Hilary Term 2020-21

Mini-Project

Paper title: Computers in Society

Your degree: Computer Science and Philosophy

Introduction

This socio-ethical impact assessment will discuss the potential social impacts of the technology Ring.

Ring is a smart video doorbell which allows users to hear and speak to visitors, as well as record video footage and receive motion notifications ("Video Doorbell Pro 2 (Hardwired)", 2021). Ring is available with an accompanying app called Neighbors, allowing users to connect with their community, share video footage and receive local crime alerts ("Neighbors App by Ring", 2019), with the mission: “to reduce crime in communities” (Siminoff, 2014).

Where Ring has relevant connections to external sources (e.g. Ring having close ties with law enforcement), the nature and extent of these current connections will be briefly discussed in order to highlight the potential ramifications of such connections, but the focus will remain on the technology itself. This assessment will outline three potential social impacts: the creation of surveillance networks, widespread facial recognition software and civilian vigilantism.

Creation of surveillance networks

Ring encourages communities to install Ring doorbells (Haskins, 2019c), with each doorbell generating video footage within a small radius of the house. As a private company, all Ring video footage is stored on servers, and any footage which is uploaded to the Neighbors app includes its location (Cameron & Mehrotra, 2019). This combination of centralised (rather than local) storage and geotagging results in a comprehensive video archive of residential areas, creating a small surveillance network.

Whether surveillance is viewed by a person as having a positive or a negative impact will depend on the person’s perspective, rather than the inherent nature of surveillance. For example, a police officer would view surveillance from the perspective of safety (and see it as a positive), whereas a political rights activist would view surveillance from the perspective of freedom (and see it as a negative). As such, it is useful to view Ring doorbells through the lens of the *social construction of technology* (SCOT). Under this theory, the concept of *interpretative flexibility* is used to describe how a technological artefact, such as smart doorbells, can employ different meanings depending on the social context (Pinch & Bijker, 1984), thus it is important not to view Ring doorbells and surveillance from a static standpoint, but rather from the various social contexts of its stakeholders.

Views on surveillance are often polarised, with discussions alternating between the idea that if you have nothing to fear you have nothing to hide, and that of an omniscient, ever-watching ‘Big Brother’ from George Orwell’s “1984”, as a result of a lack of general understanding of the issues surrounding surveillance (Richards, 2013). The following discussion will give a more nuanced outlook on surveillance and surveillance networks, and explain how surveillance can have both positive and negative impacts.

There are several positive impacts that can come from surveillance networks. They can lead to criminal arrests – Suffolk police estimate that around one hundred arrests were made in 2017 as a result of Ring doorbells ("Ring Video Doorbell helps over 100,000 UK homeowners prevent doorstep crime", 2018) – give peace of mind – a Strategy Analytics survey found that peace of mind was one of the drivers for purchasing a Ring doorbell (Watkins, 2020) – deter potential criminals – Ring has a collection of videos showing criminals “caught in the act” and deterred from committing a crime ("Caught in the Act", 2020) – and, according to the police chief in Mountain Brook, Alabama, “create a digital neighborhood watch” (Ng, 2019).

There are, naturally, various negative impacts which can arise from surveillance networks. The first is that surveillance is susceptible to abuse, and the second is that it prevents the exercising of

political freedoms. These impacts arise more readily when the surveillance is state-run or state-owned, both because surveillance information can more easily be linked with government-owned civilian information, and because it is easier for the government to mandate or encourage the use of surveillance technology than it is for a private company to do so. The following three paragraphs discuss Ring's ties with the police, the potential for surveillance abuse, and the potential for surveillance to prevent political freedom.

Ring was founded in 2012 (Siminoff, 2014), and acquired by Amazon in 2018 ("Amazon and Ring Close Acquisition", 2018). Since Ring's acquisition, several deals and agreements with law enforcement agencies have been reported. In 2019, Ring revealed that its Neighbors app was being used by 405 law enforcement agencies in the United States (Siminoff, 2019) and also gave police departments scripts to promote the purchase of their doorbells and use of the Neighbors app (Haskins, 2019b), as well as trading free Ring devices for Neighbors subscribers (Cameron, 2019). While the Neighbors app is not available in the United Kingdom ("Privacy", 2019), Ring reportedly donated over £20 000 worth of Ring products to the Metropolitan Police between 2018 and 2019 ("Amazon Ring internet-connected camera-enabled doorbells", 2019). The police can only access footage which was publicly uploaded or obtained with consent ("How Public Safety Agencies Use Neighbors", 2020), but can keep the footage indefinitely (Holmes, 2020). Ring's many links with the police create a worrying mixture of private and government-funded organisations.

The American Civil Liberties Union (ACLU) set out various ways in which public video surveillance could be abused, including discriminatory abuse and voyeurism ("What's Wrong With Public Video Surveillance?", 2002). A study by Norris and Armstrong found that 10% of targeted surveillances on women for were voyeuristic reasons, and that that voyeuristic footage would be saved and replayed as 'entertainment' (1999). When the choice on who to target is left to human decisions, bias will naturally come into play. One form of bias is racial bias, whereby black people are more likely to be targeted for 'suspicious' behaviour, or considered to be 'not from around here,' and considered as potential criminals without having engaged in any illegal behaviour. The same study found that black people were targeted 32% of the time, but only constituted 9% of arrests (with white people making up the other 91%). It is clear that there must be substantial measures put in place to mitigate these risks, both to prevent abuse from Ring employees (it was found that three Ring employees based in Ukraine had full access to all Ring video footage (Huseman, 2019)) and to prevent abuse from police officers.

One damaging impact that widespread surveillance can have is that it can prevent discussion on potentially controversial or political topics, for fear of reprimand or retribution (Richards, 2013). While this can sometimes be beneficial, such as for preventing terrorism, this can actively prevent others from exercising their beliefs. Under the United Nation's Declaration of Human Rights, every citizen has the right to freedom of religion, opinion and expression ("Universal Declaration of Human Rights", 1948), and surveillance can prevent the exercising of these freedoms when doing so would be heavily frowned upon or considered immoral. Such freedoms could range from the expression of affection between a same-sex couple, to the wearing of religious garments, or even attending certain buildings, such as mosques or pregnancy clinics. Surveillance can also prevent political expressions, such as that of openly supporting an opposing political group in a totalitarian regime. Even if there is no active surveillance at the time, the *threat* of such surveillance is often enough to curtail supposedly problematic behaviour. In order for democracy to thrive, it must be possible to freely choose which political group to join, without threat of repercussion or coercion (Goold, 2009). Much as Winner (1980) discussed how the introduction of nuclear power would necessitate an authoritarian regime, the introduction of smart doorbells would allow, and possibly even necessitate, an authoritarian structure, whereby all video surveillance is captured and stored on a central server, and matched up with other identifying information to create continuous location information on any given individual. This would, of course, be harder for a private company to do than for a government to do (since most private companies are in direct competition with each

other, and would be unwilling to freely share their data), but as mentioned above, Ring's close relations with law enforcement agencies create a worrying reality around centralised surveillance networks.

In order to mitigate these impacts, it is useful to take the structural approach encouraged in Jaques' (2019) paper on "Why the Moral Machine is a Monster". This approach advocates a top-down perspective, where technological decisions are considered as *policies*, and recommends considering what the wider impacts of implementing such policies would be. As mentioned above, it is the highly interconnected nature of Ring and various law enforcement agencies which allows the creation of surveillance networks in the first place. As such, the best mitigation step would be to put in place a policy which enforces the clear separation of private companies and the government. Under the structural approach, such policies would create a world in which law enforcement is required to be upfront and transparent about its affiliates and funding, and would ensure that any requests for video footage from private companies undergo the same scrutinous treatment (such as the requirement of a court order or search warrant) that traditional CCTV requests have required, such as requiring a time limit on the storage of footage.

Widespread face recognition software

If Ring implemented facial recognition software in its doorbells as an added feature to help homeowners identify people near their house, then given the centralised nature of Ring (all footage is stored in one place), facial recognition software could be used to both detect people (based on internal databases of recognised people) and to track people (between footage captured on different Ring doorbells).

Since Ring is owned by Amazon ("Terms of Service", 2020), and Amazon owns facial recognition software ("Amazon Rekognition", 2016), it would be feasible to then deploy that software onto Ring cameras. Indeed, a recent leak showed that Ring was evaluating the implementation of facial recognition software for "unfamiliar face detection" and "familiar face detection" (Cox, 2020).

There are various positive impacts of widespread facial recognition software. When facial recognition software is implemented by a centralised private company, this allows for the creation of a "watch-list" of known criminals, where other Ring doorbells can notify their users of a 'suspicious' person nearing the house, before the person can attempt to steal a package or attempt a break-in, helping to quickly deter criminals. Another use of such a watch-list would be to detect missing people, such as those who have been kidnapped or trafficked; in fact, in December 2019 Amazon announced a partnership with the National Center for Missing and Exploited Children (Huseman, 2019), whereby it would use the Neighbors app to help find missing children – facial recognition would certainly aid this plight.

There are two main negative impacts of widespread facial recognition technology. The first is increased racial discrimination and the second is the violation of privacy.

Racial discrimination occurs as a result of algorithmic bias in facial recognition software. Black people have a higher false match rate when compared to white people in facial recognition software tests (S et al., 2019). This can be due to the fact that photographs of black people are lower quality photographs (as lighting is not adjusted to account for darker skin tones) (S et al., 2019), or because fewer images of black people are used in the training data, making it less accurate. The higher false positive rate can have an acutely damaging effect, leading to a higher rate of wrongly imprisoned black people, and also reinforcing racial biases in police officers performing stop-and-searches or investigations (Bacchini & Lorusso, 2019).

The violation of privacy is a more complex (and less clear-cut) issue. The use of surveillance has traditionally been allowed in public as a result of "the prevailing axiom … that there is no right to

privacy in public spaces" (Hirose, 2017, p16) – that is, being in public means automatically waiving one's right to privacy. It would, therefore, seem a natural extension to say that facial recognition technology too can be installed in public spaces. Hirose's law review in 2017 concluded, however, that facial recognition software should *not* be used in public spaces (unlike surveillance) because of a *reasonable expectation of privacy*, wherein a person in public can reasonably expect to be *seen* (by passersby or surveillance cameras) but not necessarily *identified*, because of practical obscurity, where the steps to be taken (pre-technology) to identify a person would be much more constrained, involving a 'super-recogniser', and the collection of various paper files of information around the country (Hirose, 2017). As a result, a privatised and centralised collection of video footage with facial recognition technology embedded in it would effectively create a query-able location-and-identity database of any person who has ever been outside (since movements would be tracked between Ring doorbells), which, like surveillance, has the potential for a wide variety of abuse.

There are several ways to prevent these impacts, such as using privacy-preserving facial recognition software (which can detect if a face is held within a database without revealing their identity) (Sadeghi et al., 2009). However, the implementation of ad-hoc solutions leaves open the potential for "loop-holes" and various by-passing mechanisms (such as renaming the technology to "facial identification" to avoid regulations concerning "facial recognition"). Thus the most appropriate governance decision would be to sign up to the Association for Computing Machinery (ACM) Code of Ethics, which focuses on the *impact* of design decisions, rather than the decisions themselves, such as requiring the collection of the minimum amount of personal data, and requiring action against potential misuse ("ACM Code of Ethics and Professional Conduct", 2018). Signing up to such a code will also help to make the values that Ring is following more explicit and transparent, providing a more concrete framework to work within.

Encouraging civilian vigilantism

Vigilantism, or vigilante justice, is the investigation or punishment of offences without legal authority (Bateson, 2020). When civilians who are using the Neighbors app witness crimes (or perceived crimes) being committed, they may take affairs into their own hands and attempt to track down, identify or take physical action against the perceived criminal. This would begin with a user sharing a clip of a criminal, and others deciding to track down or punish the criminal.

Civilian vigilantism has been encouraged and proliferated by other apps; one example is "Vigilante": launched in 2016, it gave real-time updates on crimes occurring nearby, but only lasted two days before being taken down due to safety concerns (Hartmans, 2017). A similar app called "Nextdoor" worked as a "private social network for your neighbourhood" ("Nextdoor - Neighbourhood App", 2020), but had calls to be more active in preventing vigilantism (Main, 2020).

There are a few benefits to civilian vigilantism. The apprehension of criminals leads to fewer criminals on the streets, which potentially lowers crime rates. Additionally, if the public deal with criminals involved in petty crimes (such as package theft), this leaves law enforcement free to deal with more major crimes, such as homicides. It may also deter potential criminals, if it is known that their image may be captured on Ring doorbells, and that they may face subsequent vigilante justice.

The main negative impact of civilian vigilantism lies in the definitions of 'criminal' and 'potentially criminal'. The latter has become synonymous with 'suspicious', and the categorisation of people as suspicious and not-suspicious has a disproportionate effect on black people and people of colour; a review by Motherboard found that the *majority* of people reported as "suspicious" were people of colour (Haskins, 2019a). If the police are then called on a black person as a result, they are more likely to be killed by the police than a white person would be (Edwards et al., 2019). This

combination of being more likely to be marked as ‘suspicious’ and being more likely to be killed by the police creates a deadly vigilante-inspiring app.

Civilian vigilantism also helps create a post-truth society. The Neighbors app is a platform for sharing clips among neighbours and other houses in a neighbourhood, allowing users to upload, like, comment and share video clips taken on Ring doorbells. Since Neighbors is classed as a social networking app ("Neighbors by Ring", 2020), and since many social networks act as an echo chamber in which rumours are rapidly propagated (Choi et al., 2020), it is unsurprising that Neighbors creates a filter-bubble-like feed, where like-minded people are encouraged to comment on clips that other users have shared, thus seeing more perspectives which reinforce their beliefs, and continuing the positive feedback loop. This then creates a post-truth society – a society in which feelings and emotional responses become more important than facts when evaluating information (Iyengar & Massey, 2018) – which creates a damaging disregard for logical and scientific evidence, making it difficult for correct information to be circulated (such as certified criminals) when competing with emotion-inducing information (such as black people who have been deemed ‘suspicious’).

The best mitigation for this would be to change the design of the Neighbors app, by removing the comments section for clips and the ability for users to tag people as ‘suspicious’. Doing so will not eliminate users’ racial biases, but will limit the ways in which these can be expressed and will limit the potential damage that could come from such biases.

Conclusion

To conclude, there are several possible social impacts that could come from a widespread implementation of the Ring doorbell and accompanying app, Neighbors, from surveillance networks to widespread facial recognition software to civilian vigilantism, each with varying ethical issues arising from them. While these issues have the potential to be damaging, if the mitigations mentioned herein are correctly applied, then the risks will be much lower, so this company *should* invest in Ring.

References

ACM Code of Ethics and Professional Conduct. ACM. (2018). Retrieved from https://www.acm.org/code-of-ethics.

Amazon and Ring Close Acquisition. Amazon. (2018). Retrieved from https://amazonuk.gcs-web.com/news-releases/news-release-details/amazon-and-ring-close-acquisition-now-working-together-empower.

Amazon Rekognition. Amazon Web Services, Inc. (2016). Retrieved from https://aws.amazon.com/rekognition/.

Amazon Ring internet-connected camera-enabled doorbells. Metropolitan Police. (2019). Retrieved from https://www.met.police.uk/foi-ai/metropolitan-police/disclosure-2020/january/amazon-ring-internet-connected-camera-enabled-doorbells/.

Bacchini, F., & Lorusso, L. (2019). Race, again: how face recognition technology reinforces racial discrimination. *Journal Of Information, Communication And Ethics In Society*, *17*(3), 321-335. https://doi.org/10.1108/JICES-05-2018-0050

Bateson, R. (2020). The Politics of Vigilantism. *Comparative Political Studies*, *1*(33), 3. https://doi.org/10.1177/0010414020957692

Cameron, D. (2019). *Everything Cops Say About Amazon's Ring Is Scripted or Approved by Ring*. Gizmodo. Retrieved from https://gizmodo.com/everything-cops-say-about-amazons-ring-is-scripted-or-a-1836812538.

Cameron, D., & Mehrotra, D. (2019). *Ring's Hidden Data Let Us Map Amazon's Sprawling Home Surveillance Network*. Gizmodo. Retrieved from https://gizmodo.com/ring-s-hidden-data-let-us-map-amazons-sprawling-home-su-1840312279.

Caught in the Act. RingTV. (2020). Retrieved from https://tv.ring.com/category/videos/caught-in-the-act.

Choi, D., Chun, S., Oh, H., Han, J., & Kwon, T. (2020). Rumor Propagation is Amplified by Echo Chambers in Social Media. *Scientific Reports*, *10*(310). https://doi.org/10.1038/s41598-019-57272-3

Cox, K. (2020). *Leaked pics from Amazon Ring show potential new surveillance features*. Ars Technica. Retrieved from https://arstechnica.com/tech-policy/2020/04/ring-cameras-may-someday-scan-license-plates-and-faces-leak-shows/.

Edwards, F., Lee, H., & Esposito, M. (2019). Risk of being killed by police use of force in the United States by age, race–ethnicity, and sex. *National Academy Of Sciences*, *116*(34), 16793-16798. https://doi.org/10.1073/pnas.1821204116

Goold, B. (2009). Surveillance and the Political Value of Privacy. *Amsterdam Law Forum*, *1*(4), 3-6. https://heinonline.org/HOL/P?h=hein.journals/amslawf1&i=389.

Hartmans, A. (2017). *The controversial app for avoiding crime in your area is back in the App Store, and it's now called 'Citizen'*. Business Insider. Retrieved from https://www.businessinsider.com/citizen-vigilante-app-crime-in-your-area-photos-2017-3?r=US&IR=T.

Haskins, C. (2019a). *Amazon's Home Security Company Is Turning Everyone Into Cops*. Vice. Retrieved from https://www.vice.com/en/article/qvyvzd/amazons-home-security-company-is-turning-everyone-into-cops.

Haskins, C. (2019b). *Revealed: The Secret Scripts Amazon Gives to Cops to Promote Ring Surveillance Cameras*. Vice. Retrieved from https://www.vice.com/en/article/wjwea4/revealed-the-secret-scripts-amazon-give-to-cops-to-promote-ring-surveillance-cameras.

Haskins, C. (2019c). *US Cities Are Helping People Buy Amazon Surveillance Cameras Using Taxpayer Money*. Vice. Retrieved from https://www.vice.com/en/article/d3ag37/us-cities-are-helping-people-buy-amazon-surveillance-cameras-using-taxpayer-money?xyz.

Hirose, M. (2017). Privacy in public spaces: The reasonable expectation of privacy against the dragnet use of facial recognition technology. *Connecticut Law Review*, *49*(5), 1591-1620. https://heinonline.org/HOL/P?h=hein.journals/conlr49&i=1637.

Holmes, A. (2020). *Amazon says police can keep videos from Ring doorbells forever and share them with anyone*. Business Insider. Retrieved from https://www.businessinsider.com/police-keep-amazon-ring-doorbell-videos-forever-2019-11?r=US&IR=T.

How Public Safety Agencies Use Neighbors. Ring Help. (2020). Retrieved from https://support.ring.com/hc/en-us/articles/360031595491-How-Public-Safety-Agencies-Use-Neighbors.

Huseman, B. (2019). *Response Letter on Ring*. Vox. Retrieved from https://cdn.vox-cdn.com/uploads/chorus_asset/file/19587577/Response_Letter_on_Ring_1_6_2020.pdf.

Iyengar, S., & Massey, D. (2018). Scientific communication in a post-truth society. *Proceedings Of The National Academy Of Sciences*, *116*(16), 7656-7661. https://doi.org/10.1073/pnas.1805868115

Jaques, A. (2019). *Why the Moral Machine is a Monster*. We Robot. Retrieved from https://robots.law.miami.edu/2019/wp-content/uploads/2019/03/MoralMachineMonster.pdf.

Main, C. (2020). *Nextdoor, Ring Neighbors apps must act to discourage vigilantism*. N.J. Retrieved from https://www.nj.com/hudson/2020/06/nextdoor-ring-neighbors-apps-must-act-to-discourage-vigilantism-opinion.html.

Neighbors App by Ring. Ring. (2019). Retrieved from https://en-uk.ring.com/pages/neighbors.

Neighbors by Ring. App Store. (2020). Retrieved from https://apps.apple.com/us/app/neighbors-by-ring/id1218902777.

Nextdoor - Neighbourhood App. App Store. (2020). Retrieved from https://apps.apple.com/gb/app/nextdoor-neighbourhood-app/id640360962.

Ng, A. (2019). *Amazon's helping police build a surveillance network with Ring doorbells*. CNET. Retrieved from https://www.cnet.com/features/amazons-helping-police-build-a-surveillance-network-with-ring-doorbells/.

Norris, C., & Armstrong, G. (1999). *The maximum surveillance society: the rise of CCTV* (pp. 129, 168, 190). Berg.

Pinch, T., & Bijker, W. (1984). The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. *Social Studies Of Science*, *14*(3), 399-441. Retrieved 11 April 2021, from https://www.jstor.org/stable/285355.

Privacy. Ring. (2019). Retrieved from https://en-uk.ring.com/pages/privacy.

Richards, N. (2013). The Dangers of Surveillance. *Harvard Law Review*, *126*(7), 1934-1965. https://heinonline.org/HOL/P?h=hein.journals/hlr126&i=1964.

Ring Video Doorbell helps over 100,000 UK homeowners prevent doorstep crime. Thames Distribution. (2018). Retrieved from https://thamesdistribution.com/archives/ring-video-doorbell-helps-over-100000-uk-homeowners-prevent-doorstep-crime/.

S, K., Vangara, K., King, M., Albiero, V., & Bowyer, K. (2019). Characterizing the Variability in Face Recognition Accuracy Relative to Race. *2019 IEEE/CVF Conference On Computer Vision And Pattern Recognition Workshops (CVPRW)*, 2278-2285. https://doi.org/10.1109/CVPRW.2019.00281

Sadeghi, A., Schneider, T., & Wehrenberg, I. (2009). Efficient Privacy-Preserving Face Recognition. *International Conference On Information Security And Cryptology*, 229-244. https://doi.org/10.1007/978-3-642-14423-3_16

Siminoff, J. (2014). *The History Behind Ring*. The Ring Blog. Retrieved from https://blog.ring.com/2014/09/26/scrappy-dedicated-humbled-proud-and-excited-the-history-behind-ring/.

Siminoff, J. (2019). *Working Together for Safer Neighborhoods: Introducing the Neighbors Active Law Enforcement Map*. The Ring Blog. Retrieved from https://blog.ring.com/2019/08/28/working-together-for-safer-neighborhoods-introducing-the-neighbors-active-law-enforcement-map/.

Terms of Service. Ring. (2020). Retrieved from https://en-uk.ring.com/pages/terms.

Universal Declaration of Human Rights. (1948). Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights.

Video Doorbell Pro 2 (Hardwired). Ring. (2021). Retrieved 11 April 2021, from https://en-uk.ring.com/products/video-doorbell-pro-2.

Watkins, D. (2020). *Amazon's Ring Leads Google's Nest As 16% Of US Homes Adopt Video Doorbells: Strategy Analytics*. Business Wire. Retrieved from https://www.businesswire.com/news/home/20200213005824/en/Amazon%E2%80%99s-Ring-Leads-Google%E2%80%99s-Nest-As-16-Of-US-Homes-Adopt-Video-Doorbells-Strategy-Analytics.

What's Wrong With Public Video Surveillance?. American Civil Liberties Union. (2002). Retrieved from https://www.aclu.org/other/whats-wrong-public-video-surveillance.

Winner, L. (1980). Do Artifacts Have Politics?. *Daedalus*, *109*(1), 121-136. http://www.jstor.org/stable/20024652.