AI & SOCIETY (2023) 38:2713–2715
https://doi.org/10.1007/s00146-021-01300-2

CURMUDGEON CORNER

Digital wormholes

Elizabeth O'Neill[1]

Received: 25 July 2021 / Accepted: 27 September 2021 / Published online: 21 October 2021

Abstract

Cameras, microphones, and other sensors continue to proliferate in the world around us. I offer a new metaphor for conceptualizing these technologies: they are *digital wormholes*, transmitting representations of human persons between disparate points in space–time. We frequently cannot tell when they are operational, what kinds of data they are collecting, where the data may reappear in the future, and how the data can be used against us. The wormhole metaphor makes the mysteriousness of digital sensors salient: digital sensors have brought us to a strange place. If humans are to be capable of making sensible decisions while under observation by digital sensors, we must improve the epistemic position of potential sensor subjects.

Keywords Digital wormholes · Webcams · Microphones · Surveillance · Sousveillance · Privacy · Security

You're in a science fiction movie. Small wormholes have begun to appear in ordinary places. Two feet from your face. Atop a light-pole. Over the neighbors' door. On the dashboard of the car rounding the street corner. You encounter them wherever you go. They don't transmit matter—they won't vacuum you up and shoot you to another planet. But they're extracting facsimiles of your image and your voice, and they're sending them elsewhere. Versions of you are continuously flowing through these wormholes, yet you yourself only get flashes of information about what's going on. You can see some of the wormholes, but you can't see others. Even when you can see a wormhole, you can't tell what's actually getting transmitted—full conversations? Your heart rate and a map of your bloodflow? Images taken from a hundred meters away, so detailed that they show the pores of your skin? You can't tell when a wormhole's operational. And, these being wormholes, connecting potentially distant points in space–time, you don't know where or when the data will go. It could pop up tomorrow, next year, or on your deathbed. It may go to London or Beijing, your employer or your cousins, law enforcement or a public that will recognize you as you walk down the street. The people who receive these representations of you may keep them as long as they like. They may do with them whatever they wish: they may manipulate the representations so you appear to do or say grotesque things—for their own amusement, to upset you, for blackmail, or to damage your reputation.

The wormholes are metaphor; the scenario's not science fiction. Every day, you are subjected to cameras and other sensors whose presence you cannot reliably detect and whose intended purposes, let alone illicit uses, you cannot reliably ascertain. How the material gathered could be used against you in the future—combined with other information and processed using AI techniques—we have no way of beginning to guess. In sum, we face a sociotechnical world of information-gathering systems that's a lot more mysterious than the world anyone encountered a few hundred years ago or even a few decades ago.

As Nissenbaum (2009) has observed, a *principle of reciprocity* ("information flows bidirectionally," 145) and *principle of notice* ("subjects normally are aware when others see them," 192) have historically operated in the background of our practices of interpersonal observation. If a human nearby is watching you, you can usually see them watching you; if they are close enough to listen to you, you can often hear them, too. If you cannot, it may be because they are being *sneaky* or *peeping* or doing something else that we characterize in pejorative terms to discourage the behavior. We are highly attuned to the presence of others' eyes on us (Barret 2014, 134–137); we can detect another person's gaze unconsciously (Chen et al. 2012). By comparison, when ubiquitous cameras or other sensors replace physically-present human perceivers, we're in an alien world. We

✉ Elizabeth O'Neill
e.r.h.oneill@tue.nl

[1] Philosophy and Ethics, Eindhoven University of Technology, Eindhoven, The Netherlands

can't rely on our instincts to tell us when we're in danger. At the same time, given the newness, complexity, and fast-changing nature of our circumstances, we're also not capable of reasoning through what hazards we might be facing at any given moment.

Action must be taken to buttress the epistemic position of the potential sensor subject. To begin with, more must be done to ensure that the subject can tell that she is being observed. Even in the case where individuals voluntarily bring cameras and microphones into their own homes, the design of the sensors is inadequate. In 2020 and 2021, a time of obligatory online meetings and courses, it has become quite clear how difficult it is for people to continuously monitor whether the cameras and microphones in their vicinity are transmitting or not. Thus we have cases like the mother that inadvertently exposed herself to her daughter's elementary school class (Fox 2020) and the politicians and journalists that have unintentionally appeared naked or engaged in sexual activities in meetings (Guy 2021; Walsh 2021; Embury-Dennis 2020). Worse than the accidental operation of these digital wormholes are cases of purposeful hijacking—e.g. the many cases in which personal cameras have been hacked for the purpose of obtaining footage of people undressed or in compromising circumstances, for the sexual gratification of the hacker or for so-called sextortion (Kelley 2019; Wittes 2016; Perez et al. 2014). Then there are the cases where sensors are imposed on people against their preferences and sometimes without their knowledge—e.g., in restaurants and stores, workplaces, institutional settings, classrooms, public spaces, bathrooms, and so on.

One option is to follow an epistemic balancing principle for sensor design and use, with the aim of returning the sensor subject to the condition in which information reciprocity and notice are in force. For any sensor capable of collecting information about identifiable human persons or protected groups of persons, it must be immediately obvious to any potential sensor subjects whether the sensor is operating, the sensor's range, and what kind of data is being collected; and there must be a procedure by which possible sensor subjects can easily acquire more information about how the sensor operates, the intended uses of the data gathered, and, if applicable, when the data will be destroyed. The reason we need such a principle is that the functioning of interconnected digital sensors diverges so significantly from the functioning of the traditional interpersonal interactions in which our norms and psychology originated.

I don't claim to have a complete solution for the digital wormhole problem—the proliferation of mysterious information-collecting systems. But I do want to highlight one small piece of the solution: a simple, reliable technology that already exists yet has not been made standard issue—namely, the physical slider or lens cap that can be used to cover cameras on laptops, phones, TVs, and similar devices. Presumably, this technology has not been made standard issue—not even on personal devices—because the public does not yet recognize the extent of the dangers posed by proliferating sensors. Among other things, various device producers have repeatedly claimed that their software or other (internal, unobservable) elements of their products will suffice to give device users full control over their cameras. For instance, some promised that their cameras cannot be activated without an indicator light also turning on. An Apple Support article from 2020 regarding Macbooks states, "you will always know when the camera is on" (Apple Support 2020). Yet the multiple instances in which people have managed to activate device cameras without the associated indicator light (Anderson 2013; Soltani and Lee 2013; Brocker and Checkoway 2014; Winder 2020) suggest a security cat-and-mouse game, in which we naïve users are not in a position to tell whether or not the internal design of the device will protect us at any given moment. The physical slider easily addresses the problem of how the user and any other people in the vicinity of a camera can be confident that the device is not collecting visual representations of them. With a physical slider, one can tell at a glance from across a room whether a webcam is covered or not; if one is using one's phone in a crowd, one can easily communicate to those in the vicinity that they are not being recorded. A physical slider slams the wormhole shut.

Unfortunately, cameras on personal devices are just one small part of the digital wormhole problem. Society still faces the question of what to do about the proliferation of microphones and other types of sensors (e.g., thermal, LiDAR, radar, infrared, chemical, radio tomography, ultrasonic). For some of these, in contrast with cameras that can be physically blocked, it may be that there is no technological mechanism that simultaneously can ensure and clearly and reliably indicate that the sensor is not operating. This would mean that we are forced to rely on alternative mechanisms—e.g., laws or norms—for protecting the rights and interests of the potential subjects of these sensors. With regard to cameras, too, many questions remain. What should be done about high definition cameras that are located so far from subjects that they cannot be seen? There is also a critical question about what to do about the easy availability of undetectably small and hidden cameras, which have facilitated a terrible problem with spy-cam pornography—e.g,. filming in bathrooms, hotels, and changing rooms (Armesto-Larson 2020). Again, if there is no technological mechanism that can assure potential sensor subjects of a lack of wormholes in their vicinity, society may have to rely on alternative protective mechanisms, such as severe criminal punishments for people who create or transmit nonconsensual pornography.

Until much stronger technological, legal, or other precautions are put in place, sensors will remain digital wormholes.

To place an internet-connected baby monitor in the nursery is to open a wormhole. Installing a doorbell camera unleashes a wormhole on one's neighborhood. With every robot come wormholes. In the absence of lens covers, a crowd of people with cell phones is a crowd escorted by wormholes. Where possible, then, sensor designers should (at minimum) supply users with the technological means for ensuring and indicating to others that a sensor is non-operational. Where this is not possible, society will need to develop alternative ways to protect sensor subjects, given that our traditional psychological mechanisms for detecting observers and anticipating the consequences of observation no longer suffice to protect us.

Curmudgeon Corner Curmudgeon Corner is a short opinionated columnon trends in technology, arts, science and society, commenting onissues of concern to the research community and wider society. Whilstthe drive for superhuman intelligence promotes potential benefits towider society, it also raises deep concerns of existential risk, therebyhighlighting the need for an ongoing conversation between technologyand society. At the core of Curmudgeon concern is the question: Whatis it to be human in the age of the AI machine? -Editor.

Funding This research has been supported by the Netherlands Organisation for Scientific Research under grant number 016.Veni.195.513; the Ethics of Socially Disruptive Technologies research programme, which is funded through the Gravitation programme of the Dutch Ministry of Education, Culture, and Science and the Netherlands Organisation for Scientific Research under Grant number 024.004.031; and a fellowship at the Cornell Tech Digital Life Initiative funded by NSF Grant #SES-1650589 (PI: Helen Nissenbaum).

Availability of data and materials Not applicable.

Code availability Not applicable.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

Anderson N (2013) Meet the men who spy on women through their webcams. Ars Technica. https://arstechnica.com/tech-policy/2013/03/rat-breeders-meet-the-men-who-spy-on-women-through-their-webcams/

Apple Support (2020) Don't close your MacBook, MacBook Air, or MacBook Pro with a cover over the camera. https://support.apple.com/en-us/HT211148

Armesto-Larson B (2020) Nonconsensual pornography: criminal law solutions to a worldwide problem. Or Rev Int'l l 21:177

Barrett HC (2014) The shape of thought: how mental adaptations evolve. Oxford University Press, Oxford

Brocker M, Checkoway S (2014) iSeeYou: disabling the MacBook webcam indicator LED. In: 23rd USENIX Security Symposium (USENIX Security 14), pp. 337–352

Chen Y-C, Yeh S-L (2012) Look into my eyes and I will see you: unconscious processing of human gaze. Conscious Cogn 21(4):1703–1710

Embury-Dennis T (2020) 'I'm very ashamed': Argentine lawmaker suspended after kissing woman's breast during virtual session of congress." The Independent. https://www.independent.co.uk/news/world/americas/lawmaker-argentina-suspended-kiss-woman-breast-zoom-meeting-video-congress-b595673.html

Fox EG (2020) A mum accidentally flashed her daughter's class on Zoom and shared the story to show parents it's 'OK not to be perfect'. Business Insider. https://www.businessinsider.com.au/mom-accidentally-flashed-her-daughters-zoom-class-2020-5

Guy J (2021) Canadian MP apologizes after appearing naked during video meeting. CNN. https://edition.cnn.com/2021/04/15/americas/canada-politician-naked-camera-scli-intl/index.html

Kelley K (2019) New data on sextortion: 124 additional public cases. Lawfare Blog. https://www.lawfareblog.com/new-data-sextortion-124-additional-public-cases

Nissenbaum H (2009) Privacy in context: technology, policy, and the integrity of social life. Stanford University Press

Perez E, Prokupecz S, Cohen T (2014) More than 90 people nabbed in global hacker crackdown. CNN. https://www.cnn.com/2014/05/19/justice/us-global-hacker-crackdown/index.html

Soltani A, Lee TB (2013) Research shows how MacBook Webcams can spy on their users without warning. The Washington Post. https://www.washingtonpost.com/news/the-switch/wp/2013/12/18/research-shows-how-macbook-webcams-can-spy-on-their-users-without-warning/

Walsh J (2021) Jeffrey Toobin returns to CNN after exposing himself on Zoom call. Forbes. https://www.forbes.com/sites/joewalsh/2021/06/10/jeffrey-toobin-returns-to-cnn-after-exposing-himself-on-zoom-call/

Winder D (2020) iPhone camera hacked: three zero-days used in $75,000 attack chain. Forbes. https://www.forbes.com/sites/daveywinder/2020/04/03/iphone-camera-hijacked-using-three-zero-days-apple-pays-hacker-75000/

Wittes B, Poplin C, Jurecic Q, Spera C (2016) Sextortion: cybersecurity, teenagers, and remote sexual assault. Brookings. https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/