Visual Digital Data, Ethical Challenges and Psychological Science

Mark Levine, Richard Philpot, Sophie Nightingale and Anastasia Kordoni

Department of Psychology, Lancaster University, United Kingdom

Accepted manuscript (to be published in *American Psychologist**)

Author Note

Correspondence concerning this article should be addressed to Mark Levine,

Department of Psychology, Lancaster University LA14QY.

mark.levine@lancaster.ac.uk

This work was supported by the Engineering and Physical Sciences Research Council [Citizen Forensics - EP/R013144/1,EP/R033862/1] and the UK Research and Innovation (UKRI) through the Trustworthy Autonomous Systems (TAS) programme [EPSRC Ref: EP/V026747/1]

We have no conflicts of interest to disclose

Abstract

Digital visual data affords psychologists exciting research possibilities. It becomes possible to see real-life interactions in real time, and to be able to analyze this behavior in a fine grained and systematic manner. However, the fact that faces (and other personally identifying physical characteristics) are captured as part of these data sets, means that this kind of data is at the highest level of sensitivity by default. When this is combined with the possibility of automatic collection and processing, then the sensitivity risks are compounded. Here we explore the ethical challenges that face psychologists wishing to take advantage of digital visual data. Specifically, we discuss ethical considerations around data acquisition, data analysis, data storage and data sharing. We begin by considering the challenges of securing visual data from both public space security systems and from social media sources. We then explore the dangers of bias and discrimination in automatic data processing, as well as the dangers to human analysts. We set out the ethical requirements for secure data storage, the dangers of 'function creep' and the challenges of the right of the individual to withdraw from databases. Finally, we consider the tensions that exist between sensitive visual data that require extra protections and the recent open science movement, which advocates data transparency and sharing. We conclude by offering a practical route map for tackling these complex ethical issues in the form of a Privacy and Data Protection Impact Assessment (PDPIA) template for researchers.

Keywords: Digital visual data, ethics, Belmont principles, privacy and data protection

Public Significance Statement

Digital visual data affords psychologists with many exciting research possibilities – but is data of the highest level of sensitivity by default. This paper explores the ethical challenges around data acquisition, data analysis, data storage and data sharing for psychologists using digital visual data in research. We conclude by offering a practical route map for tackling these complex ethical issues in the form of a Privacy and Data Protection Impact Assessment (PDPIA) template for researchers.

In this paper we explore ethical issues that arise from the use of digital visual data in psychological research. We build on recent writings about the application of the Belmont principles for psychological science in the age of big data (see for example, Paxton, 2020). Our particular focus is on digital visual data – a form of data that is becoming more ubiquitous. By digital visual data we mean not only digital images captured in the form of pictures (Cromey, 2012), but also the filming of 'live action' by technologies like public space CCTV cameras (Philpot et al., 2020), smartphones (Weenink et al., 2022), head mounted video cameras (Pink, 2015), body worn cameras (Friis et al., 2020), motor vehicle dash cameras (Turner et al., 2019), drones (Fysh & Bindemann, 2018), home security cameras (Frascella, 2021) and other forms of social media film-based content creation (Legewie & Nassauer, 2018).

While digital visual data carries many of the same ethical challenges as other forms of 'big or naturally occurring data sets' (BONDS: Paxton & Griffiths 2017) there are some specific concerns that those using digital visual data need to address. In particular, any data which might capture a person's face, or other visual representation of the individual, is clearly sensitive data. When this is combined with the possibility of automatic processing of such data, then the sensitivity risks are compounded. When the method of data capture can happen without the knowledge (let alone the consent) of the individual, then the ethical challenges of using such material in research are extremely complex. Our paper explores these ethical challenges; from data acquisition, to data storage, to data processing, to data sharing.

In doing so we draw on the distinction between 'hard ethics' and 'soft ethics' proposed by Floridi (2018). For Floridi, hard ethics precedes and contributes to the shaping of legislation. Soft ethics applies after compliance with the law. Floridi writes that any legislative framework "indicates what the legal and illegal moves in the game are, so to speak, but it says nothing about what the *good* and *best* moves can be, among those that are legal, to win the game, that is, to have a better society" (Floridi, 2018, p. 4 *emphasis in original*). We propose therefore that, when it comes to decision making in the context of technological innovation, legal compliance is not a sufficient framework for guiding ethical practice in service of a better society. To that end we offer a practical route map for tackling these complex ethical issues in the form of a Privacy and Data Protection Impact Assessment (PDPIA). Our PDPIA draws from the Privacy Impact Assessment (PIA) and the Data Protection Impact Assessment (DPIA) that have been developed under European Union General Data Protection Regulations (GDPR). The PDPIA asks researchers to consider both hard and soft ethical considerations as part of the ethical review process for the use of digital visual data. We present a PDPIA template for those interested in digital visual data in psychological research – osf.io/5pex7. This template is freely available under the CC-By Attribution 4.0 International license and can be easily populated by researchers, forming the basis for data sharing agreements, research consultations and ethics board applications.

1. The Early Use of Visual Data in Psychological Research

Visual data has been important for theory development in the human sciences in general (Darwin, 1872/1999) and psychology in particular (Richards, 2002). However, when considered against the range of data types generated in psychology, visual data has historically been a poor relation Despite some early interest. in filming naturalistic settings for research purposes (c.f. Lewin’s hidden camera films of child development spaces in the 1930s (van Elteren & Luck, 1990)), an increasing emphasis on laboratory-based experimentation meant that the potential for visual technologies to capture social interaction in real-life (i.e., using photography or video cameras) was never really developed as a method. Influential psychologists like Milgram (1963) and Zimbardo (Haney et al., 1973) were more interested in the visual medium as filmmakers (i.e., using films as a way to craft the presentation of ideas) rather than as a technology or method for primary research (Millard, 2022; Reavey & Prosser, 2012).

The use of visual data in psychology was not completely absent, however. There is a strand of more qualitative work, beginning in the 1990’s, that used photographic cameras to do both image elicitation and image production for research purposes (Reavey, 2011). In these studies, research participants are either shown still images, or asked to photograph their own images, which are then used as prompts in interview studies (or occasionally analyzed in their own right (see Radley, 2010)). However, the primary focus is usually on analyzing talk or text rather than on the images themselves. Other social science disciplines, like anthropology (Banks & Jay, 2011) and sociology (Evans & Hall, 1999), have been more adept at both embracing and developing an analytic toolkit for visual data analysis. Here too, the approach has typically been qualitative rather than quantitative.

2. The New Digital Visual Landscape

Over the last 20 years, however, the picture has begun to change. The development of new digital visual technologies, and the percolation of different kinds of visual data capture into almost all areas of daily life, has changed the landscape for the potential of visual data. For example, public spaces in almost every town and city are now monitored by (CCTV) camera systems; smartphone cameras are constantly used to record snippets of everyday life which are then shared on social media platforms; workers in public-facing occupations (e.g. police, emergency services, ticket collectors, door staff) now routinely use body-worn cameras to record their interactions with the public; drivers, motorcyclists and cyclists use dash-cams and head-mounted person video cameras to record their movement through the traffic; security-concerned citizens install private doorbell cameras that also capture the public spaces outside their houses; the development of drone technologies means that both ordinary citizens and emergency services now have the capacity to fly cameras over almost all public and private space. All of this new technology means that a digital visual record of human life is now being created in a way that has never been possible before. The fact that this digital data can easily be recorded, stored and revisited means that the images themselves are available for analysis (and re-analysis) in ways that allow detailed study of complex and rich interactions.

At the same time, the growth in computing power and an increasing sophistication in analytic tools, has meant the rise of more quantitative approaches to the analysis of visual data. The application of artificial intelligence and machine learning techniques to still images (Li et al., 2020) and moving images (Sreenu & Saleem, 2019) has transformed what is possible in the automatic analysis of digital visual data. There is now a significant literature on automatic face detection (Jaquet & Champod, 2020), automated gait analysis for biometric identification (Kumar et al., 2021), automated analysis of 'anomalous' behavior in public spaces (Nyak et al., 2021), and automated analysis of behaviors in crowds (Sreenu & Durai, 2019). This is part of a wider technological turn with the potential for profound impact in all areas of human life including crime (Arrigo & Sellars, 2021), health and welfare (Iverson & Rehm, 2022) and democracy and freedom (Diamond, 2019). The ethical implications of this confluence of the availability of digital data and the new types of analytic tools are equally pertinent for the discipline of psychology. In what follows, we will explore the ethical challenges facing psychologists who seek to leverage this type of digital visual data.

3. Ethical Challenges in Visual Data Acquisition

3.1 Repurposed digital visual data

One of the primary sources of digital visual data for psychological analysis is the material that is collected by cameras located in public spaces for the primary purpose of crime prevention. These systems are often installed and owned by town, city or county councils and are governed by a variety of local and national guidance and legislative frameworks, depending on geographical area and jurisdiction. They can also include CCTV systems that are owned and managed by organizations responsible for the security of national infrastructure (e.g., transport hubs, national monuments, stadiums). In some countries (like China and Russia) the CCTV infrastructure has much stronger state control and direct management than in others (like the US or UK). In fact, the increasing privatization of public spaces in many countries means that commercial companies often control the majority of public space CCTV systems.

Therefore, the first ethical challenge to be faced when considering the potential use of CCTV footage for research is **the question of who owns the existing system** – **and for what purpose is the data being collected**. Most publicly owned systems are already governed by a set of rules which determines with whom data might be shared and under what conditions. Very often there is a clause that allows limited data sharing for the purposes of research – for example, to improve the management of health and safety incidents. So, it is usually a requirement of access to the data that researchers can satisfy conditions of privacy and anonymity of individuals in the data, data handling agreements and data security. However, the ethical considerations go beyond the question of satisfying conditions of access, to considering whether working with the data itself involves ethical challenges. If the primary reason for data collection can be considered to be unethical (e.g., surveillance of a population for the purpose of systematic discrimination) then secondary analysis of that data might be considered ethically problematic. The same is true if the data was provided by an organization which did not provide reasonable steps to inform individuals that they were being surveyed.

A second and more recent source of public space digital visual data comes from the increasing use of body-worn cameras by emergency services (and other workers) who interact with the public as part of their duties, for example, police officers, paramedics, ticket wardens. These cameras are usually worn on the chest or head and capture a view of the people that the camera wearer is interacting with. They provide a different type of digital visual record to CCTV in that they only offer a view of what is directly in front of the camera (rather than a birds-eye view), but they do (usually) record sound, unlike CCTV. The cameras themselves are also typically activated by the wearer, in terms of when they are turned on/off, and access to the footage is controlled by the service to which the camera wearer belongs. As with CCTV footage, the ethical questions with body camera footage turns on **who controls access to the footage and what the rights and expectations of the people captured in the footage might be (as well as the rights of the service workers** who wear the cameras). A case needs to be made about the balance between the rights and expectations of all those in the footage and the public benefit that might result from being able to access and analyze such footage.

A third (and emerging) source of digital visual data is that provided by the deployment of drones. Drones are increasingly deployed for law enforcement and policing activities (Sakiyama et al., 2017), global environmental monitoring (Vargas-Ramírez & Paneque-Gálvez, 2019), coverage of large public events (Codel, 2013), search and rescue operations (Mishra et al., 2020) and crisis management (Finn & Donovan, 2016). Their use in public spaces is linked with their capacity to track individuals and situations and to store and transmit live images and videos (Volovelsky, 2016). Drones include technologies that allow for facial recognition, behavior profiling, movement and location detection and can collect and transmit mobile data and other information associated with the Internet of Things (Finn et al., 2014; Schlag, 2013). Combined with their low cost and maneuverability, these capabilities have turned drones into a powerful data collection vehicle for social research (Birtchnell & Gibson, 2015). This capacity for multi-modal data collection adds a further layer of ethical complexity. For example, drones equipped with high-resolution cameras and thermal imaging tend to be more privacy intrusive than drones associated with other sensors (Finn et al., 2014). Even when visual data captures only ‘the top of people’s head’ as a strategy for anonymized data collection (Finn & Donovan, 2016), privacy violations can still occur by aggregating visual data with other types of data provided by the drones’ sensors. In other words, **the multi-functionality of drone technologies may facilitate the identification of individuals when a piece of otherwise unidentifiable information is merged with other data through triangulation.** This is also a danger with other types of visual data where visual material is connected to data not co-collected by the same technology (i.e., the triangulation of CCTV footage with police reports and smartphone data).

3.2 Social media sourced visual data

A second primary source of digital visual material comes from the avalanche of digital data which is uploaded to social media sites every day. This visual data is in the form of both still and moving images. The last official declaration (in 2010) of the number of searchable pictures on Google Images was a figure over 10 billion. That figure is now estimated to be more than 136 billion. By 2020 more than 50 billion photos had been uploaded to Instagram (Aslam, 2020). At the same time, according to YouTube’s own figures for 2021, more than 500 hours of digital film footage are uploaded every minute on that platform alone. Some of this footage comes from smartphones videos. Others from digital material uploaded from alternate sources (including CCTV cameras, dashcams, head mounted video cameras, drones).

Given the richness, ubiquity, and ready convenience of this data, there has been an increase in research which has applied visual social media data both as experimental stimuli and as a source for analysis within its own right. Researchers have used still photos of faces for studies on emotion (Keltner et al., 2019), mental health (Mueser et al., 1996), self-esteem (Borges, 2011), to name a few. There have also been concerted efforts to build identification tools (i.e., face recognition – Taskiran et al., 2020) and classification tools (e.g., gender and ‘race’ (Sheuerman et al., 2020), sexual orientation and political affiliation (Kosinski, 2021; Wang & Kosinski, 2018)) using social media sourced images. At the same time, researchers have used social media sourced video data to study real-life interactions in real-world settings. These include encounters between police and citizens (Philpot et al., 2021), behavior during robberies (Nassauer, 2018), social distancing during the Covid-19 pandemic (Hoeben et at 2021), and cycles of violence during street protests and uprisings (Bramsen, 2017). This kind of social media video data allows researchers to examine social events in which they could never realistically be present in-situ and could never hope to analyze in systematic detail.

Acquiring this kind of digital visual data can require technical skills and resources. Increasingly there are commercial data broking companies that can provide such data as a paid for service. For those with the resources to outsource data collection, there are a range of ethical considerations based around trust in the ethics of data providers (Stewart, 2021). For researchers with the technical skills to acquire data directly, there are still important ethical challenges in relation to the researcher, the uploader, those captured in the images, and for the social media platform itself. **The first question to arise, when engaging with social media platforms, is to whom the data actually belongs.** For example, while YouTube provides the technical platform for uploading and sharing videos, the site is explicit in stating that the uploader retains all ownership rights to their material. This comes with a caveat. Specifically, when uploading visual data to the site the uploader grants a worldwide, non-exclusive, royalty-free, transferable, sublicensable to YouTube (and others) to use that content (including to reproduce, distribute, modify and display it) (YouTube, 2022). This sublicense is valid until the content is removed. For the psychologist interested in this data, this highlights several known facts. First, by uploading the video to YouTube, the uploaders themselves accept the video is now (unless applying private restrictions) available in the public domain and may be viewed by others, including researchers and research participants. Second, while the uploader retains ownership of the video data, they are aware that, until this content is removed, the content may be reproduced, modified and further distributed across the YouTube platform.

This latter point, however, does not specify explicitly that the video may also be harvested and modified by psychologists for research. Typically, to download video content from YouTube without written permission violates YouTube's terms of condition. The platform does, however, also apply **a 'Fair Use' policy,** which provides exemptions for taking single copies under conditions of non-commercial education or research (Google, 2022). This creates an ethical conundrum for researchers. Namely, that YouTube allows the downloading of content for research (under the above conditions), yet YouTube does not actually retain ownership rights to the content, which remain with the uploader. This being the case**, researchers have an ethical responsibility to take reasonable steps to engage with the uploader of the content and to inform them of their intention to use their content** for a study, **providing**

where possible the option to opt out. An example of how this might work in the case of YouTube content is outlined below in the ‘Ethical Challenges for Data Storage’ section.

It is not only the consent of uploaders and the platform that are important to consider, but also the consent of all those individuals whose image is available in the photo or the video clip. When it comes to the use of still images scraped from social media sites, there is recent evidence of the importance of seeking and ensuring consent from any individual to use an image of their face. For example, Clearview AI, the facial recognition company, scraped websites such as Facebook, Instagram and Twitter to build their facial recognition tool, gleaning over 20 billion photos (Knight, 2021). In May 2022, the UK’s Information Commissioner’s Office (ICO) fined Clearview AI £7.5 million for breaching data protection laws. The judgement argued that Clearview had: failed to use the information of people in the UK in a fair and transparent way, given that individuals were not made aware or would not reasonably expect their personal data to be used in this way; failed to have a lawful reason for collecting people’s information; failed to have a process in place to stop the data being retained indefinitely; and failed to meet the higher data protection standards required for biometric data (classed as ‘special category data’ under the GDPR and UK GDPR). Clearview AI, based in the US – where there is little by way of data protection legislation – claimed they were not subject to EU law (McCallum, 2022). Yet because their web scraping practices resulted in collecting data from EU countries and because their facial recognition product was sold to EU organizations, they were deemed to be liable to the GDPR. As such, researchers (even if outside the EU) need to be mindful of when EU legislation applies. Taken together, the Clearview AI case shows that consent remains an important criterion for determining ethical use of images. **Where consent cannot be secured directly (or where no effort has been made to seek consent), then a powerful argument for beneficence has to be made before it could be considered ethically (or legally) appropriate to use such material.**

When it comes to the question of the use of video images, consent remains an important consideration. For example, it is highly unlikely that all the individuals captured in social media videos will have given their explicit permissions and consent for the video to be uploaded, or for the footage to be used in research. **However, failure to secure individual consent doesn't automatically mean that it would be unethical to use such material. A key distinction is often whether the videos are recorded in public or private spaces.** Data protection legislation recognizes that public spaces are settings in which individuals may expect to be observed (e.g., by other individuals or public CCTV cameras). This complies with the Ethics Code of the American Psychological Association (2002, Section 8.03), which states that researchers may dispense from obtaining informed consent in so far that "the research consists solely of naturalistic observations in public places, and it is not anticipated that the recording will be used in a manner that could cause personal identification or harm" (Philpot et al., 2019, p. 62). These are the same terms on which ethnographic research is conducted, where researchers frequently observe behavior in open public spaces, such as highstreets or arenas, where it is impossible to attain all persons' consent (Legewie & Nassauer, 2018). In fact, YouTube (and other platforms) do provide individuals captured on video the option to request the removal of a video if they do not want that video publicly available (Legewie & Nassauer, 2018). However, in practice, the qualifying conditions are steep—the individual must be uniquely identifiable, e.g., though the combination of image, voice, full name, contact information (e.g., address, phone number) or other uniquely identifiable information.

4. Ethical Challenges for Data Analysis

1. Bias and discrimination in automated processing

The Belmont Report's principle of justice promotes fair treatment for all, which includes a fair distribution of the risks and benefits of the research. Against this backdrop, **it is vital to recognize the potential for bias and discrimination to shape the way automated visual data is collected and analyzed.** It is now widely recognized that bias and discrimination can be introduced in algorithmic research during collection, modelling, training, and use (Ferrer et al., 2021). Algorithms tend to reflect the biases of those who created them, and the data used to train them; biased data often produce biased outcomes (O'Neil, 2016). One of the most prominent controversies concerning digital visual data is the use of face datasets heavily skewed towards white men for training facial recognition software (Stevens & Keyes, 2021). As highlighted by the National Institute of Standards and Technology Face Recognition Vendor Test such imbalances in demographic representation in the data led to differences in algorithmic accuracy (Grother et al., 2019). Given the rapid rise in use of facial recognition systems in society, these findings raise ethical and moral questions about the application of software trained on biased data – not least because there have already been numerous failings of these systems overwhelmingly for people of color (e.g., General & Sarlin, 2021).

This raises the related question of what researchers should do when the bias in data is a true representation of discrimination that exists in society? **In line with the Belmont principle of justice, it is important to consider fairness and ensure that people are treated equally; as opposed to allowing an algorithm to learn current inequality and then further reinforce discrimination.** Fairness, though, is not easily achieved, not least because there is no single universally agreed upon definition that is acceptable to everyone and across every situation (Mehrabi et al., 2021). Researchers can contribute to the pursuit of fairness by interrogating algorithms which although reflective of society, are discriminatory and thus ethically questionable in their decision making (see, for example, Mittelstadt et al., 2016; Tsamados et al., 2021). They can ensure that their own algorithm development is carefully designed, implemented, and interpreted in order to avoid producing such biased algorithms in the first place. To do so, they can include in the development team researchers from underrepresented (non-WEIRD) groups (Alfano et al., 2022), assess and report how much diversity is embodied in their research (Mitchel et al., 2019), and acknowledge asymmetric power relations (Berg, 2016).

At the same time, (and related to the problem of bias) the availability of digital visual data and developments in machine learning has led to a revival in practices which seem close to modern day phrenology (Birhane, 2020; Stark, & Hutson, 2021). This physiognomy (Jenkinson, 1997) inspired work seeks possible links between facial features and character. Such research has examined the possibility of developing algorithms to predict, for example, criminal propensity, sexual orientation, and political affiliation (Kosinski, 2021; Wang & Kosinski, 2018). This work raises a number of important questions about beneficence and justice – which are central to the Belmont guidelines. More specifically, to be able to justify such an approach, researchers would need to demonstrate that this kind of research delivers maximal possible benefits and minimizes possible harms which result as a consequence of the research. Such cost-benefit considerations include reviewing the rigor of the scientific underpinning of research and the rigor of the experimental design. There is very little robust scientific work which supports the idea that it is possible to infer unobservable theoretical constructs from other observable properties, such as facial features (Jacobs & Wallach, 2021). This kind of conceptual weakness undermines any claim to beneficence from the outset. Thus, **a key ethical question to be answered is why is the research necessary in the first place – i.e., how could it benefit people and society?**

Furthermore, in the case of research on determining sexual orientation from faces, Wang and Kosinski (2018) place disproportionate risk on the gay men and women who participated (without their knowledge) in the study. This unequitable division of risk-to-benefit across those within and those outside the LGBTQ+ community breaches justice principles, specifically fairness and equality. It is those within the community who run the risk of experiencing social, economic or physical harm from being identified against their will, and there is no discernible benefit to the wider gay community from the research having been conducted.

To avoid such pitfalls, researchers need to think carefully about the data they have collected and whether it is appropriate for the task at hand. For example, if a dataset was collected for a specific task, it cannot necessarily be forced into a different research problem (Shimron et al., 2022). **Researchers should always consider whether black box AI approaches are the most appropriate for the current research, although an exciting and innovative approach it might not be better than a more traditional psychological method – especially if the researchers are not sufficiently experienced or trained to use machine learning techniques.** At present, automated processing does not seem to be more accurate than video processing by human observers (Ryus et al., 2014). When using digital visual data, for example, researchers have shown that small perturbations to an image can result in an algorithm to misclassify – changing just one pixel in almost three-quarters of test images lead to misclassification when using state-of-the-art image recognition systems, including near misses (a cat for a dog) and far misses (a stealth bomber mistaken as a dog) (Su et al., 2019). At the same time, as we have seen, automated processing may also be sensitive to biases. However, manual processing requires a lot of time, effort, and very likely many observers will need to be included in data processing (Philpot et al., 2019). To resolve this, researchers tend to combine automated processing with a smaller number of human observers. This raises a number of ethical questions in respect of human coders which we consider below.

4.2 Dangers to human analysts

One of the ethical dangers less often considered in respect of digital data, is the potential danger to the researcher. Particularly, when dealing with contributory social media material or with material related to crime or terrorism, there is the danger that researchers will be exposed to distressing images of things like child and animal abuse, graphic sexual content, war zone footage and terrorist attacks. In her pioneering book on commercial content moderation, Roberts (2014) shows the psychological costs to the people who are asked to ensure that this kind of material does not find its way into the public sphere. There is also increasing recognition of the potential impact of this kind of exposure for researchers who work in the field of terrorism studies (Conway 2021) and combatting child sexual abuse (Tapson et al., 2021). People who are exposed to such images can experience panic attacks, anxiety, depression, other symptoms associated with PTSD, and begin to experience destructive habits and changes to their world view. With that in mind, the 2020 iteration of the Association of Internet Researchers' (AoIR) ethics guidelines emphasizes "the growing need for protecting the researchers, as well as our subjects and informants" (Franzke et al., 2020, p. 11).

Automated content moderation is often touted as the solution to this, but its increasingly clear AI is not a panacea and may in fact not be what we should be attempting to do anyway (Gillespie, 2020). As such, protecting the well-being of the research team should be prioritized (Paluck, 2009). To mitigate these risks, researchers need to build emotion management provisions into the ethical guidelines of their projects and build a support network where concerns can be raised, and practices can be informed and challenged. While security research is governed by specific legal regulations and protection acts, this does not provide a set of specific guidelines for academic research. Along with legal compliance, psychologists need to seek guidance from colleagues doing research in the same area. Colleagues can provide guidance for developing techniques that increases researchers' ability to separate themselves from the subject of the study and protect their safety. Moreover, protecting the safety of the research team involves handling researchers' digital traces. Advice and guidance for this has been recently offered by the Centre for the Protection of National Infrastructure (CPNI). Additional guidance is also available when collecting and processing data from conflict zones and from specific populations (see Baele et al., 2018; Ellsberg & Potts, 2018 for a detailed discussion and recommendations from researchers working with data about other sensitive issues). The bottom line is that **research teams have an ethical responsibility to consider the potential dangers to anybody who might be exposed to such images as part of their work** – and consider ways to mitigate the potential effects if viewing such images is unavoidable.

5. Ethical Challenges for Data Storage

5.1 Storage and processing security

It is the researcher's ethical (and legal) obligation to protect the data they collect and use. In the case of digital visual data where it is often the case that the data allows identification of an individual, for example facial images, there must be a plan for responsible and safe storage of such personally identifying data. Generally, the more information stored about an individual or the larger number of individuals included in the dataset the higher the risk of causing harm if information is unintentionally released, or maliciously hacked. If visual data is stored locally on a computer, then that must have a password and firewall system and access to the files storing the data should also be restricted through encryption. There are different forms of encryption, at varying levels of protections; that the researcher should choose a level of encryption that is proportionate to the sensitivity of the data being protected. Although mainstream access to quantum computing is still at least a few years away, researchers should bear in mind that the advent of quantum will affect encryption requirements. Even if a 128-bit encryption is the most suitable for data protection in the present day but it is likely to need revision in the future.

The option of additional protection provided through integrated use of multiple security protocols, such as hashing, anonymization, and encryption, is likely to become more commonly required in the future. As a note of caution, however, research has shown that deidentified and even anonymized data can be reverse engineered allowing the reidentification of individuals (Narayanan & Shmatikov, 2008). If researchers have collected a range of information about each individual, it is good practice to separate details across a number of files to minimize harm should one file become compromised or leaked. Cloud-based storage options are convenient, however not always permanent or secure. Researchers should be mindful that the cloud-based storage data centers could be overseas and under the jurisdiction of a different legal system. Cloud data storage should be avoided for extremely highly sensitive data. Day-to-day handling of sensitive visual data should be carried out in a secure location. Access to images and other data which may de-anonymize individuals should be restricted to those with clearance.

5.2 Function creep: the importance of data deletion

The Data Protection Act (2018) and GDPR state that personal data must be obtained and processed for a specified purpose and not kept longer than necessary. The need to be clear and transparent about the reason for using personal data is to ensure that the research purposes are reasonably in line with the expectation of individuals involved. Yet ethical review boards in educational institutions (e.g., IRB) do not sufficiently deal with the issue of function creep (Whitman, 2021). When designing a study, researchers should clearly outline the purpose for collecting and processing the digital visual data and this purpose must be documented and reviewed throughout the study process. **The purpose of research can often change over time, and it can be acceptable to develop a new purpose, as long as: 1) the new purpose is consistent with the original purpose; 2) participants give consent for their personal data to be used for the new purpose; or 3) a legal requirement exists to indicate that the new purpose involves processing that is in the public interest** (ICO, Principle b). To give an example where repurposing data is not be legal or ethical, regulators in France recently fined Ikea €1m after they repurposed their CCTV systems installed for security to monitor staff (BBC, 2021). Although there are potential benefits to reusing datasets, it is the researcher's responsibility to ensure that the data is appropriate for the research purpose. Raw data should only be kept for as long as is necessary to achieve its primary purpose. After this purpose is served, or once data sharing agreements expire (whichever is sooner), all data must be securely returned to the owner or erased through government level drive erasure procedures.

5.3 The right to withdraw from research data bases

In line with the APA ethical guidelines and GDPR, individuals, regardless of whether they provided consent or not, have the right to withdraw and to be forgotten (APA, 2017). Yet, with digital visual data this is not necessarily an easy principle to observe**. Once given,**

data can be very hard to take back. In the case of creating a dataset by having participants provide informed consent prior to taking part, researchers can consider the possibility of participant withdrawal in advance and can clearly set out the procedure and limitations for withdrawal in the information sheet, consent form, and debrief. When using data gathered without consent, for example publicly available data from social media sites, the ability to withdraw an individual's data is complex. Returning to the earlier example of Clearview AI (Knight, 2021), the company was ordered to delete data belonging to UK residents from their database. Although it remains unclear how the company will manage to adhere to the order in full, one strategy being used is through the addition of privacy request forms on their website which individuals can complete to opt out from the database. That said, completing the form involves giving Clearview AI even more personal data and although the company promise this information will be deleted, it is reasonable to assume that people will be reluctant to hand over more of their data based on the companies track record.

The lesson for researchers collecting digital visual data through large-scale web scraping is that allowing participants to withdraw can be extremely difficult. However, it is important to consider when designing a research project how such requests will be managed and dealt with ethically. Although a more time-consuming process, one approach is to make use of existing image databases that have been created for research with participants' informed consent. Nightingale et al. (2021) used this approach in their face morphing research and note that it is more ethical yet not necessarily a perfect solution. While it is easier for participants to withdraw their data, other limitations arise. There are more constraints on how researchers can use and subsequently share databases given licensing agreements, and the available facial image datasets tend to have limited diversity.

The right to withdraw is also important when considering the use of social media sourced video data. For example, it can be very difficult for a video uploader (i.e., content owner) or those captured in social media footage, to contact a researcher and ask to opt out of the study. In the example of YouTube, it is unlikely that individual would even be aware that their video has been harvested for research. It is therefore the responsibility of the researcher to make efforts to contact the uploader directly and to make explicit their intention to use this visual data for research. However, this can be easier said than done. For example, there is no messaging functionality on YouTube that allows contacting uploaders directly. One way to try and meet this ethical challenge can be seen in Philpot and colleague's (2021) study using YouTube videos as experimental stimuli to explore citizen perceptions of police power and legitimacy. When sourcing the videos, researchers posted messages in the video's comment section which outlined a description of the intended research, information around ethics board approval and the contact details of the research team in case the uploader or any aware captured individual required further information or wished to opt out. Further, the researchers regularly monitored each video's link, to ensure that the content was still open access and within the public domain. If the video was removed from the platform or the viewing restrictions changed to private, the associated data was also removed from the research study.

Outside of social media sourced video data, there are cases in which it might be considered that a fair use policy applies which allows use of material without need to acquire consent from the copyright holder (e.g., Intellectual Property Office, 2014). To apply the fair use policy, a few criteria apply such as the purpose and extent of the use. There should, for example, be substantial advancement of knowledge with public benefit. One such example might be using videos clips of politicians from news channels to develop computational techniques to identify deep fakes (e.g., Agarwal et al., 2019). If mechanisms have been put in place to protect the privacy of data that make it very difficult to trace and remove an individual's data, psychologists must refrain from collecting new data from the individual (Kaye, 2012) and from using their data for future processing (Politou et al., 2018).

6. Ethical Challenges of Doing Open Science with Visual Data

With the movement toward open science and research replicability, there is an increased expectation among scientific publishers, funding bodies and colleagues for data sharing between researchers. **Sharing digital visual data is not entirely straightforward and the option to share depends on the method of collection, there are at least four scenarios to consider.** One, if the researcher has collected the data and has participants' informed consent to share that data openly, the researcher can do so. That said, the researcher still has ethical responsibly to ensure that the participants' safety and integrity are upheld. For example, researchers should share the minimum personal information required and details of informed consent must be given to ensure that other researchers do not engage in function creep. Furthermore, the participants must be made aware of the consequences that this data sharing has on their right to withdraw/be forgotten: the researcher will only be able to control their own copy of the dataset. Two, if the researcher has collected the data but does not have participant consent to share openly, the data could still be shared privately with other researchers if participants gave consent for their data to be used by others under the conditions that they originally agreed to. In this case, the researcher would need to develop a license agreement with the other party and essentially sublet the data to them. The party subletting the data must agree to use the data in line with the terms of the license agreement which should include details relating to function creep, data storage, sharing, and deletion. Three, if the researcher has sublet the data from another source, for example from government, then they are not the data controller and must adhere to the license agreement they have entered which very likely means they cannot reshare the data. Instead, the researcher can refer interested parties to the source and allow them to enter into their own agreement directly with the controller. Four, if the researcher collects data that is publicly available, it does not necessarily mean that it is ethically appropriate to share the data. In doing so, the researcher removes an individual's ability to censor their personal information – even if they later opt to remove a photo of themselves from social media, the researcher's collection and resharing of this data means that this information is still publicly available against an individual's wishes. Removing an individual's control over the data in this way is unethical as it undermines their right to privacy.

6.1.What about reproducibility of analysis using digital visual data?

The scientific community now must deal with two contending revolutions: the replication crisis which spurred the practice of open science and the availability of masses of digital visual data that, if shared openly, could violate ethical and legal constraints (Dennis et al., 2019). To observe the ethical and legal principles and preserve individual right to privacy, one approach researchers have taken is to not release the visual dataset, source code, and learned data structures publicly. The concern here, however, particularly in the case of using AI where there are heightened concerns about issues of interpretability (black box) and bias, not releasing the code and data undermines the open science framework and scientific reproducibility (King et al., 2019). A recent review of 49 papers using machine learning approaches to create prediction classifiers, found that 22 of these papers contained demonstrable errors (Shepperd et al., 2019). Such errors are not unique to AI-techniques either, many psychological papers using more traditional analytic techniques have been shown to have errors with basic statistics (Nuijten et al., 2016). It is, therefore, feasible that the use of digital visual data which cannot necessarily be made accessible in line with open science principles will add to the problem of reporting inconsistencies.

That said, there are ways to share study materials, anonymized/sanitized data, or the most minimally processed versions (for example, x-y coordinates of joints derived from pose estimation programs (Hansen et al., 2019) or anonymized sketches (Philpot et al., 2022)) as long as appropriate caution is taken given that deidentified and even anonymized data can be reverse engineered allowing the reidentification of individuals (de Montjoye et al., 2015; El Emam et al., 2011). Another avenue for data sharing, though again with careful consideration, would be restricted-use repositories, like that managed by the Inter-university Consortium for Political and Social Research. Finally, when visual data cannot be shared, to help to mitigate the risk of misinterpretation of results, it might be useful to an interdisciplinary research team with an expert who is sufficiently trained to apply (AI) techniques to classify large visual datasets (Ostermann et al., 2021).

7. A Structured Approach to Digital Visual Ethics for Psychologists

Having outlined the key challenges facing psychologists who want to think ethically about digital visual data in their research practice, **we now take a more practical and pragmatic turn.** Many of the ethical dilemmas we have outlined have no single definitive point of resolution, and it's often the case that legal frameworks and ethical guidelines play a role in shaping decision making. However, in questions of technology and visual data, the law often lags behind (Bruschwig 2021) meaning that some practices may be legally permissible but ethically dubious. At the same time (as we have seen in the Clearview AI case - Knight, 2021) digital visual data can transcend national boundaries, meaning that researchers may be traversing different legal jurisdictions.

With that in mind, we take inspiration from one of the more developed regulatory frameworks in respect of digital privacy and security – namely the General Data Protection Regulation (GDPR) framework developed by the European Union. The GDPR developed out of the European Convention on Human Rights (1950) which enshrined the right to privacy as a basic human right. As new digital technologies were developed, the EU first created a European Data Protection Directive (in 1995), and then passed the GDPR in 2016, requiring all institutions to be compliant by March 25, 2018. We draw on elements of the GDPR framework, not as the definitive word on how to resolve ethical decision making, but rather as structure for prompting appropriate and comprehensive ethical deliberations when it comes to the use of digital visual data in research.

We recognize that, since 95% of research is still predominantly White and North American (Thalmayer et al 2021), GDPR regulations may not directly govern most psychological research practice. **However, the GDPR framework provides two important tools that can**

be adapted for psychological research. These are referred to as 'impact assessment' frameworks and concern the right to privacy (Privacy Impact Assessment: PIA) and ethical digital data use (Data Protection Impact Assessment: DPIA). A Privacy Impact Assessment (PIA) is designed to allow organizations (or research teams) to analyze how they collect, use and share information that is personally identifiable. PIAs are anticipatory in nature, being carried out before the research starts. PIAs are concerned with privacy in the round, including privacy of the person, privacy of a person's behavior, and privacy of personal communication – as well as privacy of personal data. The privacy of personal data is more specifically the focus of the Data Protection Impact Assessment (DPIA). The DPIA is designed to assess the level of risk in any project or processing activity that might involve personal information. DPIAs are undertaken before any data collection or processing occurs and encourage best practice by ensuring data protection by default and by design. They are designed to identify risk, explore how that risk may be mitigated, and justify any risks that remain after the assessment has been done.

We set out all the key ethical considerations that flow from both the PIA and the DPIA – and show how consideration of each of these dimensions can lead to more ethically informed research decision making. Moreover, we go beyond the current concerns of the DPIA to include other important ethical concerns identified in the current paper – including ethical dangers for analysts themselves and the ethics of engaging with Open Science practices. **We draw all these concerns together in a single Privacy and Data Protection Impact Assessment (PDPIA) tool which we make available for psychologists, via the Open Science Framework, to use as part of the ethical research design of studies using digital visual data** – osf.io/5pex7. Here we include a PDPIA template – which forms the basis for how researchers can record their own PDPIA process and outcome – and a set of steps and instructions for completing the PDPIA template.

7. Conclusion

In common with other kinds of data in this era of ‘big or naturally occurring data sets’ (BONDS: Paxton & Griffiths 2017), digital visual data affords psychologists with many exciting research possibilities. It becomes possible to see real-life interactions in real time, and to be able to analyze this behavior in a fine grained and systematic manner. However, the fact that faces (and other personally identifying physical characteristics) are captured as part of these data sets, means that this kind of data is at the highest level of sensitivity by default. There have already been examples of ethically suspect practice by governmental, commercial and academic research teams using this kind of data. If psychologists are to comply with the Belmont principles in the age of big data (see Paxton 2020), then this requires updated guidelines to help shape research practice.

In this paper we explored the ethical challenges that face psychologists wishing to leverage digital visual data. We considered the challenges in respect of data acquisition, data analysis, data storage, and the place of digital visual data in the new open science movement. Using examples of how these ethical challenges have already begun to play out in a range of research domains, we mapped the terrain that psychologists need to consider. We then used this mapping exercise to offer a practical and solution focused approach to how the discipline might move forward when it comes to using digital visual data in ethically informed ways.

Our approach was shaped by engagement with one of the more developed attempts to enshrine privacy and digital rights in law (the European Union General Data Protection Regulation (GDPR) framework). While recognizing that most psychological research is conducted in the United States, and is thus outside the (direct) reach of the GDPR framework, we suggest that the ‘impact assessments’ elements of GDPR are a useful point of reference. By combining prompts from both the Privacy Impact Assessment (PIA), and the Data Protection Impact assessment (DPIA), we offer a Privacy and Data Protection Impact Assessment (PDPIA) framework for psychologists who want to work with digital visual data. Our PDPIA framework encapsulates all the dimensions covered in this paper, and is made available to researchers through the Open Science Framework – osf.io/5pex7.

The PDPIA is designed to be used at the outset of any proposed research project intending to use digital visual data, and thus to attempt to shape ethical decision making by design. It asks researchers to reflect on a systematic set of ethical questions that pertain to all aspects of the research process – including consultation, necessity and proportionality, data acquisition, processing and storage, and the identification of risk and risk mitigation. The PDPIA is designed to be a document that can be used as part of an ethics application to an Institutional Review Board (IRB) or to be shared with research partners to reassure that the proposed work is ethically sound. We conceive of the PDPIA as a living document – to be updated as technologies and circumstances change – rather than a fixed and proscriptive set of rules for research (which is why we have made it both open source and free for others to use and adapt as they see fit). One of the characteristics of the digital age is the speed with which new technologies or analytic capabilities become available. For example, in the field of digital visual data, the use of drone technology is in its infancy. There is very little psychological research which has used drone technology. However, research using drones became a feature of the response to the Covid-19 pandemic and is increasingly being used in research in humanitarian crises. It is conceivable that drones will become a much more common psychological research tool going forward and that new technologies (as yet unimagined) will come on stream. Given the rapid change in what might be possible in both technology and visual data analysis, we will need to be flexible enough to adapt to new ethical questions as they arise.

References

Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K., & Li, H. (2019, June). Protecting World Leaders Against Deep Fakes. In CVPR workshops (Vol. 1, p. 38).

Alfano, M., Sullivan, E., & Fard, A. E. (2022). Ethical pitfalls for natural language processing in psychology. In M. Dehghani & R. Boyd (eds.), *Handbook of Language Analysis in Psychology* (pp.511-530). Guilford Press.

American Psychological Association. (2002). Ethical principles of psychologists and code of conduct. *American Psychologist*, *57*(12), 1060-1073.

American Psychological Association. (2017). *Ethical principles of psychologists and code of conduct* (2002, last amended January 1, 2017). https://www.apa.org/ethics/code/

Arrigo, B. A., & Sellers, B. G. (Eds.). (2021). *The pre-crime society: Crime, culture, and control in the ultramodern age*. Bristol University Press and Policy Press.

Aslam, S. (2020). Instagram by the numbers: stats, demographics & fun facts. *Omnicore Agency, 10*.

Baele, S. J., Lewis, D., Hoeffler, A., Sterck, O. C., & Slingeneyer, T. (2018). The ethics of security research: An ethics framework for contemporary security studies. *International Studies Perspectives, 19*(2), 105-127.

Banks, M. & Jay, R. (2011). *Made To Be Seen: Historical Perspectives on Visual Anthropology*. University of Chicago Press.

BBC (2021, June 15). *Ikea France fined €1m for snooping on staff*. BBC. https://www.bbc.co.uk/news/world-europe-57482168

Berg, J. (2015). Income security in the on-demand economy: Findings and policy lessons from a survey of crowdworkers. *Comparative Labor Law Policy Journal*, *37*(3), 543-576.

Birhane, A. (2022). The unseen Black faces of AI algorithms. *Nature, 610*(7932), 451-452.

Birtchnell, T., & Gibson, C. (2015). Less talk more drone: Social research with UAVs. *Journal of Geography in Higher Education*, *39*(1), 182-189.

Borges, A. (2011). The effects of digitally enhanced photos on product evaluation and young girls' self-esteem. *Recherche et applications en marketing (English edition)*, *26*(4), 5-21.

Bramsen, I. (2017). How violence breeds violence: Micro-dynamics and reciprocity of violent interaction in the Arab uprisings. *International Journal of Conflict and Violence*, *11*, a625.

Brunschwig, C. R. (2021). *Visual Law and Legal Design: Questions and Tentative Answers*. Proceedings of the 24th International Legal Informatics Symposium IRIS 2021, 179–230.

Codel, E. (2013, July). *Drone's eye view of burning man 2013* http://youtu.be/m2ThTb6iffA.

Cromey, D. W. (2012). Digital images are data: and should be treated as such. In *Cell Imaging Techniques* (pp. 1-27). Humana Press.

Darwin, C. (1872/1999) *The expression of the emotions in man and animal.* Fontana Press.

Data Protection Act (2018). https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

De Montjoye, Y. A., Radaelli, L., Singh, V. K., & Pentland, A. S. (2015). Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science, 347*, 536-539.

Dennis, S., Garrett, P., Yim, H., Hamm, J., Osth, A. F., Sreekumar, V., & Stone, B. (2019). Privacy versus open science. *Behavior Research Methods, 51*, 1839-1848.

Diamond, L. (2019). The road to digital unfreedom: The threat of postmodern totalitarianism. *Journal of Democracy, 30*(1), 20-24.

El Emam, K., Jonker, E., Arbuckle, L., & Malin, B. (2011). A systematic review of re-identification attacks on health data. *PloS one, 6*, e28071.

Ellsberg, M., & Potts, A. (2018). Ethical considerations for research and evaluation on ending violence against women and girls. https://apo.org.au/node/194481.

European Convention on Human Rights. (1950). *EConHR.* Council of Europe.

Evans, J. & Hall, S. (1999). *Visual Culture: The Reader*. Sage.

Ferrer, X., van Nuenen, T., Such, J. M., Coté, M., & Criado, N. (2021). Bias and Discrimination in AI: a cross-disciplinary perspective. *IEEE Technology and Society Magazine, 40*(2), 72-80.

Finn, R., & Donovan, A. (2016). Big Data, Drone Data: Privacy and Ethical Impacts of the Intersection Between Big Data and Civil Drone Deployments. In B. Custers (Ed.), *The Future of Drone Use. Information Technology and Law Series, 27*. T.M.C. Asser Press.

Finn, R. F., Wright, D., Donovan, A., Jacques, J., & De Hert, P. (2014). *Privacy, data protection and ethical risks in RPAS civil applications: Final report to the European Commission*. http://ec.europa.eu/DocsRoom/documents/7662.

Floridi, L. (2018). Soft ethics, the governance of the digital and the General Data Protection Regulation. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376*(2133), 20180081.

Franzke, A. S, Bechmann, A., Zimmer, M., Ess, C. and the Association of Internet Researchers (2020). *Internet Research: Ethical Guidelines 3.0.* https://aoir.org/reports/ethics3.pdf

Frascella, C. (2021). Amazon Ring Master of the Surveillance Circus. *Federal Communications Law Journal*, *73*(3), 393-422.

Friis, C. B., Liebst, L. S., Philpot, R., & Lindegaard, M. R. (2020). Ticket inspectors in action: Body-worn camera analysis of aggressive and nonaggressive passenger encounters. *Psychology of Violence, 10*(5), 483-492.

Fysh, M. C., & Bindemann, M. (2018). Human–computer interaction in face matching. *Cognitive Science*, *42*(5), 1714-1732.

General, J. & Sarlin, J. (2021, April 29). *A false facial recognition match sent this innocent Black man to jail*. CNN Business. https://edition.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html

Gillespie, T. (2020). Content moderation, AI, and the question of scale. *Big Data & Society*.

Google. (2022, July). *Fair Use on YouTube*. https://support.google.com/youtube/answer/9783148?hl=en-GB

Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test Part 3: Demo graphic Effects, *NIST Interagency/Internal Report (NISTIR)*, National Institute of Standards and Technology, Gaithersburg, MD.

Haney, C., Banks, C., & Zimbardo, P. (1973). A study of prisoners and guards in a simulated prison. *Naval Research Review*, *9*, 1–17.

Hansen, L., Siebert, M., Diesel, J., & Heinrich, M. P. (2019). Fusing information from multiple 2D depth cameras for 3D human pose estimation in the operating room. *International Journal of Computer Assisted Radiology and Surgery, 14*(11), 1871-1879.

Hoeben, E. M., Bernasco, W., Suonperä Liebst, L., van Baak, C., & Rosenkrantz Lindegaard, M. (2021). Social distancing compliance: A video observational analysis. *PLoS ONE, 16*(3), e0248221.

Intellectual Property Office (2014, Nov 18). Changes to copyright law. UK Government. https://www.gov.uk/government/publications/changes-to-copyright-law

Iversen, T., & Rehm, P. (2022). *Big Data and the Welfare State: How the Information Revolution Threatens Social Solidarity*. Cambridge University Press.

Jacobs, A. Z., & Wallach, H. (2021, March). Measurement and fairness. In *Proceedings of the 2021 ACM conference on Fairness, Accountability, and Transparency* (pp. 375-385).

Jacquet, M., & Champod, C. (2020). Automated face recognition in forensic science: Review and perspectives. *Forensic Science International, 307,* 110124.

Jenkinson, J. (1997). Face facts: a history of physiognomy from ancient Mesopotamia to the end of the 19th century. *The Journal of Biocommunication, 24*, 2-7. PMID:9399135

Kaplan, S., Handelman, D., & Handelman, A. (2021). Sensitivity of neural networks to corruption of image classification. *AI and Ethics, 1,* 425-434.

Kaye, J. (2012). The tension between data sharing and the protection of privacy in genomics research. *Annual Review of Genomics and Human Genetics, 13*, 415-431.

Keltner, D., Sauter, D., Tracy, J., & Cowen, A. (2019). Emotional expression: Advances in basic emotion theory. *Journal of Nonverbal Behavior*, *43*(2), 133-160.

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics, 26,* 89-120.

Knight, W. (2021, October 4). *Clearview AI Has New Tools to Identify You in Photos*. Wired, Kosinski, M. (2021). Facial recognition technology can expose political orientation from naturalistic facial images. *Scientific Reports, 11*, 1-7.

Kumar, M., Singh, N., Kumar, R., Goel, S., & Kumar, K. (2021). Gait recognition based on vision systems: A systematic survey. *Journal of Visual Communication and Image Representation, 75*, 103052.

Li, L., Mu, X., Li, S., & Peng, H. (2020). A Review of Face Recognition Technology. *IEEE Access*, *8*, 139110-139120.

Legewie, N., & Nassauer, A. (2018). YouTube, Google, Facebook: 21st century online video research and research ethics. *Qualitative Sozialforschung*. Freie Universität Berlin.

Conway, M. (2021) Online extremism and terrorism research ethics. *Terrorism and Political Violence, 33*(2), 367-380.

McCallum, S. (2022, May 23). *Clearview AI fined in UK for illegally storing facial images*. BBC. https://www.bbc.co.uk/news/technology-61550776

Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. *ACM Computing Surveys (CSUR)*, *54*, 1-35.

Milgram, S. (1963). Behavioral study of obedience. *Journal of Abnormal and Social Psychology* , *67*, 371-378.

Millard, K. (2022). *Double Exposure: How Social Psychology Fell in Love With the Movies*. Rutgers, UP.

Mishra, B., Garg, D., Narang, P., & Mishra, V. (2020). Drone-surveillance for search and rescue in natural disaster. *Computer Communications*, *156*, 1-10.

Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., ... & Gebru, T. (2019, January). Model cards for model reporting. In *Proceedings of the conference on fairness, accountability, and transparency* (pp. 220-229).

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), 2053951716679679.

Mueser, K. T., Doonan, R., Penn, D. L., Blanchard, J. J., Bellack, A. S., Nishith, P., & DeLeon, J. (1996). Emotion recognition and social competence in chronic schizophrenia. *Journal of Abnormal Psychology, 105*(2), 271–275.

Nassauer, A. (2018). How robberies succeed or fail: Analyzing crime caught on CCTV. *Journal of Research in Crime and Delinquency, 55*(1), 125-154.

Nayak, R., Pati, U. C., & Das, S. K. (2021). A comprehensive review on deep learning-based methods for video anomaly detection. *Image and Vision Computing*, *106*, 104078.

Nightingale, S. J., Agarwal, S., & Farid, H. (2021). Perceptual and computational detection of face morphing. *Journal of Vision, 21*, 1-18.

Nuijten, M. B., Hartgerink, C. H., Van Assen, M. A., Epskamp, S., & Wicherts, J. M. (2016). The prevalence of statistical reporting errors in psychology (1985–2013). *Behavior Research Methods, 48*, 1205–1226.

O’Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishers.

Ostermann, T., Röer, J. P., & Tomasik, M. J. (2021). Digitalization in psychology: A bit of challenge and a byte of success. *Patterns*, *2*, 100334.

Paluck, E. L. (2009). Methods and ethics with research teams and NGOs: Comparing experiences across the border of Rwanda and Democratic Republic of Congo. In *Surviving Field Research* (pp. 50-68). Routledge.

Paxton, A. (2020). The Belmont Report in the age of big data: Ethics at the intersection of psychological science and data science. In S. E. Woo, L. Tay, & R. W. Proctor (Eds.), *Big data in psychological research* (pp. 347–372). American Psychological Association.

Paxton, A., & Griffiths, T. L. (2017). Finding the traces of behavioral and cognitive processes in big data and naturally occurring datasets. *Behavior research methods, 49*(5), 1630-1638.

Philpot, R., Liebst, L. S., Levine, M., Bernasco, W., & Lindegaard, M. R. (2020). Would I be helped? Cross-national CCTV footage shows that intervention is the norm in public conflicts. *American Psychologist*, *75*(1), 66-75.

Philpot, R., Liebst, L. S., Lindegaard, M. R., Verbeek, P., & Levine, M. (2022). Reconciliation in human adults: a video-assisted naturalistic observational study of post conflict conciliatory behaviour in interpersonal aggression, *Behaviour*, *159*(13-14), 1225-1261.

Philpot, R., Levine, M., Acre-Plata, C., . . . Bandura, A. (2021 – Stage 1 Registered Report). No procedural justice, no peace? Judgements of police legitimacy in ‘real-time’ interactions captured on camera. *Royal Society Open Science.*

Philpot, R., Liebst, L. S., Møller, K. K., Lindegaard, M. R., & Levine, M. (2019). Capturing violence in the night-time economy: A review of established and emerging methodologies. *Aggression and Violent Behavior*, *46*, 56-65.

Pink, S. (2015). Going forward through the world: Thinking theoretically about first person perspective digital ethnography. *Integrative Psychological and Behavioral Science, 49*, 239-252.

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity, 4*(1).

Radley, A. (2010). What people do with pictures, *Visual Studies, 25*(3), 268-279.

Reavey, P. (Ed.). (2011). *Visual methods in psychology: Using and interpreting images in qualitative research.* Routledge/Taylor & Francis Group.

Reavey, P., & Prosser, J. (2012). Visual research in psychology. In H. Cooper, P. M. Camic, D. L. Long, A. T. Panter, D. Rindskopf, & K. J. Sher (Eds.), *APA handbook of research methods in psychology, Vol. 2. Research designs: Quantitative, qualitative, neuropsychological, and biological* (pp. 185–207). American Psychological Association.

Richards, G. (2002). *Putting psychology in its place: A critical historical overview*. Routledge.

Roberts, S. T. (2014). *Behind the screen: The hidden digital labor of commercial content moderation*. University of Illinois at Urbana-Champaign.

Ryus, P., Ferguson, E., Laustsen, K. M., Prouix, F. R., Schneider, R. J., Hull, T., & Miranda-Moreno, L. (2014). *Methods and technologies for pedestrian and bicycle volume data collection*. Transportation Research Board.

Sakiyama, M., Miethe, T. D., Lieberman, J. D., Heen, M. S., & Tuttle, O. (2017). Big hover or big brother? Public attitudes about drone usage in domestic policing activities. *Security Journal*, *30*(4), 1027-1044.

Scheuerman, M. K., Wade, K., Lustig, C., & Brubaker, J. R. (2020). How we've taught algorithms to see identity: Constructing race and gender in image databases for facial analysis. *Proceedings of the ACM on Human-computer Interaction*, *4*(CSCW1), 1-35.

Schlag, C. (2013). The new privacy battle: How the expanding use of drones continues to erode our concept of privacy and privacy rights. *Pittsburgh Journal of Technology Law & Policy*, *13*(2).

Shepperd, M., Guo, Y., Li, N., Arzoky, M., Capiluppi, A., Counsell, S., Destefanis, G., Swift, S., Tucker, A., & Yousefi, L. (2019). The Prevalence of Errors in Machine Learning Experiments. In H. Yin, D. Camacho, P. Tino, A. Tallón-Ballesteros, R. Menezes, & R. Allmendinger (Eds.), *Intelligent Data Engineering and Automated Learning – IDEAL 2019*. Lecture Notes in Computer *Science*, *11871*. Springer, Cham.

Shimron, E., Tamir, J. I., Wang, K., & Lustig, M. (2022). Implicit data crimes: Machine learning bias arising from misuse of public data. *Proceedings of the National Academy of Sciences*, *119*, e2117203119.

Sreenu, G., & Durai, S. (2019). Intelligent video surveillance: A review through deep learning techniques for crowd analysis. *Journal of Big Data*, *6*(1), 1-27.

Stark, L., & Hutson, J. (2021). Physiognomic Artificial Intelligence. *Fordham Intellectual Property Media Entertainment Law Journal*. *32*(4), 922–978.

Stevens, N., & Keyes, O. (2021). Seeing infrastructure: race, facial recognition and the politics of data. *Cultural Studies, 35*, 833-853.

Stewart, R. (2021). Big data and Belmont: On the ethics and research implications of consumer-based datasets. *Big Data & Society*, *8*(2), 20539517211048183.

Su, J., Vargas, D. V., & Sakurai, K. (2019). One pixel attack for fooling deep neural networks. *IEEE Transactions on Evolutionary Computation*, *23*, 828-841.

Tapson, K., Doyle, M., Karagiannopoulos, V., & Lee, P. (2021). Understanding moral injury and belief change in the experiences of police online child sex crime investigators: An interpretative phenomenological analysis. *Journal of Police and Criminal Psychology*, 1-13.

Taskiran, M., Kahraman, N., & Erdem, C. E. (2020). Face recognition: Past, present and future (a review). *Digital Signal Processing, 106*, 102809.

Thalmayer, A. G., Toscanelli, C., & Arnett, J. J. (2021). The neglected 95% revisited: Is American psychology becoming less American? *American Psychologist, 76*(1), 116–129.

Tsamados, A., Aggarwal, N., Cowls, J., Morley, J., Roberts, H., Taddeo, M., & Floridi, L. (2022). The ethics of algorithms: Key problems and solutions. *AI & Society, 37*, 215-230.

Turner, B. L., Caruso, E. M., Dilich, M. A., & Roese, N. J. (2019). Body camera footage leads to lower judgments of intent than dash camera footage. *Proceedings of the National Academy of Sciences, 116*(4), 1201-1206.

van Elteren , M. , & Luck , H. (1990) . Lewin ’s films and their role in field theory . In S. A. Wheelan, E. A. Pepitone & V. Abt (Eds.), *Advances in Field Theory* (pp. 38 – 61). Sage.

Vargas-Ramírez, N., & Paneque-Gálvez, J. (2019). The global emergence of community drones (2012–2017). *Drones*, *3*(4), 76.

Volovelsky, U. (2016). Civilian Use of Drones as a Test Case for the Right to Privacy: An Israeli Perspective. In B. Custers (Eds.), *The Future of Drone Use. Information Technology and Law Series, 27*. T.M.C. Asser Press.

Wang, Y., & Kosinski, M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of Personality and Social Psychology*, *114*, 246-257.

Weenink, D., Dhattiwala, R., & van der Duin, D. (2022). Circles of Peace. A Video Analysis of Situational Group Formation and Collective Third-Party Intervention in Violent Incidents. *The British Journal of Criminology*, *62*(1), 18-36.

Whitman, M. (2021). Modeling ethics: Approaches to data creep in higher education. *Science and Engineering Ethics*, *27*, 1-18.