# Public faces?

## A critical exploration of the diffusion of face recognition technologies in online social networks

Accepted for publication in: **New Media and Society**

Authors:

Aletta J. Norval
Department of Government
University of Essex
alett@essex.ac.uk

Elpida Prasopoulou
Coventry University
elpida.prasopoulou@coventry.ac.uk

This paper has been funded by the EPSRC, grant number: EP/J005037/1

**Public faces?**

**A critical exploration of the diffusion of face recognition technologies in online social networks***

## Introduction: Framing diffusion

> Initial "governmental" applications for border control and eGovernment services will give way in the future to a wider use of biometrics for commercial and civil applications. We have termed this "the diffusion effect", arising from an increased acceptance of biometric identification by citizens in their dealings with governments (Maghiros et al., 2005: 7).

Over the last decade, we have witnessed a rapid spread of biometric technologies from the security domain to commercial and social media applications. The use of fingerprint scanning to gain access to mobile devices, voice biometrics by banking services, palm vein solutions for access to buildings, and face recognition on social media sites are just some examples of the growing use of biometrics in everyday life. This diffusion has been nurtured globally by governments and the biometrics industry (Stahl, 2011) and is treated as having undeniably positive implications: proponents suggest that the use of

biometrics, "can deliver improved convenience and value to individuals" (Maghiros et al., 2005: 10).

In this article we critically examine the diffusion of biometric technologies, focusing on face recognition. In order to do this, we use Nissenbaum's (2010) framework of contextual integrity to reveal the context-specific informational norms for biometrics in security and policing. In focusing on recent uses of biometrics in social media applications, we extend Nissenbaum's work to the study of how informational norms move and are reshaped across contexts following the diffusion of new technologies. We argue that as face recognition has been iterated over time in wider contexts, the informational norms that have been developed around initial contexts of use – in security and policing - have inadvertently been incorporated into everyday practices, influencing the way users understand biometrics and their wider use. To fully grasp the repercussions of the convergence between Web 2.0 (Braman, 2011), especially social network sites (SNS), and face recognition technologies (FRTs), we analyze the debate around Facebook's use of face recognition software for on-line photo management, seeking to disclose the historically contingent conditions for the use of face recognition. Making these conditions visible, we argue, may enable citizens to see things differently in order to start debating their privacy concerns in a language that will incorporate a broader array of issues than is the case today.

Our approach departs from existing academic accounts of biometrics that treat biometrics as a means of securitizing everyday life (Bigo, 2002). By rendering bodies into easily governable entities (Magnet, 2011), the gaze of the state over its population is expanded, citizens' relationship with the state altered (Agamben 2004:169), and techniques usually reserved for criminals are deployed in the governance of entire populations. Approaches such as these paint a dystopian picture of the uses of biometrics. Based on Foucault's reading of the Panopticon, the paradigm of "surveillance" emphasizes the ever-present state observing our every move. As a result, it ignores shifts in the uses of these technologies and fails to take note of how the diffusion of technology across different contexts, particularly in new media, impacts on the use and meaning of that technology.[1]

The focus on diffusion enables us to explore what happens when norms developed in the contexts of emergence migrate to new contexts of use that lack clearly established rules of transmission for the information generated by new technologies. If meaning is use – as Wittgenstein suggests – we need to be clear about how technologies are used, and how their uses are introduced, understood, argued for and extended to new contexts. We suggest a fine-grained analysis of diffusion that focuses upon the iteration of technologies in different contexts. Iteration here implies both repetition and alteration.[2] In being repeated, in different contexts and in different media, the meanings associated with a particular practice will bear the traces of earlier contexts of use, and

will be altered by being inserted into a new context of use. Starting from the supposition that the meanings and practices associated with a given domain – in this case, face recognition technology - enable those who subscribe to it 'to interpret bits of information and put them together into coherent stories' or narratives that shape, but does not determine further use (Howarth, 2000: 101-2), we reconstructed the horizon of intelligibility (Norval, 2007: 105) accompanying the initial emergence and use of face recognition. To establish the contours of the contexts of emergence, we collected reports on biometrics from the US Department of Homeland Security, the UK Cabinet Office, the Home Office, as well as committees from both UK Houses of Parliament, EU commissioned reports, industry white papers and promotional materials, and think tank reports. We thematically coded (Saldaña, 2009) this material to identify key framings of biometrics in industry and policy publications. We then compared these framings to views expressed and also thematically coded in academic literature and civil society and press reports on biometrics, surveillance, and privacy (Norval & Prasopoulou, 2013). Each theme was populated with representative quotes from our primary material. This methodology also allowed us to identify key actors in biometrics in security, policing and social media, and uncover informational norms governing practices in the contexts of emergence and iteration we examined (Norval & Prasopoulou, 2013). It also enabled us to see how meanings and practices (including

informational norms) are repeated and altered as the technology migrates from security contexts to everyday use in new media.

The framing of FRT in law and regulation, government documents, policy proposals and investigations, as well as their representation in industry outlets matters, for it establishes horizons of intelligibility that set limits to what could be *said* and *done* with them. Once well-established, such horizons incorporate practices of governance that guide conduct and set norms of legitimate use on the one hand, and practices of freedom, questioning and challenging existing rules of the game on the other (Tully, 2008: 23; Griggs, Norval & Wagenaar, 2014).[3] Given this, we analyzed the ways in which existing as well as emerging practices of governance seek to provide shape and give meaning to FRTs. We also investigate the new opportunities for doing things differently that are opened up by their diffusion from one set of contexts to another. This is particularly clear in the use of FRT by Facebook, as it marks one of the first deployments of a technology emerging from a security context in social media.

Our focus on iteration across contexts makes visible important aspects of the repetition and alteration of meanings associated with social practices. It serves as a critical tool to address the circumstances under which iterations become problematic, and provides an important deepening of contextually-driven approaches to privacy. Nissenbaum's work on contextual integrity focuses on breaches in institutionalized practices of transmitting information. It does so by analyzing informational norms in

terms of four key parameters, namely, 'contexts', including "structured social settings characterized by canonical activities"); 'actors', incorporating senders and recipients of information but also information subjects; 'information attributes', describing the types of information in question; and, finally 'transmission principles', which outline the terms and conditions under which information is transmitted from one party to another in a specific context (2010: 132). This approach enables in-depth analysis of privacy norms and accompanying expectations in any social context. It facilitates identification of the roots of bewilderment and protests against new digital technologies in the name of privacy by focusing on alarm caused when contextual norms are violated by new technologies (2010:3). However, it does not account for new social practices emerging with the growing integration of digital media in different walks of life (i.e. contexts) as a result of the diffusion of technologies into new contexts. After setting the scene with a discussion of the contexts of emergence of FRTs, we analyze Facebook's use of the "tag tool" for photo management as a case of iteration in a new context. To this end, we use the key parameters suggested by Nissenbaum in our analysis of the diffusion of biometrics from security and policing to social media. Our intention is to broaden the discussion of contextual integrity by showing how diffusion of new technologies in contexts without settled informational norms can have unacknowledged consequences arising from the initial context in which they emerge.

**Contexts of emergence: Tracing the face**

The face is a site of negotiation (Benjamin, Howard, & Townsend, 2011: 1). There is a long history of normative engagement with the face (Waldenfels 2002: 63-81; Edkins, 2013a; 2013b). However, as Chamayou (2013, footnote 7) argues "beneath the face of a Levinas we occasionally find the face of a Bertillon." Current developments of facial biometrics suggest that this is more than occasionally the case. In what follows we systematically analyze discursive framings of FRT in governmental and industry discourses, so as to be able to understand the particular meanings given to facial biometrics in different contexts and by different actors. It is important to note that these framings are not simply a given set of discrete, isolated statements but rather a discursive horizon that shapes and sets limits to what can be done within a given terrain (author, 2000, 2009). On this account, FRTs are not neutral techniques deployed for the purposes of identity management. Much depends upon the precise meanings attributed to, and practices associated with them (Howarth 2000), by a wide range of actors, including governments, commercial and civil society organizations (Schmidt and Cohen, 2013:56). The framing of facial biometrics in a seminal EU Frontex technical report, entitled "Biometrics for Border Security" is exemplary of much governmental and industry discourse. It traces out what purports to be a "natural" path in the diffusion of facial biometrics:

> The face is the most natural of the biometric modalities and this is how humans recognize individuals in their immediate social environment. This traditional biometric method is performed manually by comparing the actual individual with an image stored in the human brain memory. An extension of this natural identifying process done officially is when a person is identified comparing his face to an image stored in an identifying document (e.g. ID or traditional passport) by some authority. Biometric face recognition works by using a computer to analyse the subject's facial structure... Using all of this information, the program creates a unique template incorporating all of the numerical data. This template may then be compared to very large databases of facial images to identify the subject (Vakalis et al., 2006: 26).

There are a number of key moments of transition in this account of diffusion: the first is the transition from "natural," "original," processes of *recognition*, to the traditional methods of biometric *identification*; and the second from *traditional* to *digitized* biometric face recognition. The narrative structure of the text first encourages the reader to move seamlessly from recognition to identification: from a practice of social and personal interaction, to a bureaucratized, institutional practice of control, instituting new relations between the person (the data subject), image and the agency (here the state) exercising the comparison. The second transition introduces a further complexity: with digitized biometric face recognition, we have not just a comparison of a person with

his/her picture, but the comparison of a template to a number of other templates on a large database (Lips, Taylor and Organ, 2009; Whitley, Gal and Kjærgaard, 2014).

While using the face as a means of identification has many historical precedents (Caplan and Torpey, 2001), the narrative suggests that there is little difference between these practices. Social recognition, identification from a photograph, and identification and comparison by using data templates are treated as mere extensions of "natural processes". Notably, the latter is re-described as a "traditional biometric method" that "is performed manually by comparing the actual individual with an image stored in the human brain memory." Social practices of recognition are thus reduced to a mechanical vision of the performance of the "manual" task of "comparing" "the actual individual" with "an image stored in the human brain memory." The process of turning a person's face into a biometric template is portrayed as analogous to what we do in everyday social interactions: human recognition purportedly is just a practice of judging whether we know a face by comparing measurements and features in our head. The fact that biometric FRTs allows for large scale comparison of templates held on big databases is depicted as a simple further extension of a natural of processes; we are not told to which databases our templates are being compared nor is there acknowledgement of the immense possibilities of tracing that is opened up by turning the face into a machine readable algorithm.

The document further notes the key factors in favor of adopting face biometrics for machine readable travel documents (Vakalis et al., 2006:12):

- Facial photographs only disclose information that the person routinely discloses to the general public;
- The use of a photograph for identification is already socially and culturally accepted;
- It is non-intrusive;
- It does not require new and costly enrollment procedures to be introduced;
- Many countries have a legacy database of facial images captured as part of the digitized production of passport photographs;
- It can be captured from an endorsed photograph, not requiring the person to by physically present, including children;
- For watch lists, the face (photograph) is generally the only biometric available for comparison;
- It generally works when acquiring a facial image by a camera;
- Human verification of the biometric against the photograph/person is relatively simple and a familiar process for border control authorities.

These reasons display both the more general conditions of emergence of the use of biometric technologies in government and industry discourses – particularly the

emphasis on security - and reflect the technical arguments for the uses of biometrics for identification (e.g. Maghiros et al., 2005), emphasizing the historical continuity of face-related identification practices, and framing them as simple technological upgrades (e.g. NSTC, 2006).

A number of dislocatory events, including 9/11 in the USA, Madrid 2004 and the 7/7 London bombings, led to a wider diffusion of biometrics, justified by arguments that biometrics provide security and protection in the post 9/11 world, that it enhances migration control, facilitates economic growth,[4] and ease of movement; and that it contributes to better government services (see Maghiros et al., 2006). Given the ever closer co-operation between governmental organizations and the biometrics industry,[5] it is not surprising that the industry repeats many of the arguments around security. However, there are also notable differences. A shift from security to safety adds an emphasis on technological innovation in addition to the need to safeguard society, secure identity and protect personal data through the body "as the only reliable password" visible in arguments justifying FRTs.

The step-change in the introduction of digitized biometrics is covered over by statements that suggest a simple continuity with normal social practices: we "routinely" disclose our faces to the general public. Disregarding the fact that the "naturalness" of facial biometrics is highly contestable in a multi-cultural context where faces and their presentation in public are deeply politicized, the assumption is that once these steps are

naturalized, the further extension of facial biometrics becomes easier and seemingly obvious. One such further, very significant, change concerns the movement from using facial biometrics to identify individuals and to compare them to watch-lists and other databases, to what is known as "remote biometrics." The argument in "Biometrics for Border Security" continues:

> The technology exists today for cameras to scan a crowd, matching faces against a database of known terrorists and criminals and has many promising applications, including fast, positive identification of airline passengers, access control for personnel, and crowd screening … because a person's face can be captured by a camera from some distance away, facial recognition has a clandestine or covert capability (i.e. the subject does not necessarily know he/she has been observed) (Vakalis et al., 2006: 26).

This argument repeats the security narrative, as well as familiar technical justifications, both of which are familiar tropes in industry and government discourses on biometrics (Cohen, 2012; Accenture 2013). Yet, another twist is introduced: the clandestine uses and covert capabilities of biometrics where the subject is not aware of being observed. Counter to good practice (Biometrics Institute, 2013), this extension seeks to naturalize the use of biometrics without the subject's consent.

The long-standing use of the face in government identity schemes in tandem with a tightly knit argument framing face recognition as imitating normal brain activity

(Safran, 2015) during identification, propelled its development far beyond security and policing applications. The range of commercial and other uses are constantly evolving (see Schmidt and Cohen 2008:38). For many, the most alarming use of FRT is in online social networks (Acquisti et al., 2014). It is for this reason that Facebook is an excellent case to trace how elements of the horizon of intelligibility elaborated by governments and the biometrics industry are reworked when entering everyday life. Its "tag suggestions" tool allows us to explore if and how accepted informational norms are breached, and how this is publicly justified and contested, if at all.

**Contexts of iteration: The use of face recognition by Facebook**

Facebook introduced face recognition to improve the way users manage pictures uploaded on their profiles. The "tag suggestion" tool uses FRT to identify human faces in each picture and suggest names for the user to easily tag them.[6] Indicative of a growing sense of face recognition as something already normalized in social practices Facebook opted for a fast roll-out without discussing the technology that enables tag suggestions; there were no special announcements, just a blog enthusiastically describing the new possibilities opened up by the tool, portraying it as enhancing convenience and improving customer experience by facilitating the curation of digital content:

> Unlike photos that get forgotten in a camera or an unshared album, tagged photos help you and your friends relive everything from that life-altering skydiving trip to a birthday dinner where the laughter never stopped.[7]

Privacy advocates were and remain critical of how Facebook introduced face recognition (see Hargittai, 2010; and Fernback and Papacharissi, 2007: 730).[8] Civil society organizations in the U.S. filed a complaint with the Federal Trade Commission,[9] alleging that Facebook engaged in unfair and deceptive trade practices.[10] Spearheading the complaint, the Electronic Privacy Information Center (EPIC) put it thus:

> Facebook routinely encourages users to "tag," i.e. provide actual identifying information about themselves, their friends, and other people they may recognize. Facebook "associate[s] the tags with [a user's] account, compare what these tagged photos have in common and store a summary of this comparison." Facebook automatically compares uploaded photos "to the summary information we've stored about what your tagged photos have in common." Facebook gave no notice to users and failed to obtain consent prior to collecting "Photo Comparison Data," generating unique biometric identifiers, and linking biometric identifiers with individual users.

In his opening statement to the Fourth US Senate Hearing of the Subcommittee on Privacy, Technology and the Law (2012), Franken (2012) highlighted the issues raised by the use of FRT:

> Once someone has your faceprint, they can get your name, they can find your social networking account and they can find and track you in the street, in the stores you visit … Your face is a conduit to an incredible amount of information about you. And facial recognition technology can allow others to access all of that information from a distance, without your knowledge.

Facebook's response to its critics has been evocative of core arguments in government and industry discourse. Users are assumed not to have objections to the use of biometrics once they find a service useful and enjoyable. As Facebook's Manager of Privacy and Public Policy argued in his testimony to the U.S. Senate (Sherman, 2012):

> Facebook is committed to building innovative tools that enhance people's online experiences while giving them control over their personal information. Our integration of facial recognition technology into tag suggestions on Facebook exemplifies this commitment.

Evoking the idea of privacy-by-design,[11] Facebook positioned the tag-suggestion tool as a service that enhances privacy, encouraging users to disclose data. Users, it argues, are in control of their data and can choose whether they want to be identified in their friends' photos:

> When people share photos on Facebook, our online audience selectors enable them to determine with precision the audience with whom the photos will be shared (Sherman 2012).

Indeed, Facebook's arguments are intelligible *because* they iterate understandings of face recognition methodically developed by governments and the biometrics industry. The idea of innovation, so predominant in Facebook's rhetoric, is central to the diffusion of biometrics (Accenture 2013) and fits perfectly with its corporate strategy of investing in technologies that ostensibly enhances human connectivity.[12]

However, these frames obscure significant privacy-related issues raised by the convergence of FRT and online social networks. It is here that tension arises between informational norms in security uses and social media. As Barocas and Nissenbaum (2014: 47) note, "computing and information technologies have been radically disruptive, allowing information practices that frequently diverge from entrenched informational norms." The capacity to create biometric databases of digitized faces originating from photos uploaded on Facebook, and aggregating this information with data from the users' activity, is a case in point.[13] These digitized faces become a new information type that irrevocably links identity with personal history, setting this application apart from other uses of face recognition. These developments challenge both existing norms around the use of personal photographs, departing from situations in which normally only one's closest friends would know one's activities and preferences, and not in the detail recorded by Facebook, and introducing new information types. They also change existing transmission principles. The tag tool affects the information flow of photographs. Rather than being at the behest of the data

subject (the person uploading the photograph), they now become the object of secondary disclosures (disclosures by others), leading to new privacy – and reputational – concerns (Martin and del Alamo, 2016: 251). Indicative of the unacknowledged consequences and breaches of informational norms, these issues arise from the diffusion of biometric technologies into everyday practices, in the context of societies in which almost every aspect of our lives produce recordable data.[14]

**The unacknowledged consequences of diffusion**

The acquisition of on-line photo sharing sites by large social media companies such as Facebook and Google allowed face recognition to tap into an ever evolving on-line depository of user generated content that is not regulated by governments.[15] Joseph Atick (2011) likens this situation to a perfect storm where unprecedented convergence of several technological developments creates an environment where new kinds of face recognition applications threaten privacy on a very large scale. Given this it is important to reflect on why the biometrics industry treated the diffusion as trivial (Safran, n.d.), but also why, despite legal challenges, users did not reacted against it as strongly as with other FRTs such as Google Glass. It is here that attention to the diffusion of framings from their initial contexts of emergence clearly comes into play. One of the main reasons why this was not foreseen is to be found in the sedimentation of arguments on the neutrality of biometrics that made the biometrics industry myopic to

the controversial combination of face biometrics, social media and large scale use of personal data. This could also explain the privacy paradox (Taddicken 2014): why people use these technologies and disclose personal information despite concerns raised by privacy and civil rights groups, and unease expressed by users (Martin and del Alamo, 2016: 251). It is plausible that user understanding of face recognition is indeed mediated by the available frames, and is being perceived as an automation of practices of identification we "have been doing all along" as suggested in government and industry framings, and that the disclosure of personal information is increasingly seen as a normal part of modern life (Ellias, 2014). Contributing to this line of thought is the rhetoric in favor of privacy-by-design adopted by those involved in the development and use of biometrics (Federal Trade Commission, 2012) ostensibly ensuring that the personal data collected through biometrics is safely stored and not used in contexts other than that in which it was collected. These technologies are framed as rigidly regulated by governments and trade associations to safeguard individual privacy.[16] As a result, users may feel safe to use face recognition in social media, falsely reassured by the idea that benign contexts should not allow for malevolent uses.[17]

However, the Facebook tag tool shows that matters are considerably more complicated than users may assume. Privacy is not safeguarded simply by respecting traditional privacy requirements and practices. As technologies cross contexts, new social practices are developed and it is difficult to trace the direction of these changes

and to develop appropriate new privacy regulations (cf. n.a. 2007, pages 1870-91; Koops, Hildebrandt & Jaquet-Chiffelle (2010-11: 497-561). As Introna and Nissenbaum note, FRT disrupts normalized flows of information "by connecting facial images with identity" and "connecting this with whatever other information is held in a system's database" (Introna & Nissenbaum, 2009: 44). This is why, in the context of social media, attention to informational norms is so important. The critical issue in the case of Facebook is not just whether or not face recognition should be an opt-in service, suggesting an unproblematic incorporation of biometric technology in social media. Central to the case is the convergence of social media, digital photography and biometrics in a rapidly growing database qua archive which is up-for-grabs by anybody. Yet, the transmission principles agreed between Facebook and its users, upon registration to the platform, make no provision for consent to the creation of new information types (biometric databases of photos). The prevailing context of a generalized archive consisting of public images, supplemented by personal photographic archives allowing people to position themselves as they choose (Sekula, 1986), is rapidly being transformed into a public archive where everybody can see everybody. Existing widely-agreed, information types and transmission rules stipulating the use of public and private photographic archives are altered to the extent that quite frequently all the actors involved are not fully known either, yet these fundamental changes in the moral economy of the image as well as its role in identification - formal

and informal – remain unaccounted for in current framings. Face recognition contributes to this change by lifting anonymity from the part of the archive that was previously expected to be private,[18] *making everybody a public face*. As FRT algorithms transform faces into unique data templates, creating new information types, they contribute not only to the success of face recognition in photo management, but to other new uses, such as those associated with remote face recognition. As a result, the identification of faces that can take place even in pictures where faces are not photographed in a standardized way (Sekula 1986), opens up new forms and possibilities of transmission, often without the information subject's consent.

As noted above, not only is the place of the sender and recipient of photographs altered, and with it the prevailing norms of publicity, but new actors and novel, unacknowledged principles of transmission disrupting existing norms of information flows, are coming into being. Every aspect of contextual integrity is altered in some way: the boundaries between existing public and private uses of photographs are altered; information subjects no longer have exclusive control over the dissemination of their images; secondary disclosure and disclosers enter the scene; and data linkages create new information attributes with multiple and unregulated new possibilities of transmission and use. All of these demand new ways to think about and implement privacy-protective practices.

Traditionally questions relating to information recipients and the principles governing the transmission of data, if addressed at all, have been framed through established mechanisms of notice and consent, which are no longer adequate given the possibilities of data moving from one context to another in unacknowledged and largely unregulated ways.[19] Contestation of these new deployments has involved legal action, governmental attempts to regulate the new uses, and some citizen wariness.[20] In the case of Facebook, reactions have focused on the thin conception of user consent (given that it treated the introduction of tagging tools different from privacy policies), not on a deeper questioning of the proportionality of using biometrics to identify one's friends. Equally, trade-offs between privacy and convenience were hardly discussed as Facebook's drawing of an equivalence between privacy and some user control over personal data tended to foreclose this discussion. This point is clearly made by the Center for Technology and Democracy:

> Facebook has stirred up significant controversy with its face recognition tools, in large part because it turned these features on by default ... Users may opt-out of tagging on a photo-by-photo basis, but opting out of the system as a whole is complicated. Given the steps necessary to delete the face print "summary" data associated with each user's account and the fact that Facebook uses persuasive language to try to dissuade users from deleting the data completely, it is unlikely most users would go this far (Lynch 2012).

Despite the limitations of the focus on a thin idea of user consent, and debate about whether privacy laws should focus on preventing the misuse (Mundie 2014), or on limiting the collection and retention of personal data (Cavoukian 2014), the Facebook case triggered efforts to regulate the use of biometrics in social media and relate them to personal data (GAO, 2015). Central to this is the idea of empowering users so that biometrics become part of a *quid pro quo* relationship, where users may consent to have their biometrics collected but they will also demand to be able to revoke them and move to a different digital ecosystem if they think they are not sufficiently protected, or demand the "right to remain anonymous" and to be forgotten, established in EU and Californian law (Hadley 2013; Toobin 2014), as well as a "right of reply" as a mechanism to re-establish control over information about after it has been disclosed (Martin and del Alamo, 2016: 259-62). To assess the degree of protection offered by online social networks, companies will have to become more transparent and open about how they use personal data and which connections they can establish with the information available on user profiles. Such approaches, if adopted, will fundamentally change the way people incorporate biometrics into their everyday lives, emphasizing transparency and accountability on behalf of users. They do require individuals to be more informed and proactive regarding their personal data. While there is some skepticism about to what extent individuals are both able and willing to take on these tasks (Matzner et al, 2016: 280-7), recent research suggest that young adults, for

instance, do care about privacy, and that there is a need to shift the focus of education programs away from a focus only on personal safety, to also include issues around information security and privacy (Hoofnagle et al, 2010: 20) as an individual as well as a social responsibility (Matzner et al, 2016: 302). These findings are confirmed by other studies (Quinn 2013), highlighting the crucial role of digital literacy in active information control online (Park 2011:233). They also corroborate Nissenbaum's (2010: 229) and our approach which positions privacy issues within wider social and other contexts from within which existing norms are affirmed or challenged, altered and modified, and new norms emerge, constructing new modes of interaction. As we show in this article, this approach facilitates an emphasis on the need for citizens to actively develop a context-driven approach to privacy once the diffusion of new technologies across contexts and its consequences are also incorporated into any discussions on privacy.

**Conclusion: Traceability and iteration**

At the outset of this article, we suggested that the analysis of the "diffusion effect" in the case of the extension of biometric technologies from security to everyday contexts is under-developed and insufficiently theorized. We noted several problematic presumptions with existing accounts of this effect:

- The presumption of continuity: both those who are promoting and those critical of biometrics, assume that nothing changes in the diffusion process. It is simply a matter of one and the same technology being transposed from one context to another.
- The presumption that the diffusion effect is uniformly positive, found both in governmental and in industry representations of biometrics.
- The presumption that the biometric technologies that are being diffused, are neutral in character.
- Finally, the presumption that the process of diffusion itself is apolitical in character.

To make visible and address the problems with these presumptions, we have argued that framings of biometric technologies are not neutral, and that they contribute to creating, instituting and maintaining horizons of intelligibility that sets limits to the ways we engage with biometrics. Moreover, we have argued that as biometric technologies move from practices associated with security and policing to the everyday, accompanying discourses are significantly reworked and the meanings of practices are re-signified in important ways.

To fully understand diffusion, we have argued, it is necessary to treat it as an *iterative* practice, where alteration is an integral part of every repetition. Contrary to extant views, context here matters in two senses. On the one hand, we have argued that contexts of emergence need to be analyzed, as they shape our understandings and uses

of biometrics. On the other hand, contexts of iteration are equally important as the technology is repeated in contexts and media that are different from the initial use. Hence, to expect that technologies will seamlessly carry over from one context to another is foolish. To capture contexts of emergence, we analyzed the justifications deployed to promote the introduction of biometrics, focusing on securitization and economic growth. Nevertheless, these framings ignore the significant changes biometrics introduce in the relation between state and citizen, as well as in the relations between bodies and technologies, described by Amoore (2006: 338) as the "ubiquitous" deployment of the biometric border. Turning to the wider contexts of iteration, particularly in industry usage, we found a similarly complex picture: there are some aspects of the original framing of biometric technologies that carry over to industry representations, but others do not. Continuities compete with discontinuities. Accompanying a shift from security to safety is a view of biometrics, not as tool for the state to observe and govern the population, but as a positive and much needed tool to be used by citizens in their everyday life. This is one clear example of the fact that iteration introduces the potential for change, and for doing different things with what seems to be the "same" technologies.

It is precisely in this respect that much of the literature on biometrics fails: analysts do not take cognizance of the fact that the diffusion of biometrics exceeds security contexts. If they do, they are blinded by the assumption that the context of

emergence is dominant and remains so, despite an altered context of use. That is, while it is true that there is an ongoing "securitization" of everyday life, there is more to diffusion than this. If limited to the assumption of the dominance of the initial context of emergence, the strongly dystopic arguments look correct: our lives are increasingly securitized, and we have little if any choice in the matter. We live in a surveillance state and have become mere docile bodies.

As we have argued, the situation is considerably more complicated and, as a result, potentially promising for citizen rights. This is apparent in our discussion of facial biometrics. The introduction of FRT in Facebook took advantage of a horizon of intelligibility strongly representing biometrics as technological tools at the service of everyone. As a result, it circumvented questions regarding the necessity for such technologies in social media, especially as content management tools. Nonetheless, the introduction of biometrics without the explicit consent of users, a common practice in security contexts, sparked awareness of the diffusion of biometrics, produced as a result of a "clash of contexts" (Nissenbaum, 2010: 224). As civil society organizations contested the way biometrics is diffused, they also challenge elements of the horizon of intelligibility. Most importantly, the proposed solutions call into question deep-seated assumptions regarding this particular technology, seeking to empower citizens by demanding more control over personal data. Given the iterative nature of diffusion, it is possible that the newly emerging practices will leak back to the original contexts of use,

mainly security, allowing for a more transparent and controlled use of biometrics by citizens.

The justifications and representations of biometric technologies, in all their forms, institute ways of thinking and doing things that seek to govern conduct: the conduct of those deploying them, as well as the conduct of those who use biometrics. Perhaps the most important shift in this regard is one that we can only glimpse at present: a shift from what has been called "societies of surveillance" to "societies of traceability." The former corresponds well to the view that we live in panoptic societies, where there is an ever-present state observing our every action and utterance. The recent revelations about the US' PRISM and the UK's 'Mastering the Internet' programs seem to confirm this view. We would, however, do well to reflect more closely on the shift in the uses of biometrics, and the fact that they now are tools that are used, not by states, but by individuals; not in hierarchical relations of surveillance, but in horizontal relations of traceability (Chamayou, 2013). What is interiorized through habitual diffusion in each case is different. In the case of societies of surveillance, we focus on the fact of being observed, while in societies of "dataveillance" the focus is on the traceability of people and of things. Face-tagging is but one such an example. As Chamayou (2013) puts it, "automatic recording apparatuses" are "integrated into the activity itself, every material flow now being coupled with a production of a flow of

data." In this context, traceability "consists in organizing within the present the future capability of rereading the past" (Chamayou, 2013).

The question of the nature of diffusion is not one that can be treated in isolation from these monumental changes accompanying the digitization of life through new media. These processes, while they continue to be available to scrutiny from above, also institute a wide range of new relations between citizens, things, media organizations and institutions, captured in large part by attention to "information flows". What we are certain of, is that every diffusion involves new affordances. We ignore this at our peril. This is particularly clear when we give attention to how informational flows are altered, and accepted norms and practices challenged by the diffusion of new developments around technologies such as face recognition and its deployment in online social networks as well as in wider spheres of public life. Attention to changes in information flows will alert us to areas of possible controversy, where the public as well as civil society groups will play an increasingly important role in developing mechanisms for understanding and responding to an increasingly complicated network of activities that affect our lives and the uses made of personal data. There is a long way to go before users are entitled to know what data are being collected about them, by whom and for what purposes, and for which they can give authorization in an informed fashion.[21]

**References**


Accenture https://www.accenture.com/gb-en/insight-biometrics-2013-checkpoint-future-video (accessed 11 August 2016).

Accenture (2012) Improved homeland security management and biometrics through the US-VISIT program. Available at: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-US-Department-of-Homeland-Security-Improved-Homeland-Security-Management-and-Biometrics.pdf (accessed 15 January 2014).

Accenture (2014) Protecting public safety. Available at: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Protecting_Public_Safety.pdf (accessed 10 February 2014).

Acquisti A, Gross R and Stutzman F (2014) Face recognition and privacy in the age of augmented reality. *Journal of Privacy and Confidentiality* 6(2): 1-20.

Agamben G (2004) Bodies without words. *German Law Journal* 5(2): 168-169.

Allevate http://allevate.com/index.php/about (accessed 11 August 2016).

Atick JJ (2011) Face recognition in the era of the cloud and social media. *Security News*. Available at: www.ibia.org/download/datasets/929/Atick%2012-7-2011.pdf (accessed 26 March 2014).

Barocas S and Nissenbaum H (2014) Big data's end run around anonymity and consent. In: Lane J, Stodden V, Bender S and Nissenbaum H (eds) *Privacy, Big Data and the Public Good*. New York, Cambridge University Press, pp. 5-43.

Benjamin A, Howard M and Townsend C (2011) Informed faces. *Angelaki 16*(1): 1-3.

Bigo D (2002) Security and immigration. *Alternatives 27*(Special Issue): 63-92.

Biometrics Institute (2013) Privacy guidelines. Available at: http://www.biometricsinstitute.org/data/Privacy/BiometricsInstitute_BIOEMETRICS_GUIDELINES_V1.pdf (accessed 8 May 2015).

Braman S (2011) Privacy by design: Networked computing, 1969-1979. *New Media & Society* 14(5): 798-814.

Caplan J and Torpey J (eds) (2001) *Documenting Individual Identity*. Princeton: Princeton University Press.

Cavoukian A (2014) Data minding. *Foreign Affairs* (September/October).

Chamayou G (2013) Fichte's passport. *Theory & Event 16*(2).

Clarke R (1988) Information technology and dataveillance. *Communications of the ACM 31* (5): 498-512.

Cohen JE (2012) *Configuring the Networked Self*. New Haven: Yale University Press.

Derrida J (1977) *Limited Inc*. Evanston, Illinois: Northwestern University Press.

Digital Captapult (2014) Trust in digital data. Available at: http://www.digitalcatapultcentre.org.uk/personal-data-trust-report-download/ (accessed 18 September 2015).

Edkins J (2013a) Still face, moving face. *Journal of Cultural Research 17*(4): 414-429.

Edkins J (2013b) Dismantling the face. *Environment and Planning D*, 31(3): 538–553.

Elias P (2014) A European perspective on research and big data analysis. In: Lane J, Stodden V, Bender S and Nissenbaum H (eds) *Privacy, Big Data and the Public Good*. New York, Cambridge University Press, pp.173-191.

Electronic Privacy Information Center. Facebook Privacy. Available at: https://epic.org/privacy/facebook/ (accessed 8 May 2015).

Federal Trade Commission (2012) Facing facts. Available at: https://www.ftc.gov/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies (accessed 15 June 2014).

Fernback J and Z Papacharissi (2007) Online privacy as legal safeguard. *New Media & Society* 9(5): 715-734.

Franken AI (2012) What facial recognition technology means for privacy and civil liberties. Statement to the United States Senate Judiciary Committee Subcommitee on Privacy, Technology, and the Law. Available at: https://www.gpo.gov/fdsys/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf (accessed 12 December 2015).

Government Accountability Office (2015) Facial recognition technology. http://www.gao.gov/assets/680/671764.pdf (accessed 28 November 2015).

Greenwood D, Stopczynski A, Sweatt B, Hardjono, T and Pentland A (2014) The New Deal on data. In: Lane J, Stodden V, Bender S and Nissenbaum H (eds) *Privacy, Big Data and the Public Good*. New York, Cambridge University Press, pp. 192-210.

Griggs, S., Norval, A.J. and H. Wagenaar (2014) *Practices of Freedom: Decentred Governance, Conflict, and Democratic Participation.* Cambridge: Cambridge University Press.

Hadley, ME (2013) California gives its teens the right to be forgotten. *Caveat Vendor.* Available at: http://www.paulhastings.com/publications-items/blog/caveat-vendor/2013/09/30 (accessed 27 January 2015).

Hargittai, E (2010) Facebook privacy settings. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/rt/printerFriendly/3086/2589 (accessed 5th February 2016).

HIDE (2009) Ethical brief in technology convergence. Available at: http://www.hideproject.org (accessed 10 February 2014).

Hoofnagle C, King J, Li S and Turrow J (2010) How different are young adults from older adults when it comes to information privacy attitudes & policies?

Howarth, D (2000) *Discourse*. Buckingham: Open University Press.

Introna, L and Nissenbaum, H (2009) Facial recognition technology. Center for Catastrophe Preparedness and Response (CCPR), New York University.

Koops BJ, Hildebrandt, M and Jaquet-Chiffelle, DO (2011) Bridging the accountability gap. *Minnesota Journal of Law, Science & Technology 11*(2): 497-561.

Lips M, Taylor JA and Organ J (2009) Identity management, administrative sorting and citizenship in new modes of government. *Information, Communication & Society 12*(5): 715-734.

Maghiros I, Punie Y, Delaitre S, Lignos E, Rodríguez M, Ulbrich M, Cabbera M, Clements B, Beslay L, and Van Bavel R (2005) *Biometrics at the Frontiers*. Institute for Prospective Technological Studies. Technical Report EUR 21585 EN. http://ftp.jrc.es/EURdoc/eur21585en.pdf (accessed 10 May 2014).

Magnet S A (2011) *When Biometrics Fail*. Durham: Duke University Press.

Martin Y-D and del Alamo J M (2016) Forget about being forgotten. In: Gutwirth S, Leenes R and De Hert P (eds) *Data Protection on the Move*. Netherlands: Springer, pp. 249-75.

Matzner T, Masur P K, Ochs C & von Pape T (2016) Do-it-yourself data protection. In: Gutwirth S, Leenes R and De Hert P (eds) *Data Protection on the Move*. Netherlands: Springer, pp. 277-305.

Mundie G (2014) Privacy pragmatism. *Foreign Affairs* (March/April).

n.a. (2007) In the face of danger: facial recognition and the limits of privacy law. *Harvard Law Review 120*(7): 1870-1891.

National Science and Technology Council (2006) *Face Recognition*. Subcommittee on Biometrics. http://www.biometrics.gov/Documents/FaceRec.pdf (accessed 8 May 2015).

Nissenbaum H (2010) *Privacy in Context.* Stanford, CA: Stanford University Press.

Norval, A.J. (2000) The things we do with words. *British Journal of Political Science* 30: 313-46.

Norval, A.J. (2007) Aversive Democracy. Inheritance and Originality in the Democratic Tradition. Cambridge: Cambridge University Press.

Norval, A.J. (2009) 'No Reconciliation without Redress': Articulating political demands in post-transitional South Africa'. *Critical Discourse Studies* 6 (4): 311-21.

Norval, A.J. and Prasopoulou, E. (2013) In search of citizen engagement: Examining representations of biometrics in government and industry discourses. Paper presented to the annual IPA conference, Vienna, 3-6 July.

Park, Y J (2011) Digital literacy and privacy behaviour online. *Communication Research* 40(2): 215-36.

Safran (n.d.) Automatic facial recognition. Available at: www.morpho.com/IMG/pdf/facial_recognition-2.pdf (accessed 10 January 2014).

Saldaña J (2009) *The Coding Manual for Qualitative Researchers*. London: Sage.

Schmidt E and Cohen J (2013) *The New Digital Age*. London: John Murray.

Sekula A (1986) The body and the archive. *October* 39(Winter): 3-64.

Sherman R (2012) Statement to the United States Senate Judiciary Committee Subcommittee on Privacy, Technology, and the Law. Available at: https://www.gpo.gov/fdsys/pkg/CHRG-112shrg86599/pdf/CHRG-112shrg86599.pdf (accessed 12 December 2015).

Stahl BC (2011) IT for a better future. In: Von Schomberg R (eds) *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*. Luxembourg: Publications Office of the European Union, pp. 18-33.

Steel E (2011) A face launches a 1,000 apps. *Wall Street Journal*. Available at: http://www.wsj.com/articles/SB10001424053111903885604576488273434534638 (accessed 13 May 2015).

Strong C (2015) Private Lives? *The Market Research Society*. Available at: https://www.mrs.org.uk/pdf/private%20lives.pdf (accessed 12 December 2015).

Taddicken, M (2014) The 'privacy paradox' in the social web. *Journal of Computer-Mediated Communication* 19(2): 248-73.

Toobin J (2014) The solace of oblivion. *The New Yorker.* 2014/09/29.

Tractica (2015) Biometric Markets Forecast 2015. Available at: https://www.tractica.com/research/biometrics-market-forecasts/ (accessed 8 May 2015).

Tully J (2008) *Public Philosophy in a New Key*. Volume I. Cambridge: Cambridge University Press.

Vakalis I, Hosgood B and Chawdhry P (2006) Biometrics for Border Security. EUR 22359 EN. Frontex - Joint Research Unit.

Waldenfels B (2002) Levinas and the face of the other. In: Critchley S and Bernasconi R (eds) *The Cambridge Companion to Levinas*. Cambridge: Cambridge University Press, pp. 63-81.

Whitley EA, Gal U and Kjærgaard A (2014) Who do you think you are? *European Journal of Information Systems 23*(1): 17-35.

Zimmer M (2008) The gaze of the perfect search engine. In Spink A and Zimmer M (eds) *Web Search. Vol 14.* Berlin: Springer, pp. 77-99.

*We would like to thank the anonymous reviewers for their insightful comments on this article.

This paper has been funded by the EPSRC, grant number: EP/J005037/1

[1] Introna and Nissembaum (2009) is a notable exception to surveillance-driven approaches.

[2] "Iteration" is understood in the Derridean sense, as a practice of repetition that involves a degree of alteration in every repetition (Derrida, 1977).

[3] Governments and transnational institutions, industry and civil society organizations all engage in practices of governance, referring to "the way in which the conduct of individuals or groups might be directed" (Tully, 2008: 124).

[4] Tractica (2015) predicts the global biometrics market in consumer device authentication, mobile banking and IT systems to be worth $14.9 billion by 2024.

[5] Accenture (2012) built the Department of Homeland Security US-VISIT program. Allevate similarly works closely with law-enforcement, intelligence and government agencies.

[6] Once photos are uploaded, the software recognizes human faces and biometric templates are created and stored, allowing Facebook to suggest names for people in the photos by comparing their faces with the stored biometric templates. https://www.facebook.com/help/www/124970597582337 (Accessed June 23, 2013).

[7] https://www.facebook.com/blog/blog.php?post=467145887130

[8] For a timeline of Facebook's privacy policy and legal actions against it, see https://epic.org/privacy/facebook/ (Accessed May 8, 2015).

[9] These include the Electronic Privacy Information Center, the Center for Digital Democracy, Consumer Watchdog, and the Privacy Rights Clearinghouse.

[10] For detail on the complaint, see: https://www.epic.org/privacy/facebook/facebook_and_facial_recognitio.html (Accessed December 8, 2013).

[11] "The … future of privacy cannot be assured solely by compliance with … regulatory frameworks; … privacy assurance must … become an organization's default mode of operation." https://www.privacybydesign.ca/index.php/about-pbd (March 26, 2015).

[12] Facebook's founder's Letter to Shareholders: http://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm. (February 10, 2014).

[13] Facebook recently changed its data policy, allowing it to track users across the Web. (https://www.facebook.com/about/privacy/update/; Accessed May 23, 2015)

[14] We use the term 'unacknowledged' rather than 'unintended' consequences since companies consciously seek to extend their capacity to mine personal data, yet this remains unacknowledged.

[15] U.S. Senator Franken notes: "In 2010, Facebook enrolled its then-800 million users into its facial recognition program, Tag Suggestions … Over the past three years, Facebook has leveraged its … billion-strong user base - and its library of 220 billion photos - to build a truly extraordinary database of faceprints." https://www.franken.senate.gov/?p=press_release&id=2554 (Accessed May 22, 2015)

[16] Only a third of Europeans "are aware of the existence of a national public authority protecting their rights regarding personal data" (Elias, 2014: 181). Nevertheless, as people become more conscious of the uses of personal data there is evidence of growing disquiet. For instance, 76% of respondents to an UK survey recorded concern about a lack of control over how and with whom personal data is shared (Digital Catapult, 2015: 8).

[17] Hoofnagle *et al* (2010:4) notes that high proportions of 18-24 year olds 'believe incorrectly that the law protects their privacy online and offline more than it does.'

[18] "Private" here refers to the reasonable expectation that photographs will be available only to a limited range of one's friends, as determined by one's Facebook privacy settings.

[19] Traditional privacy policies are too complicated and lengthy for the ordinary user to make sense of data sharing in the age of big data (Strandburg, 2014). As Barocas and Nissenbaum (2014, 57, 59) note, online privacy policies "offered to individuals as

unilateral terms-of-service contracts (often dubbed … 'notice and consent')" tend to turn privacy questions into matters of "mere" implementation, not acknowledging that "informed consent *itself* may no longer be a match for the challenges posed by big data" because data moves from place to place and recipient to recipient in unpredictable ways. Both notice and consent need to be reworked and contextualized against the backdrop of legitimate expectations.

[20] A class action in Vienna courts followed a similar complaint brought by Schrems against Facebook Ireland Ltd. See http://www.europe-v-facebook.org/report.pdf (Accessed June 4th, 2015).

[21] Greenwood et al (2014: 201) calls this "living informed consent".