CLEARVIEW AI, OWNERSHIP, AND THE DIGITAL FACE-IMAGE IN THE AGE OF FACIAL RECOGNITION TECHNOLOGY

by

ALEX FIEDLER

A THESIS

Presented to the Department of Data Science
and the Robert D. Clark Honors College
in partial fulfillment of the requirements for the degree of
Bachelor of Data Science

June 2025

An Abstract of the Thesis of

Alex Fiedler for the degree of Bachelor of Science
in the Department of Data Science to be taken June 2025

Clearview AI, Ownership, and the Digital Face-Image in the Age of Facial Recognition Technology

Approved: *Ramón Alvarado, PhD, Assistant Professor*
Primary Thesis Advisor

The American facial recognition company Clearview AI created an app that allows clients—including police departments and government agencies such as the FBI and Department of Defense—to use photos to search a database of over 30 billion photos that have been scraped from the Web. Clearview's activities have raised alarm bells and fueled conversations regarding data ethics, privacy, and the ownership of personal data. Clearview AI deals specifically with a type of personal data called the *face-image*, or a two-dimensional, photographic representation of the real human face, as in a reflection or digital photo. The scholarship thus far has mostly neglected to explore the ramifications of the face specifically as a form of data and potential object of possession. To understand the face as data and the face as a potentially owned object, it will be necessary to develop how the face operates in terms of the ethical/social relations between humans and what happens when the face is captured in a static face-image and its data extracted through facial recognition technology. Many have speculated that the face acts as a window into the soul or as a canvas for the emotional and moral inner lives of human beings, but how does the face in all of its transparency and opacity operate when two distinct human consciousnesses encounter each other? Using Levinas and Sartre, I will argue that the face acts as a medium for discursive, ethical relations between humans that then becomes objectified upon

being seen or captured (Morris 2015, 67). Furthermore, I will also argue that current facial recognition technology further transforms the objectified face-image by extracting its features and mining it for quantitative data. Given the status of the face, I recommend clear, specific policy delimiting when the processing of digital data is allowed and mandating consumer education about data processing, such that netizens enter digital spaces with complete information regarding the potential for the distribution of their data, including their face-image.

Acknowledgements

I would first like to thank Dr. Ramón Alvarado. I am consistently impressed with his depth of knowledge on data ethics and applied philosophy. This project arose out of insights from his class and conversations had in his office. He is an intellectual inspiration to me, and I have him to thank for introducing me to the wide-ranging, exciting field of data ethics.

I would also like to thank Dr. Ulrick Casimir. Having taken two of his classes, one freshman year and one junior year, I can honestly say that my writing would not be where it is today without his guidance. His candor, wisdom, and sense of humor are always appreciated.

Finally, and perhaps most importantly, I would like to thank my parents. Their financial, moral, and emotional support is what made this project possible. I truly could not have done this without them.

Table of Contents

Introduction

In September 2024, the Netherlands sued American facial recognition company Clearview AI for about $30 million. This was just the latest in a long series of suits, both domestic and abroad, targeting the once secretive startup. Clearview sees itself as "the Google of facial recognition"—their app can take an input of a photo of a person and output virtually every photo of the person on the Internet (Hill 2023). These photos—tens of billions of them—were scraped from sites such as Facebook, Instagram, LinkedIn, and Venmo. It hardly seems a surprise that such an enterprise would encounter stiff social and political resistance. Certainly, many people would intuitively recoil at the idea of a corporation having unauthorized, unlimited access to every photo of them online, especially considering that Clearview's largest customers include police departments and the Department of Homeland Security.

However, though Clearview's actions may raise alarm bells for many, they also raise ethical questions much more thorny and nuanced than they seem on the surface. After all, Clearview sourced their photos from social media sites. Debates have been waged since virtually the dawn of the Internet as to whether the online space constitutes a "public forum" and what expectations of privacy, if any, consumers should have as they surf and post. Examining the nature of this possible privacy breach raises still more questions: did social media users renounce their rights to the ownership of their pictures by posting them online? What rights, if any, did they have in the first place?

The extent to which netizens own their data and may justly exercise privacy rights over it may depend on the type of data in question. With respect to this question, the face is a highly particular form of biometric, personal data. That is to say, while it is wholly unique to each individual and thus can be used to identify any living person, it is also highly public information.

Anyone with a functioning sense of sight can access the visual "data" of another's face, and the intuition of facial identification comes intuitively to most people. Considering the extent to which faces are visible in public settings, enforcing ideas of "privacy" and "ownership" with respect to the face seems like a rather tall order. However, it remains possible that the data of the face and its associated face-image deserves protection for other reasons besides its ready identifiability. Socially, faces serve as a mode of communication and serve as a venue for expressing an individual's emotions. Face-to-face interactions, then, take the form of a conversation.

In *Totality and Infinity*, Emmanuel Levinas takes this face-to-face conversation and places it at the root of ethics and thus the root of all philosophy. His work on developing this confrontation implies what might be ethically important about the face. However, when the face becomes captured in a face-image, something fundamental changes about this interaction: the face becomes a new sort of object. Further changes happening as the face-image is mined for data with facial recognition technology. To explain this phenomenon, we turn to Sartre and his concept of objectification. First, though, it is paramount to understand how facial recognition technology actually works.

Literature Review

How facial recognition works

Facial recognition is "a way of using software to determine the similarity between two face images in order to evaluate a claim" (Crumpler & Lewis 2021, 1). A computer sees a face as a matrix of numbers, each number representing the shade of a different pixel. The image is then fed through filters which perform calculations that gradually simplify the original image into a template that various other images may be compared against. Ideally, a template will be unique to the original image but easily comparable to other instances (Crumpler & Lewis 2021, 5). When two templates are compared against each other, the algorithm assigns the pair a "similarity score" on a scale of 0 to 1. For real matches, there will be a high probability of a high similarity score and a low probability of a low similarity score; for real non-matches, there will be a low probability of a high similarity score and a high probability of a low similarity score (Crumpler & Lewis, 12). A "comparison threshold" determines whether or not the algorithm recognizes the two images as a match. For example, a comparison threshold of 0.8 will yield a match for pairs with a similarity score of 0.8 or higher.

Totality and Infinity

In Lithuanian French philosopher Emmuanel Levinas' seminal work of phenomenology, *Totality and Infinity*, ethics is centered as the origin of philosophy, or the "first philosophy," rather than merely a branch of philosophy (Cailler 2011, 137). Ethics, to Levinas, begins with what he calls the "face to face" relation. Such an encounter between the self and the observable but ultimately unknowable being that Levinas refers to as "the Other" has an effect of a call to moral clarity: "The being that expresses itself imposes itself, but does so precisely by appealing

to me with its destitution and nudity—its hunger—without my being able to be deaf to that appeal. Thus in expression the being that imposes itself does not limit but promotes my freedom, by arousing my goodness." (Levinas 1961, 200). Levinas sees such an encounter as not just powerful but foundational—foundational to the very formulation of reason and dialectics themselves. The encounter with the face of the other demands a response in kind, opening up a discourse that proves inevitable once the expression has occurred and been observed. This is how Levinas can make such a bold claim as "preexisting the plane of ontology is the ethical plane" (201).

To Levinas, the face is the outward appearance of a being possessing an unknowable interiority (Mensch 2015, 114). Thus, "I" can glean only limited information from an encounter with the Other. Their physical features (eyes, nose, mouth, etc.) are available to me, but their interiority (memories, thoughts, sensations) are not. Levinas' philosophical project in *Totality and Infinity* centers the uniqueness of the individual interiority, so it keeps embodiment in mind in its approach to ethics. As a result, Levinas sees any ethics that treat every individual as equivalent as limited (117). Furthermore, he rejects the idea that vision gives the self access to any kind of objective experience of the Other. Levinas uses the example of eating an apple to illustrate this point. When we eat an apple, we experience sensations such as taste, digestion, and perhaps hunger being satiated. It is not that we are experiencing the objective apple or even that we are experiencing objective qualities of the apple mediated by our sensations. Our experience of the apple is a private one that only we, as unique, embodied individuals, have access to. However, such sensations are not attached to the "I," either. The quality of sensation actually precedes the subject-object distinction and transcends the relation between "I and non-I" (116).

Being and Nothingness

` Jean-Paul Sartre builds on the work of the phenomenological tradition to which Levinas belongs in his work in *Being and Nothingness*. Like Levinas, his philosophy is highly embodied, rejecting Cartesian mind-body dualism and instead positing the body as "the continuing subject of conscious experience and action" (Morris 2015, 65). Any embodied subject is capable of being perceived by others (ibid). Additionally, any embodied subject that possesses consciousness must be "object-directed." Sartre's conception of the objected-directed, embodied subject departs from the prior philosophical standard that conceived of the mind as a private, self-contained space that had no direct relation to the outside. Instead, Sartre posits that consciousness *is* the conscious subject's relation to external objects (66). Objects to Sartre can be many things—literal physical objects, feelings or sensations, nonphysical objects of focus (i.e. hopes and dreams)—but the object-directed nature of consciousness is the point and a foundational building block of Sartre's conception of the human experience (ibid).

The pre-Sartrean perspective of the private, self-contained mind was problematized simply by the existence of other consciousnesses. However, Sartre's embodied perspective of consciousness solves this quandary by allowing for interactions between embodied subjects. When the desires of different subjects clash, as expressed through action, conflict emerges, although cooperation may certainly also emerge if said desires correspond with each other (Morris 2015, 66-67). Furthermore, such interactions actually allow individuals to construct their own self-knowledge. "We are selves not only as bodily subjects, but also as constructed, long-term patterns of purposive actions undertaken in the public realm" (67). Others perceive the actions we take publicly, but we do not directly perceive these actions and instead understand them only through occasional self-reflection (ibid). Thus, we may not actually know our own

actions, desires, and goals as much as others do. Here is where the "objectification" occurs—Sartre conceives of the self as an object for ourselves and others rather than as a subject, and the reactions of others help us self-reflect and form ideas about ourselves.

To the layperson, the word "objectification" generally has a rather negative connotation. Feminist scholars have extensively mapped out how sexual objectification can contribute to the domination and subjugation of women. However, as Morris (2015) notes, objectification, while certainly negative in some circumstances, may be a neutral or even positive phenomenon in others (80). Sartre argues that objectification in the broad sense actually plays a foundational role in our self-conception.

The face as data

What kind of data is the image of the face, exactly? As per Crumpler & Lewis' explanation, we know that the computer "sees" a face as a matrix of numbers, which becomes increasingly simplified as filters are applied. However, this tells us little about how a face image ought to be treated ethically. "Personal data" is defined as "data which relate to, or can be used to identify, a living person" (Macnish & Gautier 2020, 43). The face image would obviously qualify, by this definition, as personal data: every face is unique, and a face can readily be used to identify its corresponding human. It is important to note here that the face image being personal data does not all imply a status as de facto *private* data. Anytime a person exists in public, unmasked, they bare their face and thus expose this "data" for anyone watching to see. Of course, this matters little without any accompanying information. A person could show their face in public and still be anonymous if onlookers do not possess any other information which could be used to identify them. If a person's face image gets distributed, this could certainly pose a

threat to their being if the person looking to identify them had malicious intent or the image was from the context of compromising circumstances.

Perhaps people feel so protective of their face image not just because of its potential to be an identifiable data point but because of the psychological and emotional weight that the face carries. Barker & Munster (2016) note that "the human face is often seen, culturally and analytically, as the primary site of the expression of emotion and character, becoming the place for imaging and fixed identity" (103). Faces communicate much, and they are objects of continual fascination for humans. It is no wonder that thinkers from Darwin to Deleuze and Guttiari have spent time studying them. As technology for measuring and imaging the face progresses, so does our conception of the face's emotive and expressive qualities (Barker & Munster 2016, 103). Today, facial recognition technology turns the face into "a completely abstracted and yet highly technical image," manipulated and optimized constantly for the sake of accuracy and efficiency (115).

Data ownership

When the face image becomes digital—i.e. is posted online—the question of who owns the image becomes paramount for answering my research question. While little scholarship that I have found addresses the digital face image specifically, there fortunately exists an ever-growing body of work on data ownership and privacy in the digital age.

Rees (2013), for example, recommends that control of personal data be understood as a matter of legal property rights. Thus, he contends that parties which manage personal data (such as social media companies) actually ought to pay users for the privilege of handling their data/property (Reese 2013, 78). Hummel, Braun, & Dabrock (2020), on the other hand, argue that while data ownership and data as property would be difficult to establish legally, data

ownership rhetoric reflects calls for material redistribution and recognition of data users. Macnish & Gautier (2020) likewise argue that arguments for data ownership do not hold water but instead advocate for a system of shared "custody" of data, where both parties from which the data was sourced and the parties that manage the data have responsibilities as the data changes hands.

If it is not already apparent, there does not seem to be much scholarly consensus on the subject of data ownership. Rees appears to be in the minority in pushing for a strong, legal property regime that applies to personal data. Most scholars of the subject wrestle with the reality that control over the data changes hands, such as between social media users and companies.

The face image can be incorporated into conversations of data ownership when viewed as personal data. Is ownership of one's face the same as ownership of the *image* of one's face? Some might find the concept of owning their own face to be a little odd—the face is, after all, part of the body, not a separate possession that a person owns. However, after the point where face images are posted online, the language of ownership and property begins to be employed. This question is of vital import considering the processes by which face image data are handled online. When social media users upload photos, depending on what they sign in the Terms and Conditions, they may very well sign away the ownership rights of their photos. These photos could then, in theory, be sold to third parties or used to fuel generative AI. If they were scraped by another company, the act might violate the ownership rights of the site *or* the user—that is, if ownership can be established at all. In this situation, ownership may have been passed from the user to the company, the user may be "leasing" their data to the company and thus still retain full property rights over it, or no property/owner relation may exist at all, making the consideration more one of responsibility or of fair treatment of the data. All of this impacts the issue of what

companies might ethically do with the face image data once it is posted to their site. Another important question here would be whether the face image should have special consideration, hearkening back to the previous section.

Framework

I situate my project in the context of the fields of data ethics and AI ethics. Derived from computer and information ethics, data ethics differentiates itself from its predecessors by bringing a data-centric perspective where the focus is on the content of the computation process rather than the hardware (Floridi & Taddeo 2016). AI ethics responds to the concern over the proliferation of new technologies (Kozim & Koshiyama 2020, 1).

My argumentation relies on the groundwork laid in a diverse range of academic areas. Understanding the rights of consumers as they relate to their digital face-image relies on a solid philosophical understanding of ownership. To grasp the nature of the data, I must develop a comprehension of the ethical importance of the human face so I can tell what exactly is at stake. Of course, knowing how facial recognition technology itself works is paramount. Finally, I should have at least a basic knowledge of the current legal and political treatments of facial recognition, and any limitations thereof, so I can best recommend solutions. My aim here is to apply my ethical framework towards practical, workable ideas that will reduce the harms associated with data sharing and facial recognition technology.

It should be noted that while ethics may inspire legal schema, ethics and legality are separate areas. What is legal may not necessarily be ethical, and what is ethical may not necessarily be legal. My thesis will be an ethics thesis, not a legal thesis, so for most of my analysis I focus on developing a strong philosophical footing to ground my concerns. I hope to thoroughly explore the ethics of the capture of the digital face-image, which should imply the ethical grounding on which different actions taken with regards to this data object might lie. The legal components of my thesis thus amount to applying the ethics. Using my work on “the ethics

of the face," I can judge whether different legal actions that have been taken thus far are ethical or not and determine the most ethical legal and political treatment of facial recognition technology.

Analysis & Discussion

When Levinas talks of the face in *Totality and Infinity*, he is of course not just talking about the physical human face but rather using the face to face relation as an image to explore his theories of subject-object interactions. By using *Totality and Infinity* in a project about the face-image, I am applying this subject-object relationship to human beings, in a sense literalizing the metaphor. Depending on the perspective in which we situate the relation, we are all in a sense either selves or Others. Our face-image, in the digital form, is the Other with which the "selves" of corporations, Clearview AI clients, or other digital citizens (for the sake of example) interact. The difference between this type of relation and a physical face to face encounter is that our faces, digitized, objectified, and transformed into data, are unable to speak or otherwise interact. The "discourse" that Levinas believes to be prompted by the face to face encounter is reduced to the self's interpretation of their sensations.

As previously established, the face-image clearly falls within the scope of personal data, as it provides a unique identifier that can be used to track individual human beings. The face-image furthermore falls into the subcategory of biometric data, or data used for recognition/identification purposes based on an individual's biological or behavioral characteristics. Face-images are a visual biomarker, alongside such other identifiers as fingerprints and irises. However, face-images are entirely unique due to the ease with which humans can read and intuit face-image data. While irises cannot be read with the naked eye and reading fingerprints requires specialized training, faces can be compared by virtually any untrained human (World Bank).

Upon being captured in a digital face-image, the face is transformed into a distinct, new object, but of course, the face already *was* an object, as was the body and the "self." In *Being and*

Nothingness, Sartre views objectification as an inherent catalyst for formulating one's self-knowledge in an environment where conscious, embodied selves interact (Morris 2015, 67). The face, however, presents a distinctive case study in objectification, as we have visual access to the faces of others insofar as they are visible to us in a public setting, but we do not have access to our own face except through the mediation of technology or reflection. Since our seeing organs are located on our faces, we cannot ever directly see our own faces (save for glimpses of our hair, nose, or lips that we might catch in our peripheral vision). Our only way to glimpse our own face is through some form of mediation: for instance, a reflection in a pond, a mirror, or as captured through the camera lens.

Before being captured and reflected back to us as a face-image, the face existed to us visually only as an imagined entity. One could perhaps discern some of the qualities of their face through touch or through hearing their face described, but the full visual "picture" of their face would not be clear. The face-image, then, gives us a real visual object with which to conceive of our face. Of course, by the time we view the face-image, the extent to which its visual representation accurately reflects the original object of our "real" face at all is highly questionable. Human eyesight itself is already highly fallible, and the camera further distorts the image of the face in various ways. By the time the face is captured as a digital or photographic face-image, the end product is at best a static, flattened, limited representation of the real object.

Facial recognition further transforms the face-image in a different sense, extracting data from the face-image's representation. Thus, the products of the objectification process diverge further from the original object. Can the manner in which a facial recognition algorithm perceives a face be defined as "sight" at all? The algorithm takes the face-image and produces objects such as matrices, templates, and similarity scores. It can produce analyses of the face

image at a scale and speed that would be virtually impossible for humans. Yet the complete, pictorial representation of the human face and all of the potentialities that it carries is virtually lost. The face in any form—real or a representation—is no longer present to inspire any kind of Levinasian "discourse," and there is no longer a sentient "self" left to participate in the discourse. A Sartrean objectification has at this point occurred numerous times and in numerous ways, and the more advanced facial recognition technology becomes, the more abstracted and higher-order the objectification will likewise become.

A utilitarian might object that this whole arrangement may be justified if the facial recognition apparatus has tangible benefits to human lives. After all, the police departments and government agencies that use Clearview AI's services could use the technology to catch terrorists and violent criminals, potentially saving human lives. It would be difficult to argue that the ethical violation of facial objectification outweighs the saving of human lives. Indeed, the general public largely appears to agree with the utilitarian argument: in a 2022 Pew Research Poll, a plurality of 46% of U.S. adults believed that "the widespread use of facial recognition technology by police would be a good idea for society," as opposed to 27% who believed it would be a "bad idea" (Tyson et al 2022).

It is less clear, however, the extent to which the general public knows how much information can be extracted from their face-images and that virtually everyone who has any sort of public online presence likely appears in Clearview AI's database. If the public's participation in the whole objectification/facial recognition scheme was entirely consensual and well-informed, this would greatly strengthen the utilitarian argument. After all, to a certain extent, participation in systematic and institutionalized objectification can be mitigated by refusing to participate in the spaces where this objectification occurs. For example, someone not wishing to

get x-rayed by the TSA could simply make the choice to not fly. Granted, Clearview AI's scraping of photos from social media sites was a highly clandestine affair before Kashmir Hill broke the story. However, a federal court ruling on a case concerning LinkedIn and HiQ, a company that scraped employee information from LinkedIn, found that the scraping was legal, so clearly, a risk of being legally subject to scraping exists (Hill 2023).

Companies that produce online services generally use terms and conditions and conditions agreements to inform netizens of the risks they take on and rights they forfeit by using the service. However, these contracts—despite being legally binding—are notoriously overlong and difficult to read. A 2013 study applied a "SMOG readability formula" to a number of terms and conditions agreements and found that they were "far beyond what a functionally literate adult could be expected to understand" (Luger et al 2013). Likewise, a 2014 paper published in The Journal of Legal Studies found, after examining the browsing of more than 48,000 netizens accessing the websites of 90 online software companies, that only one to two out of every 1,000 users access the license agreement and most that do only read a small part of it (Bakos et al 2014). Clearly, the flow of information—including who might have access to their face-image and what it might be used for—remains opaque to most netizens.

Conclusion

Considering the free flow of data on the Web, formulating policy that allows netizens to consent to the distribution of their data, including the resulting objectification of their face-image, in an informed manner may seem near impossible. However, such a policy in fact already exists. The European Union General Data Protection Regulation (GDPR) instructs data processors to process data only for the purposes explicitly specified to the person whose data is being processed (data subject), collect only as much data as is necessary for the specified purposes, and store personal data only for as long as is necessary (Wolford 2025). It also mandates strong security protections for personal data and provides guidelines for the acceptable circumstances in which to process data. On the topic of consent, the GDPR states that "consent must be freely given, specific, informed, and unambiguous" and that consent requests must be in "clear and plain language." Notably, "data subjects can withdraw previously given consent whenever they want"—informed participation in the system is ongoing (ibid).

Certainly, the GDPR has its limits. The EU site itself admits that "[t]he regulation itself is large, far-reaching, and fairly light on specifics, making GDPR compliance a daunting prospect" (Wolford 2025). Language such as "clear and plain language" leaves much to be desired. It is easy to imagine tech companies attempting to pass off long, convoluted terms and conditions agreements as "clear and plain language." Overall, the GDPR seems to be more of a statement on the EU's values regarding data protection than actionable policy. Should GDPR norms be imported to other countries, conversations would need to be had amongst lawmakers regarding how to translate the broad regulation into transparent, specific, and implementable laws. Furthermore, I believe that companies could increase transparency and promote informed consent for data processing by launching mass education campaigns to teach consumers about

data processing and distribution. Ideally, whenever someone posts a photo online, they would know exactly where it could end up.

This thesis drew from foundational phenomenology to build a framework for an ethical understanding of the human face. To Levinas, the face was the beginning of ethics, and the self's interaction with the Other inspired a moral discourse, even as vision itself offers only limited information. Sartre's concept of objectification in *Being and Nothingness* helps explain what happens as the face is captured in a face-image and subsequently dissected with facial recognition technology. While the ownership of the face-image by the data subject may be difficult to prove, modern facial recognition technology increasingly appears to resemble a process of hyper-objectification in which a Levinasian discourse is prevented, the remaining relation at the end of the process being one between the face-image transformed into data objects and a non-sentient algorithm.

This situation may seem quite dismal. Fortunately, conversations and scholarship regarding data protection are more abundant than ever. I hope that this thesis contributes to the scholarship by demonstrating how the face is not just a form of data but an indispensable part of human relations, one that deserves protecting.

Bibliography

Bakos, Yannis, Florencia Marotta-Wurgler, and David R. Trossen. 2014. “Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts.” *The Journal of Legal Studies* 43 (1): 1–35. https://doi.org/10.1086/674424.

Barker, Michele, and Anna Munster. 2016. “The Mutable Face.” In *Imaging Identity*, edited by Melinda Hinkson, 101–16. Media, Memory and Portraiture in the Digital Age. ANU Press. https://www.jstor.org/stable/j.ctt1rrd7ms.11.

Crumpler, William, and James A. Lewis. 2021. “How Does Facial Recognition Work?: A Primer.” Center for Strategic and International Studies (CSIS). https://www.jstor.org/stable/resrep32894.

Floridi, Luciano, and Mariarosaria Taddeo. 2016. “What Is Data Ethics?” *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374 (2083): 20160360. https://doi.org/10.1098/rsta.2016.0360.

Hill, Kashmir. 2023. Clearview AI and the end of privacy, with author Kashmir Hill. https://www.theverge.com/23919134/kashmir-hill-your-face-belongs-to-us-clearview-ai-facial-recognition-privacy-decoder.

Hummel, Patrik, Matthias Braun, and Peter Dabrock. 2021. “Own Data? Ethical Reflections on Data Ownership.” *Philosophy & Technology* 34 (3): 545–72. https://doi.org/10.1007/s13347-020-00404-9.

Kazim, Emre, and Adriano Koshiyama. 2020. “A High-Level Overview of AI Ethics.” SSRN Scholarly Paper. Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.3609292.

Levinas, Emmanuel. 1979. *Totality and Infinity*. Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-94-009-9342-6.

Luger, Ewa, Stuart Moran, and Tom Rodden. 2013. “Consent for All: Revealing the Hidden Complexity of Terms and Conditions.” In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2687–96. CHI ’13. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2470654.2481371.

Mensch, James R. 2015. *Levinas’s Existential Analytic : A Commentary on Totality and Infinity*. Evanston, Illinois: Northwestern University Press.

Sutton Morris, Phyllis. 1999. “Sartre on Objectification: A Feminist Perspective.” In *Feminist Interpretations of Jean-Paul Sartre*, 64–89. Penn State Press.

Rees, Christopher. 2013. “Who Owns Our Data?” SSRN Scholarly Paper. Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.2310662.

Sartre, Jean-Paul. 1943. *Being and Nothingness: An Essay in Phenomenological Ontology*. Abingdon, Oxon, Uk: Routledge.

Tyson, Lee Rainie, Cary Funk, Monica Anderson and Alec. 2022. “2. Public More Likely to See Facial Recognition Use by Police as Good, Rather than Bad for Society.” *Pew Research Center* (blog). March 17, 2022. https://www.pewresearch.org/internet/2022/03/17/public-more-likely-to-see-facial-recognition-use-by-police-as-good-rather-than-bad-for-socie•ty/.

Wolford, Ben. 2025. “What Is GDPR, the EU’s New Data Protection Law?” GDPR.eu. 2025. https://gdpr.eu/what-is-gppr.