PimEyes offers its facial recognition search engine to the public with limited capabilities for free and with more advanced capabilities on a tiered pricing scheme from $29.99 to $299.99 per month. Recent

estimates put the number of searches that take place using the service at 118,000 per day (Arntz, 2023). The site makes use of 'web crawlers', like those used by search engines like Google, which find 'publicly available' images of faces on the web and 'index' them based on a set of parameters which PimEyes refers to as 'facial fingerprints'. Because of this, PimEyes is able to argue that it does not collect people's images without their consent (although it does collect biometric data based on those images). The service is marketed as a means for people to search for pictures of themselves in order to detect the unauthorised use of their images online, but it is also used by people wishing to investigate, 'dox', stalk or blackmail others. Indeed, as I will discuss below, the latter uses seem to be the most common, leading Ella Jakubowska, a policy advisor for the privacy advocacy group European Digital Rights to call PimEyes 'stalkerware by design' (Hill, 2022).

In order to understand the PimEyes website as a *site of engagement*, I collected different kinds of data, including all the text and images displayed on the site, all the media stories it links to, as well as other stories about the company from mainstream media outlets (totalling 23), and legal briefs of complaints made against the company in the UK and Europe. In order to get a sense of users' experiences with the service, I also downloaded the first 20 videos from a TikTok search of #PimEyes, as well as the first 25 posts from a Reddit search for the company's name. The Reddit posts included a total of 117 comments and came from a range of subreddits such as r/privacy, r/CreatorsAdvice, r/Sextortion, r/catfish and r/OSINT (OSINT being an acronym for 'open source intelligence'). I analysed these data using the principles of nexus analysis I described above, focusing on how the discourses in place, the interaction orders the site creates, and the historical bodies of users and victims of users interact to promote certain kinds of social actions and social identities, as well as how these components are affected by broader Discourses, social relationships, and social norms that 'circulate through' the site via the media, the discourse of users, and the company's own corporate communications.

4.1. Discourses in/out of place

The most basic way that the PimEyes website functions as a surveillant interface is the way the semiotic resources on the site (text, images, hyperlinks, menus and input boxes) function to guide users through a particular series of 'transactions' (Hookway, 2014). As with many such websites, as users work their way through these transactions, they find the choices they are provided with narrowing in a manner that progressively nudges them into purchasing increasingly expensive features, which, in this case, are marketed to users as necessary to protect their privacy.

Upon visiting the homepage (https://pimeyes.com/en), the user is confronted with the headline: FACE SEARCH ENGINE/REVERSE IMAGE SEARCH/ UPLOAD PHOTO AND FIND OUT WHERE IMAGES ARE PUBLISHED next to a cartoon image of someone taking a selfie next to what appears to be the Leaning Tower of Pisa. Underneath this is a search box (Fig. 1) which resembles the familiar interfaces of search engines like Google. When clicked, it provides a field where users can drag and drop images and a button that can be clicked or tapped if they wish to use the camera in their device to take a picture of themselves. Underneath the search window is a reassuring piece of text that informs them that their photo will not be stored. On the computer version of the homepage, a banner runs along the bottom of the screen with the logos of well-known media companies: CNN, BBC, *The Washington Post*, and *The New York Times*, who appear to be endorsing the site. The ease and familiarity of the interface and the air of respectability created by these well-known brands combine to incite the curious user to upload a photo. Those who choose instead to scroll down the page are offered further incentives, first in the form of a passage entitled 'How PimEyes can help you' which explains, 'Our face finder helps you find your face and protect your privacy.' Underneath this text is another button that says 'Perform a search and try it'.

Those who continue to scroll down are offered still more information under the title HOW IT WORKS/PROtect your privacy, which is arranged under four headings representing the steps users are meant to take: 1. Upload a photo, 2. Access results (via the web addresses of sites where your image appears), 3. Set an alert (to monitor when your photo appears on the internet), and 4. Erase your photo (from external websites). The small print underneath these 'instructions', however, reminds users that, if they wish to engage in steps 2, 3 and 4, they must purchase a paid plan. The bottom of the homepage contains information on how users who have uploaded photos can 'opt out' of PimEye's search results (although at no point are users asked if they wish to 'opt in').

Users who choose to upload a photo are taken to a screen where the photo they have uploaded is displayed back to them along with boxes that they must tick to see the results of their search, one confirming that they are over 18, and the other two confirming that they have read the Terms and Conditions and accept the Privacy Policy, even though neither of these were made available *before* they uploaded their photo (Fig. 2). Like many solicitations of 'tick box consent' (Rock, 2016), this request is strategically issued at a point in the sequence of actions (right after the user has already uploaded their photo, and right before they are able to see their results) at which they are least likely to interrupt the process in order to review the lengthy Terms and Conditions and Privacy Policy that are available elsewhere on the site (Jones, 2020). This screen also offers other options, such as a button labelled 'Deep Search', but activating this button only results in a notification that the user must purchase a paid plan in order to use this feature.

After clicking Start Search, the user is presented with a series of thumbnails of images that the search engine has found (Fig. 3) with partial URLs (which are usually not enough to find the actual page where the image is posted). In order to 'unlock' the results, enabling the user to identify the source of the images, payment is required, either in the form of a one-time fee that will only unlock the current results, or a monthly subscription. If the user wants to avail themselves of the other services listed above, such as assistance from the company in sending DMCA or GDPR takedown notices to sites where they would like their images removed, or alerts when new images of them appear online, they need to purchase the more expensive PROtect plan for $79.99 a month or the most expensive Advanced plan for $299.99 per month.

This sequence of transactions constitutes what Scollon (2001: 139) has referred to as a 'funnel of commitment', a situation in which, the further one proceeds with a sequence of actions, the more difficult it becomes to terminate the sequence. This is particularly true for users

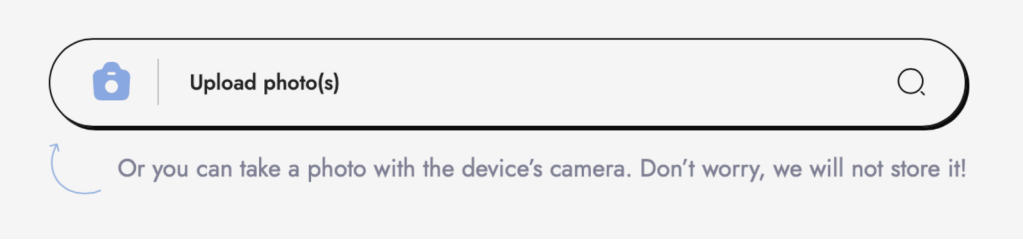


Fig. 1. Search box on home screen.

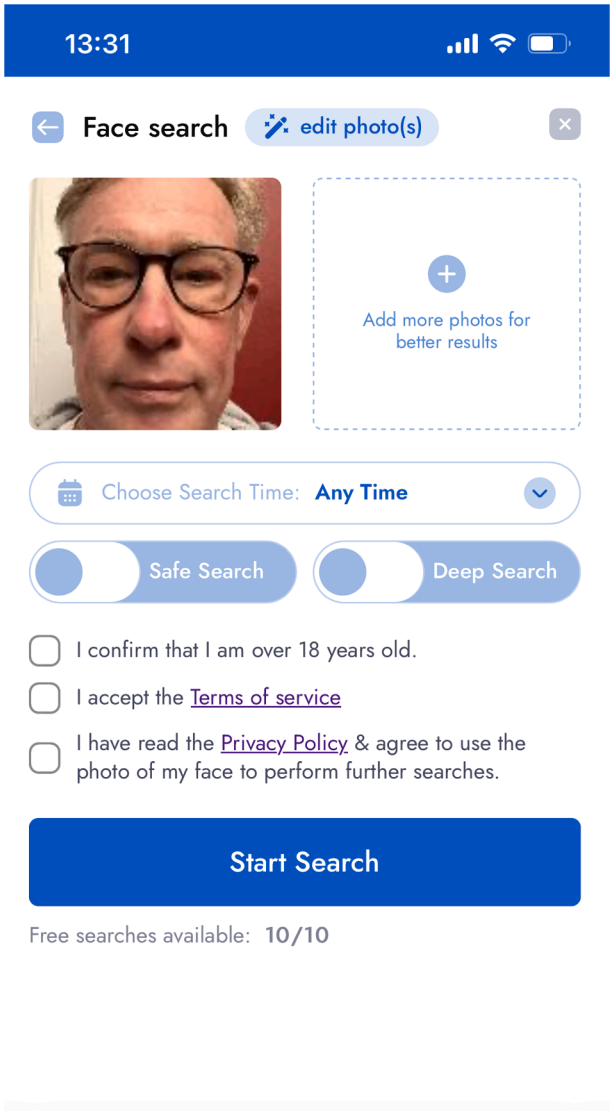


Fig. 2. Image search 1 (of author's face).

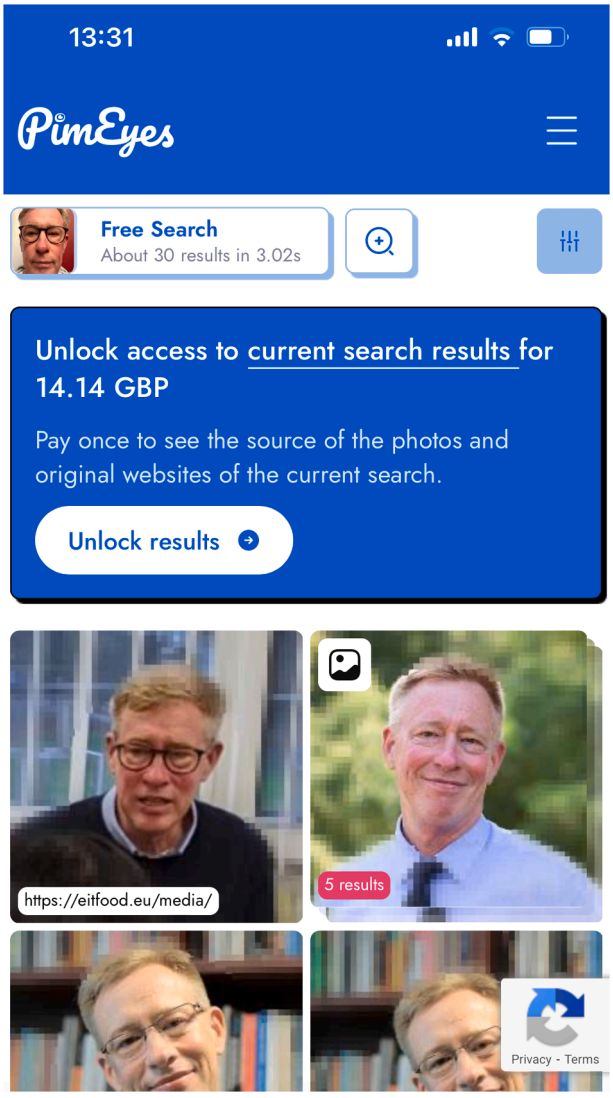


Fig. 3. Image search 2 (of author's face).

whose search results include images that they did not know were available online, especially if they seem to be being used for questionable purposes. Indeed, no matter what images are returned, the user is unable to 'unlock' the results to confirm if they are being used for questionable purposes without paying.

Like the television screens that display the images of jaywalkers in China, the crucial 'discourse in place' for users of this site is their own image looking back at them in a way that is presumably not only visible to them, but also to others. The main difference here is that, rather than being confined to the space of a single screen, the images that PimEyes displays are presented as being *somewhere else* — that is, potentially *out of place,* appearing on websites over which the user has no control and which make them susceptible to (mis)recognition (Sekula, 1986). The only way to remedy this 'mis-placement' of the self, or even to find out exactly where these image are, is to descend further into the 'funnel of commitment'.

Users' narratives of their experiences with PimEyes posted on Reddit often focus on the moment of confronting the potential 'out of placeness' of their faces as pivotal to their decisions to further engage with the site, as illustrated by the examples below:

> While I didn't find any nudes of mine doing this search, I found one very recent public modeling pic, and one picture of me in jail after a DUI. … WILD. I immediately put in a request to hide my images. (r/CreatorsAdvice: 'Pimeyes?')
>
> The picture it matched to was taken in 2015 when I was about 13. … it was posted to a website with the url: us.smutr.com. …. When I search Smutr, there is a porn website …where users can upload their own content including photos. PimEyes won't let me click the link to the photo directly unless I pay $33 (in my currency). (r/RBI: 'An old picture of me as a minor is being used on a strange website')

Even users who have been *mis*-recognised by the program still sometimes feel compelled to purchase a plan, just in case others might similarly mis-recognise them. One user wrote:

> I was REALLY worried, because one of them looked too much like me, so I had to pay to the link and check that it actually had nothing to do with me in the video (r/OSINT: 'Searched for myself on pimeyes and found what looks like my face on pornsites)

Even after the user has paid to 'unlock' their results, they still need to take additional steps to resolve the 'out of placeness' of problematic images. First, they need to remove them from the PimEyes search results so others who use the service won't find them, a step which is only necessary because they have been indexed by PimEyes as a result of their initial search. In order to do this, they must complete an 'opt-out'

request and provide a copy of the image along with an (anonymised) scan of their passport or driver's license, but this will only remove the image from the PimEyes index. If users want help in getting the offending page to remove their image, they need to purchase a PROtect Plan, which is designed to *keep* users engaged with the site by providing them with more than 25 opportunities a day to search using other images as well as alerts when new images matching their face appear on the web. Some users have compared this process to 'legal extortion' (see e.g. data real-lies, 2022; Strathern, 2023), given that users are, 'in essence, paying the same company that uncovered the images to also take them down' (Harwell, 2021: para 32).'The only reason I need PimEyes,' one user tweeted, 'is because PimEyes exists.'.

4.2. Interaction (dis)orders

These accounts of the gradual disempowerment of users as they engage with the discourses in place contrast with the broader Discourses of individual agency that are promoted elsewhere on the site. The 'Frequently asked Questions' page, for instance, claims that the service '*empowers* individuals to conduct image based searches' (emphasis mine), and the company's 'About Us' page declares: 'We believe that everyone has the right to find themselves on the Internet and protect their privacy and image.' On the same page, the company also invokes Discourses of 'democracy' and 'equality':

> We truly believe that it is necessary to democratize facial recognition technology. It should not only be reserved for corporations or governments. We're proud to say that we have helped thousands of ordinary people in finding their illegally used photos and protecting their privacy.

These Discourses of 'rights and responsibilities' help to highlight that when the Scollons (2004) (drawing on Goffman, 1983) speak of 'interaction orders' as parts of sites of engagement, they are invoking not just the sets of rules, rights and responsibilities that adhere to particular sites of engagement, but also norms of interaction that are more generally valued in particular societies. Rawls (1987) points out that there is something inherently moral in Goffman's notion of the interaction order since adhering to norms regarding rights and responsibilities in a particular situation (for instance, not 'jumping a queue') is often associated with broader ideas of social order, civility, and citizenship. In other words, interaction orders are where broader 'social contracts' are instantiated in situated actions. Some interaction orders are governed by taken for granted social roles (such as the roles of parent and child). Others, like the interaction order on this website, need to be discursively constructed through invoking certain familiar social identities and cultural storylines (Davies and Harré, 1990). In this case, the imputation of 'rights' on the site's users, the use of words like 'democratize', and the reference to powerful entities like 'governments and corporations' invoke a storyline about how, in some 'so called democracies', powerful elites are able to violate the rights of citizens because of their access to resources that are not available to 'ordinary' people. These Discourses function to frame the product that PimEyes is offering not just as a public service, but as a way of remedying a 'disordered' set of relationships in society in which individuals are denied their basic rights to protect their privacy but others (corporations, governments) have access to technology that can be used to invade it.

But governments and corporations are not the only or even the main threats constructed for users of this site: they also include 'scammers, identity thieves, (and) people who use your image illegally.' 'Many scenarios exist where your images could end up on the Internet without you knowing' the site tells its users, including someone 'stealing your identity', 'individuals with inappropriate intentions who might exploit [your] photos by posting them on inappropriate websites', and 'revenge porn' — 'a vindictive ex-partner [seeking] retaliation by sharing intimate, nude images of their former boyfriend or girlfriend on various websites.' Such scenarios also constitute 'disordered' interaction orders in which people are infringing on the 'rights' of users as a result of having access to 'resources' (photos) that they should not have access to. Remedying such disorders is ostensibly the main 'use case' for the service, a use case which positions users and the company in a broader relationship of 'victim' and 'protector'.

There are other use cases, and other interaction orders, however, that are less prominent on the site itself, mostly because they fall outside of the (legal) use case the company promotes to legitimise their product. These involve people using the service to search for images of people *other* than themselves, often for the purpose of doxing, abusing or blackmailing them. In fact, there is every indication that this is a common use of the service. The website Similarweb.com (2023), which provides audience analytics for websites, indicates that nearly 80 % of PimEyes's visitors are males, over half between the ages of 18–34, whose top browsing interests are 'Adult' themed sites and 'Computers, Electronics and Technology'. The analysis also shows that 40.47 % of referral sites sending traffic to PimEyes are categorised as 'Adult'. Such referrals also come from message boards and social media sites. Nine of the 25 posts I collected from Reddit mentioned using the site to find images of other people, with some posters offering to help others conduct searches (e.g., 'Will let you use my pimeyes search,' r/OSINT) and 6 of the 20 TikTok videos I watched advise or instruct viewers on using the tool for this purpose.[1]

Strathern (2023: para 23) reports that users of anonymous image boards like 4Chan regularly 'offer out their PimEyes subscriptions for others to use, crowdsourcing the identities of women and searching for explicit photos of them online.' These other sites serve as secondary interfaces through which the very 'scammers, identity thieves and people who use your image illegally' that the site promises to protect users from are brought into the interaction order, not as 'threats', but as *customers*.

To be fair, PimEyes considers the uses promoted on these other sites to be unauthorised, but this is mentioned only a few times on the main site. One sentence in the lengthy 'Manifesto' on the About Us page states: 'PimEyes is not intended for the surveillance of others and is not designed for that purpose.' An item in the 24 item FAQs mentions, 'PimEyes is intended solely for personal use. Pursuant to our Terms of Service, any search pertaining to other individuals is strictly prohibited.' Finally, Section 2 of the Terms of Service itself states:

> User should use the Services solely for private, personal, and legitimate consumer purposes, in accordance with the principles of good manners and etiquette. It is Your obligation to furnish only Your personal photograph. You are obliged to furnish the photograph of a third person (other than You), if it is in compliance with the applicable legal norms.

It is notable that the language used in the Terms of Service (which is the only legally binding language) is significantly vaguer than that offered elsewhere on the site, referring to 'principles of good manners and etiquette' and 'applicable legal norms.' More importantly, it is possible for users to conduct image searches on the site without encountering any of this language, and, as has been noted in a number of legal complaints against the company (see e.g. Big Brother Watch, 2022), users are not required to take any steps to verify that the pictures that they are uploading are of them (though they are required to verify their identity if they want pictures of themselves *removed* from the site).

While these less savoury use cases are not promoted on the site itself, they are discussed extensively in all the media articles about the product that are linked to on the site's homepage via complimentary quotes presented in cartoon callouts (see e.g. Fig. 4). The quote 'PimEyes, a search engine that's handy for reverse image searching and facial recognition,' links to an article in *Vice* (Fermeșanu, 2020) by a woman

[1] See for example https://www.tiktok.com/@twinkdetective/video/7241339293917302062?q=pimeyes&t=1704900525312.

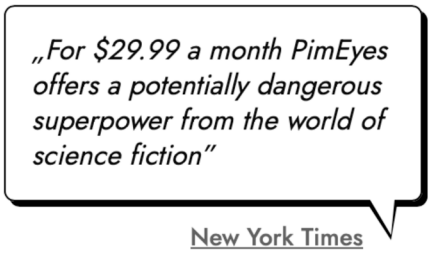


Fig. 4. Link to 'positive' media promoted on the homepage.

who uploaded an image of her mother's would be boyfriend to the site. The quote 'The facial recognition site PimEyes is one of the most capable face-searching tools on the planet' is from a *Washington Post* article (Harwell, 2021) headlined: 'This facial recognition website can turn anyone into a cop — or a stalker' which talks about how the site 'has become a hit among digital "creeps" and others eager to investigate strangers.' And the rather more troubling quote 'For $29.99 a month PimEyes offers a potentially dangerous superpower from the world of science fiction' is linked to a New York Times article (Hill, 2022) which provides a thorough exposé of the ways the service can be abused. In other words, while the company is reticent about these use cases on its own site, it treats as 'positive' media coverage which highlights them. These links provide additional layers to the interface, which further reinforce the use of the site for purposes which the company regards as 'unauthorised'.

Finally, there are interaction orders connected to the interface that are more morally ambiguous, involving users who upload images of people that they suspect of scamming *them*, especially dating site matches and potential 'catfish'. The site is discussed extensively on the r/catfish subreddit (E.g. 'Pimeyes is the ultimate search engine for catfish photos people use' r/catfish) and is also promoted for this purpose on TikTok. A female TikTok influencer who advertises herself as a former New York city police officer, for example, advises her followers to 'stay safe' by using the service to search for the images of romantic partners they have met online.[2]

It is important to note that these different interaction orders that congregate around PimEyes as a site of engagement are not separate, but rather influence one another in significant ways. It is the availability of PimEyes as a surveillance tool for 'scammers', identity thieves and internet trolls that makes it even more 'useful' as a tool for those who might be victimised by such people. In other words, the different interaction orders — 'authorised' and 'unauthorised' – operate in a symbiotic relationship, each reinforcing the other. As one TikToker noted: 'Nice business model…I create a problem and then I charge to solve that problem.'[3].

4.3. Historical bodies

How likely potential users are to be entrapped in this site's 'funnel of commitment' is also determined by the experiences and dispositions that have accumulated in their *historical bodies* over time. These might include experiences of being the victim of revenge porn or catfishing (or having perpetrated such practices), or of hearing the stories of victims that circulate with great regularly in the media and on social media with headlines like "'Catfish' sex predator targeted women with revenge porn texts' (Kirk, 2018). When we consider people's historical bodies as ways in which they 'interface' with technologies, we mostly think about the competencies they have built up in operating the physical and semiotic interfaces of devices and software. What scholars often pay less attention to are the *emotions* that people bring to their experiences with technologies, and how they affect how people engage with them (c.f. Giaxoglou, 2020; Nabi and Gall Myrick, 2023). In the case of PimEyes, an undeniable dimension of this interface is the broader *affective atmosphere* (Anderson, 2009) of dread that has become part of many people's online lives, fuelled by the well documented increases in practices like doxing, cyberbullying and online misogyny (European Parliament, 2021).

What is interesting is how PimEyes itself has quickly become part of this broader Discourse of fear. Media coverage of the site, for instance, prominently features words like 'alarming', 'scary' and 'disturbing', as in the headlines below:

A Face Search Engine Anyone Can Use is **Alarmingly** Accurate (*The New York Times*
Goodbye Privacy: Face Search System is **Alarmingly** Accurate (*Indie Hackers*)
This Facial Recognition Site is **Creeping** Everyone Out (*PC Magazine*)
'Creepy' AI Site Can Find Every Photo of You Online (New York Post)
PimEyes Search-By-Photo **Stalker Scare** (Vaughn Data Systems)
World's Most **Disturbing** Website Can Find Every Photo of You that Exist on the Web (*Mirror*)
How a **Scarily** Accurate Face Recognition Tool Can Cause Privacy Concerns (*TRT World*)

Performances of fearful affect also feature in nearly every one of the TikTok videos about the service that I watched, with influencers saying things like:

'This is personally really spooky…'
'This AI tool is terrifying. What you can do with it is mind blowing'
'This is so unbelievably creepy to me…'
"I've used this website so many times…very creepy I'm not gonna lie'
'Here's the scary website that feels illegal to know'
'This is simultaneously the coolest and the most frightening website I have ever seen…'

In fact, it is hard to find anything about PimEyes online that doesn't talk about how scary it is, and these portrayals of the dangers associated with online image searchers feed into deep-seated feelings about issues like surveillance, sociality, sex, and identity associated with the internet more generally (Hillis et al., 2015). As Ollier-Malaterre's (2023) findings regarding surveillance cameras at Chinese traffic crossings show, these emotional responses can often be complex and contradictory. Just because something seems 'creepy' does not necessarily lead people to avoid it. It sometimes, in fact, can act as an attractor. In 2001, Google CEO Eric Schmidt confessed that one of the company's strategies for creating engaging products was to 'get right up to the creepy line' (Saint, 2010: n.p.). The same might be said of PimEyes: its 'creepiness' is a feature rather than a bug, seducing people to engage with the site out of prurient curiosity or fear that something untoward might be going on with their own online identity.

5. Conclusion

This analysis has illustrated how digital interfaces for surveillance operate not just through their technological and semiotic interfaces, but through dynamic assemblages of discourses, social relationships, and embodied dispositions. When it comes to PimEyes, the key point is the way the different components of the interface *work together* to lure people into surrendering pictures and purchasing expensive monthly subscriptions. The discourses in place on the site funnel users into engaging further with the service through a series of transactions designed to progressively highlight their vulnerability to exposure. As

[2] https://www.tiktok.com/@loveline.911/video/7275872074290384174?is_from_webapp=1&sender_device=pc.
[3] https://www.tiktok.com/@aisavvy/video/7271243636606651649?q=pimeyes&t=1704900525312.

they navigate through these transactions, interaction orders between the site, its users, and the people who may be misusing their images emerge, with users being positioned in sometimes contradictory roles as customers, victims, 'watchers' and 'watched'. Meanwhile, the emotions and experiences users bring to the site in their historical bodies, including both fear and fascination with digital privacy threats, make them more susceptible to further feelings of vulnerability from seeing their own images looking back at them in their search results. Like Foucault's panopticon, where the mere threat of being watched is enough to produce compliant subjects who internalize the gaze of power, PimEyes' interface works to transform people into watchers of themselves, engendering in them a sense of constant exposure and a feeling of responsibility for policing their own visibility.

What is unique (and insidious) about PimEyes is the fact that it operates both as a tool for protecting oneself from surveillance and a tool for conducting surveillance of others, and these two practices exist in a kind of symbiotic relationship: every time a user uploads their picture to the PimEyes database in an attempt to 'protect their privacy', it becomes more likely that others will be able to use the tool to successfully find images of them online.

One way PimEyes legitimises its service is by recruiting a range of Discourses into the interface, invoking notions of democracy and empowerment, protection and care, as well as exploiting narratives of stalking and abuse that circulate online. Another way they legitimise their activities is by rhetorically disaggregating the different components of the interface, pretending for instance that the discourses in place are independent of interaction orders and historical bodies. One example of this is the PimEyes CEO's attempt to escape responsibility for the fact that the tool is used for stalking by insisting, 'the *user* is the stalker, not the search engine' (Meineck and Köver, 2022). Sadly, current privacy laws, which focus on issues of individual consent and personal data, are ill-equipped to address the ways in which sites like PimEyes construct privacy violations as inevitable and necessary. By treating the semiotic elements of the interface (e.g. privacy policies and terms of use), the rights and responsibilities of the actors involved, and the dispositions of individual users as separate issues, such laws fail to account for how these elements work together to enrol people into affective economies of surveillance.

This analysis points to the need for a more holistic approach to digital privacy that goes beyond a focus on individual consent and data protection to consider the broader affective and social dynamics of digital interfaces. Rethinking privacy in an age of facial recognition and other biometric technologies requires attending to the ways in which interfaces produce new subjectivities and social relations, new embodied practices and new 'affective atmospheres' (Anderson, 2009) within which surveillance takes place. The analysis also points to the inadequacies of approaches to the analysis of digital interfaces that see them simply as 'texts' or 'tools' through which people interact with digital technologies. Interfaces are better seen as social practices, or, more specifically, as *nexuses* of practice which make certain kinds of actions, social identities and social relationships possible. A key question for scholars of digital media, then is: what kinds of practices, identities and social relationships are new interfaces powered by AI technologies like facial recognition making possible, and what consequences will these have for our personal and political lives?

CRediT authorship contribution statement

Rodney H. Jones: Writing – review & editing, Writing – original draft, Validation, Software, Resources, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization.

Declaration of competing interest

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

References

Anderson, B., 2009. Affective atmospheres. Emot. Space Soc. 2 (2), 77–81. https://doi.org/10.1016/j.emospa.2009.08.005.

Andrejevic, M., Selwyn, N., 2022. Facial Recognition. Polity Press, Cambridge.

Arntz, P., 2023. October 25. Face search engine PimEyes stops searches of children's faces, 17 December 2023 from *Malwarebytes*. https://www.malwarebytes.com/blog/news/2023/10/face-search-engine-pimeyes-stops-searches-of-childrens-faces.

Bauman, R., Briggs, C.L., 1990. Poetics and performance as critical perspectives on language and social life. Ann. Rev. Anthropol. 19, 59–88.

Big Brother Watch. 2022. Submission to the Information Commissioner request for an investigation into Carribex Lrd. T/A PimEyes unlawful processing of biometric data. Retrieved 17 December 2023 from https://bigbrotherwatch.org.uk/wp-content/uploads/2022/11/20220912-Big-Brother-Watch-Submission-re-PimEyes-AS-SENT.pdf.

Clarke, R., 1988. Information technology and dataveillance. Commun. ACM 31 (5), 498–512. https://doi.org/10.1145/42411.42413.

data real-lies, 2022. Pimeyes is extorting victims of sexual abuse. December 2023 from *Medium* 18. https://data-real-lies.medium.com/pimeyes-is-extorting-victims-of-sexual-abuse-8ceef45299a3.

Davies, B., Harré, R., 1990. Positioning: The discursive construction of selves. J. Theory Soc. Behav. 20 (1), 43–63.

de Seta, G. 2021, December 14. Heikeji 黑科技 ['black technology']. Retrieved 2 January 2024, from AI Now Institute website: https://ainowinstitute.org/publication/heikeji-黑科技-black-technology.

De Souza, E., Silva, A., 2006. From cyber to hybrid: Mobile technologies as interfaces of hybrid spaces. Space Cult. 9 (3), 261–278. https://doi.org/10.1177/1206331206289022.

Djonov, E., van Leeuwen, T., 2017. The power of semiotic software. In: Richardson, J. (Ed.), Flowerdew, J. The Routledge Handbook of Critical Discourse Studies. Routledge, Abington, Oxon, Routledge, pp. 566–581.

Farman, J., 2021. Mobile Interface Theory: Embodied Space and Locative Media, 2nd edition. Routledge, New York.

Fermeşanu, L. 2020, July 8. I put my mum on Tinder and she instantly got catfished. *Vice*. Retrieved 18 December 2023 from https://www.vice.com/en/article/qj4bk3/tinder-catfish-dating-scam-mum.

Foucault, M., 1975. Discipline and Punish: The Birth of the Prison. Random House, New York.

Galloway, A.R., 2012. The Interface Effect. Polity Press, Cambridge, UK, Malden, MA.

Gee, J.P., 2014. An Introduction to Discourse Analysis: Theory and Method, 4th ed. Routledge, New York.

Giaxoglou, K., 2020. A Narrative Approach to Social Media Mourning: Small Stories and Affective Positioning. Routledge, New York.

Goffman, E., 1983. The interaction order: American Sociological Association, 1982 presidential address. Am. Sociol. Rev. 48 (1), 1–17.

Golfman, E., 1963. Behavior in Public Places: Notes on the Social Organization of Gatherings. The Free Press, New York.

Haggerty, K.D., Ericson, R.V., 2000. The surveillant assemblage. Br. J. Sociol. 51 (4), 605–622.

Haraway, D.J., 1991. Simians, Cyborgs, and Women: The Reinvention of Nature. Routledge, New York.

Harwell, D., 2021. May 14. This facial recognition website can turn anyone into a cop—Or a stalker. Retrieved 17 December 2023 from Washington Post. https://www.washingtonpost.com/technology/2021/05/14/pimeyes-facial-recognition-search-secrecy/.

Hayles, N.K., 1999. How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics. University of Chicago Press, Chicago.

Hill, K., 2022, May 26. A face search engine anyone can se Is alarmingly accurate. *The New York Times*. Retrieved 16 December 2023 from https://www.nytimes.com/2022/05/26/technology/pimeyes-facial-recognition-search.htmlu.

Hillis, K., Paasonen, S., Petit, M. (Eds.), 2015. Networked Affect. The MIT Press, Cambridge, MA.

Hookway, B., 2014. Interface. The MIT Press, Cambridge, MA.

Introna, L., Wood, D., 2002. Picturing algorithmic surveillance: The politics of facial recognition systems. Surveill. Soc. 2 (2/3), 177–198. https://doi.org/10.24908/ss.v2i2/3.3373.

Johnson, S., 1997. Interface Culture: How New Technology Transforms the Way We Create and Communicate. Basic Books, New York.

Jones, R.H., 2020. Discourse Analysis and Digital Surveillance. In: Georgakopoulou, A., De Fina, A. (Eds.), The Cambridge Handbook of Discourse Studies. Cambridge University Press, Cambridge, pp. 708–731.

Kirk, T. ,2018, December 6. 'Catfish' sex predator targeted women with revenge porn texts. London Evening Standard. Retrieved 18 December 2023 from https://www.standard.co.uk/news/crime/catfish-sex-predator-targeted-women-with-revenge-porn-texts-a4010436.html.

Kvåle, G., 2016. Software as ideology: A multimodal critical discourse analysis of Microsoft Word and SmartArt. J. Language Politics 15 (3), 259–273. https://doi.org/10.1075/jlp.15.3.02kva.

Manovich, L., 2001. The Language of New Media. MIT Press, Cambridge MA.

Meineck, S., Köver, C., 2022, September 8. PimEyes-CEO: 'The user is the stalker, not the search engine'. *netzpolitik.org*. Retrieved 18 December 2023 from https://netzpolitik.org/2022/pimeyes-ceo-the-user-is-the-stalker-not-the-search-engine/.

Mozur, P., 2018. Inside China's dystopian dreams: A.I., shame and lots of cameras. The New York Times.
Nabi, R.L., Gall Myrick, J. (Eds.), 2023. Emotion and Media Technology: Digital Media Use and Emotional Experience. Oxford University Press, Oxford.
Norris, S., Jones, R.H., 2005. Discourse in Action: Introducing Mediated Discourse Analysis. Routledge, London.
Norval, A., Prasopoulou, E., 2017. Public faces? A critical exploration of the diffusion of face recognition technologies in online social networks. New Media Soc. 19 (4), 637–654. https://doi.org/10.1177/1461444816688896.
Ollier-Malaterre, A., 2023. Living with Digital Surveillance in China: Citizens' Narratives on Technology, Privacy, and Governance. New York, NY, Routledge, Abingdon, Oxon.
Parliament, E., 2021. Combating gender based violence: Cyberviolence. European Union, Brussels.
Rawls, A.W., 1987. The interaction order sui generis: Goffman's contribution to social theory. Sociol Theory 5, 136–149.
Rock, F., 2016. Talking the ethical turn: Drawing on tick-box consent in policing. In: Ehrlich, S., Eades, D., Ainsworth, J. (Eds.), Discursive Constructions of Consent in the Legal Process. Oxford University Press, Oxford, pp. 93–117.
Scollon, R., 1998. Mediated Discourse as Social Interaction: A Study of News Discourse. Longman, London.
Scollon, R., 2001. Mediated Discourse: The Nexus of Practice. Routledge, London.
Scollon, R., Scollon, S.W., 2004. Nexus Analysis: Discourse and the Emerging Internet. Routledge, London.
Sekula, A. ,1986. The Body and the Archive. October 39, 3–64. Doi: 10.2307/778312.
Selfe, C.L., Selfe Jr., R.J., 1994. The politics of the interface: Power and its exercise in electronic contact zones. Coll. Compos. Commun. 45 (4), 480–504.
Similarweb.com, 2023. Pimeyes.com. Assessed 26 December 2023 from https://www.similarweb.com/website/pimeyes.com/#demographics.
Strathern, F., 2023. AI search engine PimEyes facilitates image-based sexual abuse of women… Then sells them the solution. Byline Supplement. https://www.bylinesupplement.com/p/ai-search-engine-pimeyes-facilitates.