FREDERICK A. & BARBARA M. ERB INSTITUTE UNIVERSITY OF MICHIGAN

WDI PUBLISHING

case W86C15
July 27, 2020

Andrew Hoffman

Ring Inc. and Law Enforcement: The Cost of Keeping Neighborhoods Safe

Lily Smythe,[i] vice president of marketing at Ring, Inc., stared out at the Pacific Ocean from her office at Ring headquarters in Santa Monica, California. She had made sure to leave her house extra early that morning to beat the usual onslaught of Los Angeles commuter traffic so she could have a few minutes before her morning meeting to gather her thoughts. Smythe had put this meeting on the calendar with her Ring marketing team to discuss how to respond to a recent open letter calling into question Ring's coordination with local law enforcement agencies.

On October 7, 2019, a coalition of civil rights groups made public an open letter to local, state, and federal law enforcement agencies calling for an end to their partnership with Ring on the basis of risks to civil liberties, privacy, and civil rights (see **Exhibit 1**). Smythe and her team believed their response would have important implications for the future of the camera-enabled doorbell company. Smythe saw these partnerships as key to the growth and future success of Ring and the company's response would be equally important to assuage current customers.

Smythe also thought about the future of Ring with regard to public reception about instant personal identification. Amazon.com, the parent company of Ring, had recently filed patents for Rekognition, a facial-identification software that could enhance the powers and value of Ring doorbells.[1] Historically, Amazon had taken a hands-off approach to managing its subsidiary companies, but as owner, Amazon certainly could have final say in important strategic decisions.

How should Ring respond to the risks set forth in the open letter? What should the nature of Ring's relationship be with local, state, and federal law enforcement agencies and how should these agencies be able to utilize the technology? Would features of Ring lead to biased profiling and false arrests? Did sharing information collected from Ring products constitute a violation of privacy and civil liberties for citizens?

[i] Lily Smythe is a fictional character.

Published by WDI Publishing, a division of the William Davidson Institute (WDI) at the University of Michigan.

Smythe and her team faced these and many other questions as they entered the conference room, grabbed coffee, and began crafting a strategy to answer the open letter in a way that would put Ring in a strong position for both the short and long term.

Overview of Ring

Growing up, Jamie Siminoff was always in his garage building and tinkering with things. After college and back in his garage after several failed attempts at launching new products, he found it frustrating how often he was interrupted by the doorbell ringing and wondered if there was a product on the market that would let him answer the door from his phone. Doorbot, which eventually became Ring, was his solution to this common problem.[2]

In 2013, Siminoff pitched the Doorbot doorbell on the television reality series *Shark Tank* as "caller ID for your door." *Shark Tank* panelist Kevin O'Leary made an offer, but Siminoff declined. However, publicity from his appearance on the TV show was enough to drive up sales and attract such investors as Richard Branson and Shaquille O'Neal. Over the next few years the company rebranded to Ring and began to conquer the smart doorbell market, reaching up to 97% share of US video doorbell sales in 2017.[3]

With almost a monopoly on the market, Ring was purchased by Amazon in 2018 for over $1 billion. While details of the deal were not disclosed publicly, a Ring spokesperson stated that Siminoff maintained his role as Ring CEO and Amazon generally allowed Ring to operate independently.[4]

Ring's stated mission was to "reduce crime in neighborhoods" and Siminoff credited his wife for encouraging him to build the product so she could safely answer the door. Ring's blog offered many stories of individuals and families whose homes and safety had been protected because of Ring products. Ring's website said:

> "This mission drives our team and strategy throughout every decision. It's the statement we live by when we design and engineer not only the products you see today, but the future features and innovations that we will deliver for a long time to come. It also makes the late nights and seemingly impossible tasks more bearable as we know our hard work will create happy customers and make a positive impact on our homes, our communities, and the world."[5]

Product

The Ring Doorbell was a 4.98" x 2.43" x 0.87" device that connected to a home Wi-Fi network and sent real-time notifications to a smartphone, laptop, or tablet when someone was at the door. The device activated when someone pressed the doorbell button or when motion was detected near the door. It could be installed to work with existing doorbell wiring or with battery power. Installation was easy with materials like wood, concrete, brick, or even glass.

Once the equipment was installed, the customer downloaded an app and got access to the device, including live streaming video (HD) and two-way audio (see **Exhibit 2**). A subscription "Protect Plan" allowed for a cloud-storage video recording of every ring, motion, and live event in the last 60 days. The Neighbors App, which launched in 2018, allowed users to share footage with other users in the same neighborhood and also provided an option for users to share footage with local police departments (see **Exhibit 3**). According to Ring's blog:

> The Neighbors App gives you real-time crime and safety alerts from your neighbors, the Ring News team and local law enforcement, so we can work together to stop burglaries, prevent package theft and make our communities safer for all. And if you spot something suspicious in your area, you can anonymously post a text, photo or video to keep your community on the lookout.[6]

Ring went on to offer customers security cameras, smart lighting, and do-it-yourself home security systems. Customers could connect multiple Ring products to the Ring application on their phones to monitor their property even if they were not at home. Ring also began offering a professional monitoring subscription service for 24/7 emergency support.

Law Enforcement's Relationship with Technology

Technology and the business sector have always played a significant role in American law enforcement. By the mid-20th century, American policing had been radically affected by technological advances such as the two-way radio, telephones, and patrol cars. More recently, biometrics, robotics, thermal imaging, artificial intelligence (AI), and facial recognition technology further changed the practice of American law enforcement.[7]

In bringing together the necessary stakeholders to implement these kinds of new technology, there was a strong push toward "collaborative policing," meaning multi-sector collaboration in the area of law enforcement.[8] This approach sometimes included working with public sector entities such as social services and public health agencies, but also increasingly included collaboration with large corporations and technology companies such as Ring Inc.[9] Police implemented new tools such as facial recognition because they felt it made policing tactics more effective. While regulations varied widely and concerns were raised about due process and privacy, police departments often argued that collaborating with businesses such as Amazon, to refine facial recognition technology and video surveillance, improved overall public safety.[10]

Regulatory Environment for Technology Use by Law Enforcement

Video Surveillance

Laws and governance regarding the use of video surveillance were sparse at federal, state, and local levels despite an increasing potential to infringe on US citizens' constitutional rights. No Supreme Court rulings were definitive about whether video surveillance infringed on First or Fourth Amendment rights. The statutes that did exist were typically on a state level and limited use to police investigations.[11]

With the improvement of technology and proliferation of systems such as Ring's (and little legal precedent), divisive viewpoints surfaced regarding video surveillance. On one hand, networks of video surveillance could be used by law enforcement to identify and capture dangerous criminals, as seen, for example, with bombings in London in 2005.[12] On the other hand, broad access by law enforcement could infringe on constitutional rights to privacy, anonymity, and due process.

Artificial Intelligence and Facial Recognition

By 2016, according to a report published by the Georgetown Law Center on Privacy and Technology, the faces of more than 117 million American adults were available to law enforcement officials through a face recognition network.[13] The US government regulations on AI primarily focused on autonomous vehicles and weaponry.[14] However, as part of the 36-nation Organization for Economic Cooperation and Development

(OECD), the US government did agree to adopt international guidelines for the development and use of AI.[15] However, policymakers and regulators generally agreed that regulation had not kept pace with the technological advancement.[16]

In an attempt to address this void, in early 2019 a bill was introduced in the US House of Representatives that proposed guidelines for government decision-making with regard to AI. The bill said that the government's chief information officer had to establish an inventory of all the AI procured by the government. This inventory had to include any biases portrayed by the AI or if the AI made decisions that might infringe upon the constitutional rights and privileges of an individual. Some federal legislators also pushed for AI regulation to extend beyond government to the corporate sector. For example, the proposed Commercial Facial Recognition Privacy Act of 2019 would ban commercial use of facial recognition technology for identifying or tracking a user without their consent.[17]

At the state and local levels, legislators pushed to restrict AI use. In 2018, New York City became the first local government to regulate the accountability of automated decision-making. The law made recommendations about how automated decisions are to be shared with the public, and put in place procedures to address decisions that may negatively impact certain groups.[18] In May 2019, San Francisco became the first major city to ban the use of facial recognition software. Other California cities indicated they would follow suit. In Massachusetts, to address racial and gender bias, a bill was introduced to place a moratorium on facial recognition software.[19]

Ring's Partnerships with Law Enforcement

As it grew, Ring developed partnerships with over 400 law enforcement agencies (see **Exhibit 4**) to provide them free access to the Neighbors App, including the Neighbors Portal Tool, so that officers could engage with the community. Officers were given options to post public safety updates and request video footage from Ring users.[20] Ring stated that when "making a video request to Ring, law enforcement must reference a relevant case, and can only request video recordings within a limited time and area. With each request, customers decide whether to share all relevant videos, review and select certain videos to share, take no action (decline), or opt-out of all future requests."[21]

The Neighbors Portal limited the amount of information law enforcement could obtain by blocking direct access to devices and users, user account information, and device locations. However, there were reports of police departments attempting to work around these limitations. In 2019, CNET reported that Ring had shared density maps with law enforcement that allowed them to see concentrations of Ring devices, without needing to utilize specific addresses.[22] Ring then removed this feature. By January 2020, Ring was partnering with 770 police departments, and Vice News reported that Amazon had coached police on how to more successfully get video from Ring users without obtaining a warrant.[23]

Law enforcement agencies viewed partnering with Ring as a "force multiplier," as expressed by Houston Police Officers' Union President Joe Gamaldi, allowing them to expand their coverage and therefore increase public safety.[24] As part of these partnerships, Ring sometimes donated devices to police agencies to provide to the community. Ring maintained that donated devices were "no-strings-attached" and said it worked with law enforcement partners to ensure that residents did not feel pressured to provide footage in exchange for a device. Ring declared:

> Ring customers are in control of their videos, when they decide to share them and whether or not they want to purchase a recording plan. Ring has donated devices to Neighbor's Law Enforcement partners for them to provide to members of their communities. Ring does not support programs that require recipients to subscribe to a recording plan or that footage from Ring devices be shared as a condition for receiving a donated device. We are actively working with partners to ensure this is reflected in their programs.[25]

According to reports by Ring and its partners, the devices worked to reduce crime and support law enforcement in identifying and apprehending suspects. For example, in 2016 Ring and the Los Angeles Police Department gave away doorbells in Wilshire Park, a middle-class neighborhood that was a frequent target for burglaries. The 40 doorbells it gave away represented 10% of the homes in the area, but the burglary rate fell by 55% over six months.[26]

In another case, the Westminster Police Department in California used the Neighbors app to ask if anyone had video relating to the location of a burgled gun safe on a certain day and time. The department received hundreds of videos that helped them identify vehicles associated with the crime and bring two suspects into custody. Detectives said this was their first time using the Ring platform to make arrests and they continued using it to support their efforts.[27]

Competitive Landscape

Ring enjoyed the blue-ocean advantage of being the first company to come to market with a smart doorbell, but had several competitors offering similar products and services.

SimpliSafe

Founded in 2006 and headquartered in Boston, SimpliSafe operated in the safety equipment industry with approximately 800 employees and annual revenue of approximately $130 million.[28] SimpliSafe said it offered "Protection for every window, room and door. Against intruders, fires, water damage, medical emergencies & more. All monitored 24/7 by professionals ready to dispatch police."[29]

SkyBell

SkyBell was founded in 2013, headquartered in Irvine, California, and had a dozen employees. Annual revenue was approximately $1.5 million.[30] SkyBell described its product as "a smart video doorbell that allows you to see, hear, and speak to the visitor at your door whether you're at home, at work, or on the go."[31]

DoorBird

DoorBird was founded in 2007 and headquartered in Berlin, Germany. It employed approximately 64 people and had annual revenues of approximately $1.6 million.[32] DoorBird offered "notification on your smartphone when the doorbell button is pressed. You can see your visitors, talk to them and open the door—from anywhere in the world—via smartphone and tablet. DoorBird stands for the combination of exclusive design with the most innovative IP technology in the field of door communication."[33]

Nest

Nest was founded in 2010 and headquartered in Palo Alto, California. Owned by Google, Nest employed approximately 208 people. It designed and manufactured sensor driven Wi-Fi products, including a doorbell similar to Ring's, and had annual estimated revenues of approximately $110 million.[34] It positioned its

brand this way: "We love home. Home makes you feel safe. Comfortable. But what if your home could do more? Like be more helpful. Truly helpful. What if your home could learn to take care of the people inside it, and the world around it?"[35] Nest had major competitor potential because it was owned by such a powerful data processing company.

Public Concerns

Smythe looked down at her watch as she left what had been a long but productive meeting with her team. It was now 11:23 a.m. PST, and she had promised a response to her team by 2:00 p.m. regarding the direction to take. She felt this would give her team enough time to draft a response to the open letter by end of business that could be released to the public the following morning. She wanted to make sure she thought through each concern carefully, as the response would have serious implications for the company going forward. Based on the notes she had received from her team, as well as their lengthy discourse, she felt the company needed to focus on three key issues.

Privacy

Smythe was keenly aware that many consumer concerns around Ring's video surveillance technology centered on privacy. In fact, Ring had just finished dealing with several security breaches and one had actually been sanctioned by the company. It allowed employees in Ukraine to access users' data, including live video streams, resulting in what was seemingly unnecessary intrusions.[36] The second was when hackers accessed a Ring camera placed in a child's bedroom, speaking to and intimidating the child through the device.[37] Most recently, the company had to deal with the fact that 3,762 Ring owners' data had become compromised. The leaked information included emails, passwords, and access to cameras' live feeds.[38]

The meeting had uncovered complicated issues of privacy the company had to grapple with as the capabilities of Ring expanded. For example, Ring cameras were to be installed only to capture the device owner's private property, not public roads or sidewalks. Ring policy also stated it did not knowingly record footage of children. However, Ring did not verify if device purchasers installed their cameras in line with these policies. So, passersby on the street, including children, could be recorded by a Ring device. This footage could then be accessed by police departments partnering with Ring with owners' consent, and police could keep the footage indefinitely and share it with whomever.[39,40]

Smythe knew that these and other public concerns were recently documented by US Sen. Edward Markey of Massachusetts.[41] Of specific concern was the fact that Ring did not have security requirements for police departments that requested user footage, and the police did not necessarily need a warrant to view users' footage, provided that users consented willingly.[42] While there was no mechanism in place for police to obtain footage without user consent, Smythe and her team wondered about the privacy implications when users complied—for the users themselves, as well as whomever might be captured on that user's footage.

Civil Rights

Smythe's team recognized that partnerships with police departments could trigger anxiety over the implications of the technology on civil rights, particularly racial profiling through neighborhood and police surveillance. The team noted that Ring camera footage could be shared with neighbors to warn people of potential suspicious activity, and misperceptions could increase with regard to racial profiling. Smythe was aware that footage posted to the app featured people of color at disproportionate rates.[43]

There was also concern that the capacity to record and store these videos indefinitely could have civil rights implications. What if, for example, US Immigration and Customs Enforcement officers used this data

to try to track down Dreamers[ii] or undocumented immigrants?[44] What if Ring decided to develop facial recognition technology to scan footage for specific people or *types* of people?

Facial Recognition

Ring did not use facial recognition technology per se, but published reports[45] had asserted that this could be a next step for the footage captured by Ring cameras. Smythe realized the potential negative implications of facial recognition technology were varied and far-reaching. AI technology seemed benign: how could an inanimate software possibly harbor ill-will or biases? However, as Smythe knew, all AI software was coded by people and people had biases, whether implicit or explicit. In addition, AI could be built on data that was already biased in nature.

Smythe shivered as she thought back to the example of the New Orleans Police Department (NOPD) using an algorithm designed by the software company Palantir to predict and curb crime before it occurred. Smythe knew that the software likely exacerbated racial biases in policing, and that New Orleans faced at least one lawsuit regarding use of the software.[46] The algorithm was partially based on the NOPD's Field Interview Card database that included encounters, reported by police, that did not result in an arrest. If a police officer held racial biases, s/he may have interacted more often with citizens of color, thus ensuring that citizens of color would be overrepresented in the database.[47] These individuals would then show up more frequently in searches on Palantir's software, regardless of whether they had committed a crime or were likely to do so. These same issues could easily arise with Ring's facial recognition software, in something as seemingly benign as a neighborhood watch list.

Decision Time

It was now 1:30 p.m. and Smythe opened a new memo on her computer. She needed to assemble her thoughts to deliver to her team. Her goal was to give them an actionable direction to take in terms of response to the open letter. How should Ring respond to allegations that company technology infringed on constitutional rights to privacy, anonymity, and due process? Should Ring be used to serve the public interest beyond just identifying who is at your porch on your property? Should Ring continue to expand its partnership and capabilities with federal, state, and local law enforcement agencies? What should this partnership look like? Does Ring have an obligation to its customers to establish firmer regulation around the use of customer data and emerging technology? Smythe grappled with these questions among many more as she started forming her strategy.

[ii] The DREAM Act (Development, Relief and Education for Alien Minors) was a bill in Congress that would have granted legal status to certain undocumented immigrants who were brought to the United States as children and went to school in this country.

Exhibits

Exhibit 1

Open Letter Addressing Ring's Partnerships with Law Enforcement

Open letter calling on elected officials to stop Amazon's doorbell surveillance partnerships with police

Posted October 7, 2019, 3:18 PM

Dear local, state, and federal officials,

The Washington Post has reported that there are currently more than 400 police departments across the United States who have entered into surveillance partnerships with Amazon's camera enabled doorbell company, Ring. These partnerships pose a serious threat to civil rights and liberties, especially for black and brown communities already targeted and surveilled by law enforcement.

A key component of the partnership turns police departments into marketing agencies and police officers into salespeople for Amazon. Amazon provides officers with talking points to promote their technology and products to residents, and requests departments market the products at city events. While Amazon gives participating departments free products for promotion, the majority of the products are privately purchased from Amazon. In some municipalities taxpayer money has been used to subsidize Amazon surveillance products for residents' use. On the back end, Amazon carefully scripts everything that authorities say about the program, and coaches police on the best talking points to get customers to hand over their footage.

With no oversight and accountability, Amazon's technology creates a seamless and easily automated experience for police to request and access footage without a warrant, and then store it indefinitely. In the absence of clear civil liberties and rights-protective policies to govern the technologies and the use of their data, once collected, stored footage can be used by law enforcement to conduct facial recognition searches, target protesters exercising their First Amendment rights, teenagers for minor drug possession, or shared with other agencies like ICE or the FBI.

Amazon's internal corporate policies raise serious privacy concerns. The Ring technology gives Amazon employees and contractors in the US and Ukraine direct access to customers' live camera feeds, a literal eye inside their homes and areas surrounding their homes. These live feeds provide surveillance on millions of American families—from a baby in their crib to someone walking their dog to a neighbor playing with young children in their yard—and other bystanders that don't know they are being filmed and haven't given their consent. Additionally, the technology has no end-to-end encryption leaving this extremely private and sensitive footage vulnerable to cyber-attacks, stalkers, or foreign governments.

Amazon has not been transparent about plans to integrate facial recognition into Ring cameras. Amazon Ring has denied any connection between their technology and facial recognition software, but according to the Washington Post, Ring filed two patents in November 2018 "that describe technology with the ability to identify "suspicious people" and create a "database of suspicious persons." Ring's terms of service allow the company to "access and use your User Recordings" for "developing new Products and Services," which covers facial recognition. The Information reported Ring's Ukraine-based research team accessed customer's surveillance footage to train image recognition software. As facial recognition software has been shown to disproportionately misidentify people of color, women and transgender people, it further compounds existing civil liberties concerns and expands suspected criminality centered in racial profiling and gender bias.

As Amazon continues to grow in influence, so do the costs and effects of their domination. Freedom of information requests reveal Amazon carefully scripted and regulated the talking points police departments could use in discussing the Amazon-police partnership. Departments were forbidden from using words like 'surveillance' in any communication related to the partnership. This level of censorship and control is indicative of Amazon's business model of using monopolistic practices to vacuum up enormous amounts of data. That data is then leveraged to bolster Amazon's corporate interests, often at the expense of local businesses and smaller competitors. Amazon's latest encroachment with the Ring-police partnerships exemplify the company's willingness to do what it takes to expand their data empire. Once they have this data, there is nothing stopping them from using it for their own profit-driven purposes.

Amazon Ring partnerships with police departments threaten civil liberties, privacy and civil rights, and exist without oversight or accountability. Given its significant risks, no surveillance partnerships with Amazon Ring should have been established, or should be established in the future, without substantial community engagement and input and elected official approval. To that end, we call on mayors and city councils to require police departments to cancel any and all existing Amazon Ring partnerships, and to pass surveillance oversight ordinances that will deter police departments from entering into such agreements in the future. We further call on Congress to investigate Ring's practices and demand more transparency from the company.

Sincerely,

The undersigned:

Fight for the Future, Media Justice, Color of Change, Secure Justice, Demand Progress, Defending Rights & Dissent, Muslim Justice League, X-Lab, Media Mobilizing Project, Restore The Fourth, Inc., Media Alliance, Youth Art & Self Empowerment Project, Center for Human Rights and Privacy, Oakland Privacy, Justice For Muslims Collective, The Black Alliance for Just Immigration (BAJI), Nation Digital Inclusion Alliance, Project On Government Oversight, OpenMedia, Council on American-Islamic Relations-SFBA, Million Hoodies Movement for Justice, Wellstone Democratic Renewal Club, MPower Change, Mijente, Access Humboldt, RAICES, National Immigration Law Center, The Tor Project, United Church of Christ, Office of Communication Inc., the Constitutional Alliance, RootsAction.org, CREDO Action, Presente.org, American-Arab Anti-Discrimination Committee, and United We Dream.

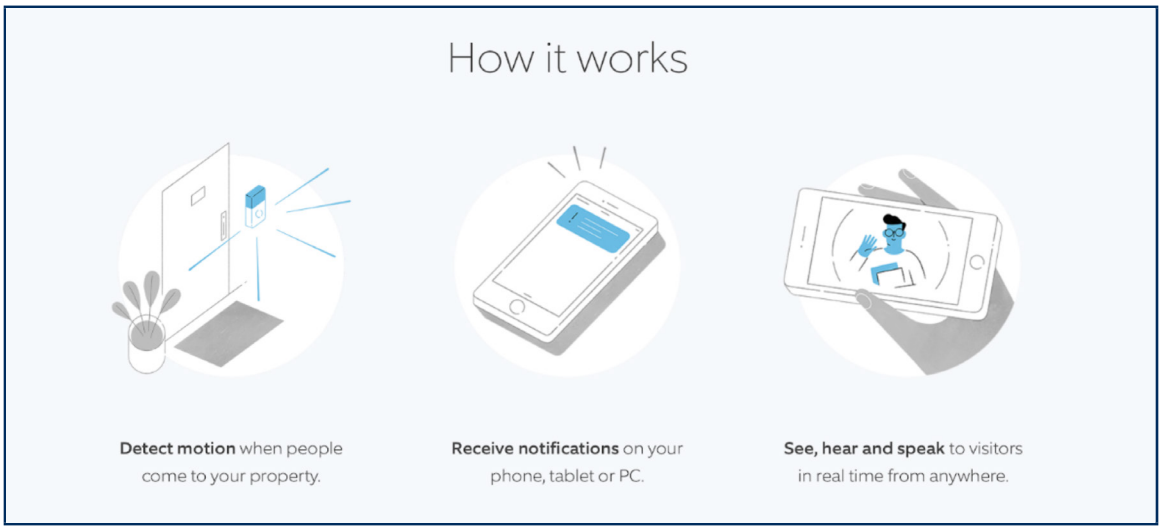
Tags: #press-release

Source: "Open letter calling on elected officials to stop Amazon's doorbell surveillance partnerships with police." https://www.fightforthefuture.org/news/2019-10-07-open-letter-calling-on-elected-officials-to-stop/.

Exhibits (cont.)

Exhibit 2

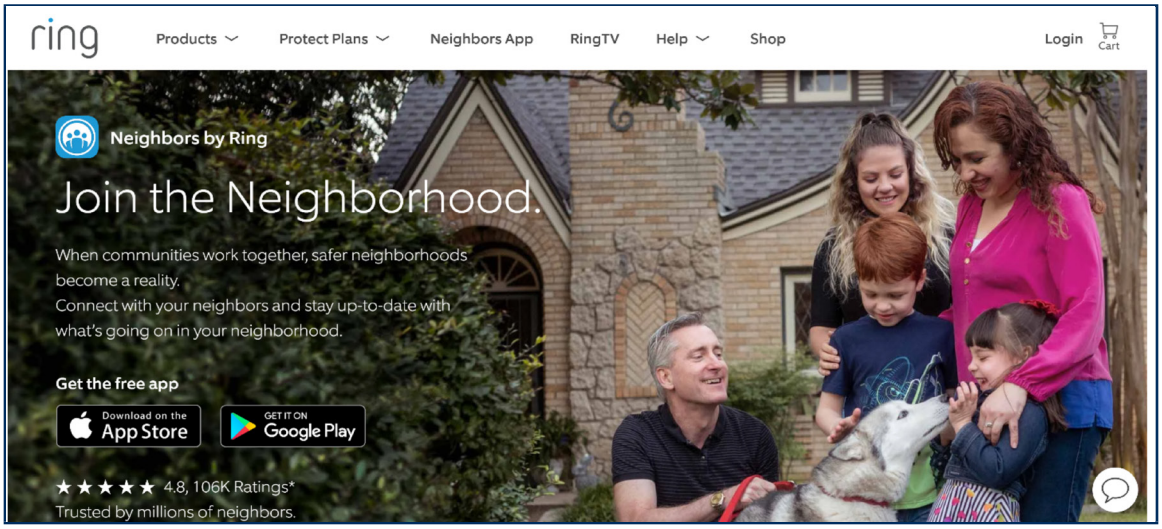
How the Ring Doorbell Works



Source: "Ring Video Doorbells." *Ring Inc.* https://shop.ring.com/pages/doorbell-cameras.

Exhibit 3

Neighbors by Ring App Online Advertisement



Source: "Neighbors by Ring." *Ring Inc.* https://store.ring.com/neighbors.

Exhibits (cont.)

Exhibit 4
Ring Inc. Active Law Enforcement Map

"We share updates when new law enforcement agencies join Neighbors through the app, social media and local press, but our users have asked for an additional way to search this information. Our new Active Law Enforcement Map makes it even easier for users to see if their local law enforcement team is involved with Neighbors. We will keep the map updated so users can search either by zip code, address or visually by zooming into a region or city."

Source: Siminoff, Jamie. "Working Together for Safer Neighborhoods: Introducing the Neighbors Active Law Enforcement Map." *Ring Inc.*, 28 Aug. 2019. Blog. https://blog.ring.com/2019/08/28/working-together-for-safer-neighborhoods-introducing-the-neighbors-active-law-enforcement-map/. Accessed 17 Apr. 2020.

Endnotes

1 Fowler, Geoffrey. "The Doorbells Have Eyes: The Privacy Battle Brewing over Home Security Cameras." *Washington Post*, 31 Jan. 2019. www.washingtonpost.com/technology/2019/01/31/doorbells-have-eyes-privacy-battle-brewing-over-home-security-cameras/. Accessed 3 Feb. 2020.

2 Wetzel, Kim. "From Sharks to Shaq: Ring CEO Jamie Siminoff's unusual road to success." *Digital Trends*. 29 Sept. 2018. https://www.digitaltrends.com/home/ring-ceo-jamie-siminoff-unusual-road-to-success/. Accessed 4 Feb. 2020.

3 Adams, Susan. "The Exclusive Inside Story of Ring: From 'Shark Tank' Reject to Amazon's Latest Acquisition." *Forbes*. 27 Feb. 2018. https://www.forbes.com/sites/susanadams/2018/02/27/amazon-is-buying-ring-the-pioneer-of-the-video-doorbell-for-1-billion/#3aab8a7d706c. Accessed 4 Feb. 2020.

4 Adams, Susan. "The Exclusive Inside Story of Ring: From 'Shark Tank' Reject to Amazon's Latest Acquisition." *Forbes*. 27 Feb. 2018. https://www.forbes.com/sites/susanadams/2018/02/27/amazon-is-buying-ring-the-pioneer-of-the-video-doorbell-for-1-billion/#3aab8a7d706c. Accessed 4 Feb. 2020.

5 "Our Mission: To Reduce Crime in Neighborhoods." *Ring Inc*. https://shop.ring.com/pages/about. Accessed 3 Feb. 2020.

6 "Introducing the Neighbors App: The New Neighborhood Watch." *Ring Inc*. 8 May 2018. https://blog.ring.com/2018/05/08/introducing-the-neighbors-app-the-new-neighborhood-watch/. Accessed 3 Feb. 2020.

7 McCampbell, Michael S. "The Collaboration Toolkit for Community Organizations: Effective Strategies to Partner with Law Enforcement." *U.S. Department of Justice, Office of Community Oriented Policing Services*, 2014. Washington, D.C. http://rems.ed.gov/docs/COPS_CollaborationToolkit_CommunityOrgs.pdf. Accessed 5 Feb. 2020.

8 "Smart Policing Collaboration Principles." *The Henry C. Lee Institute of Forensic Science, University of New Haven*, 2017. http://www.henryleeinstitute.com/wp-content/uploads/2017/03/SPICollaborationPrinciples.pdf. Accessed 5 Feb. 2020.

9 "Smart Policing Collaboration Principles." *The Henry C. Lee Institute of Forensic Science, University of New Haven*, 2017. http://www.henryleeinstitute.com/wp-content/uploads/2017/03/SPICollaborationPrinciples.pdf. Accessed 5 Feb. 2020.

10 Fussell, Sidney. "The Always-On Police Camera." *The Atlantic*, 26 Sept. 2018. https://www.theatlantic.com/technology/archive/2018/09/body-camera-police-future/571402/. Accessed 3 Feb. 2020.

11 "Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties." *The Constitution Project*, 2006. https://www.law.berkeley.edu/files/Video_surveillance_guidelines.pdf. Accessed 3 Apr. 2020.

12 "Guidelines for Public Video Surveillance: A Guide to Protecting Communities and Preserving Civil Liberties." *The Constitution Project*, 2006. https://www.law.berkeley.edu/files/Video_surveillance_guidelines.pdf. Accessed 3 Apr. 2020.

13 Garvie, Clare, et al. "The Perpetual Line-Up: Unregulated Police Face Recognition in America." *Georgetown Law Center on Privacy and Technology*, 18 Oct. 2016. https://www.perpetuallineup.org/. Accessed 3 Apr. 2020.

14 United States, Congress, House. John S. McCain National Defense Authorization Act for Fiscal Year 2019. *Congress.gov*, https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf. 115th Congress, 2nd session, House Resolution 5515, Section 238, passed 3 Jan. 2018.

15 Delcker, Janosch. "US to endorse new OECD principles on artificial intelligence." *Politico*. 19 May 2019. https://www.politico.eu/article/u-s-to-endorse-new-oecd-principles-on-artificial-intelligence/. Accessed 3 Apr. 2020.

16 Fitch, Asa. "Facial-Recognition Software Suffers from Racial Bias, U.S. Study Finds." *Wall Street Journal*. 20 Dec. 2019. www.wsj.com/articles/facial-recognition-software-suffers-from-racial-bias-u-s-study-finds-11576807304. Accessed 5 Feb. 2019.

17 McNerney, Jerry. "H.R.2575 - 116th Congress (2019-2020): AI in Government Act of 2019." *Congress.gov*, Government Printing Office, 19 Dec. 2019, www.congress.gov/bill/116th-congress/house-bill/2575.

18 Kelly, Ben, and Yoon Chae. "INSIGHT: AI Regulations Aim at Eliminating Bias." *Bloomberg Law*. 31 May 2019. news.bloomberglaw.com/tech-and-telecom-law/insight-ai-regulations-aim-at-eliminating-bias. Accessed 3 Apr. 2020.

19 Conger, Kate, Richard Fausset and Serge F. Kovaleski. "San Francisco Bans Facial Recognition Technology." *New York Times*, 14 May 2019. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html. Accessed 5 Feb 2020.

20 Siminoff, Jamie. "Working Together for Safer Neighborhoods: Introducing the Neighbors Active Law Enforcement Map." *Ring Inc*. 28 Aug. 2019. https://blog.ring.com/2019/08/28/working-together-for-safer-neighborhoods-introducing-the-neighbors-active-law-enforcement-map/. Accessed 5 Feb. 2020.

21 "How Law Enforcement Uses the Neighbors App." *Ring Inc.* https://support.ring.com/hc/en-us/articles/360031595491. Accessed 5 Feb. 2020.

22 "Ring let police view map of video doorbell installations for over a year." *CNET*, 3 Dec. 2019. https://www.cnet.com/news/ring-gave-police-a-street-level-view-of-where-video-doorbells-were-for-over-a-year/. Accessed 3 Feb. 2019.

23 Molla, Rani. "How Amazon's Ring Is Creating a Surveillance Network with Video Doorbells." *Vox*, 28 Jan. 2020. www.vox.com/2019/9/5/20849846/amazon-ring-explainer-video-doorbell-hacks. Accessed 3 Apr. 2020.

Endnotes (cont.)

[24] Barned-Smith, St. John. "Houston police team up with Ring app to tackle crime." *Houston Chronicle*, 15 Jan. 2019. https://www.chron.com/news/houston-texas/houston/article/Houston-police-team-up-with-Ring-app-to-tackle-13533508.php. Accessed 5 Feb. 2020.

[25] Ng, Alfred. "Amazon's helping police build a surveillance network with Ring doorbells." *CNET*, 5 June 2019. https://www.cnet.com/features/amazons-helping-police-build-a-surveillance-network-with-ring-doorbells/. Accessed 3 Apr. 2020.

[26] Adams, Susan. "The Exclusive Inside Story of Ring: From 'Shark Tank' Reject to Amazon's Latest Acquisition." *Forbes*. 27 Feb. 2018. https://www.forbes.com/sites/susanadams/2018/02/27/amazon-is-buying-ring-the-pioneer-of-the-video-doorbell-for-1-billion/#3aab8a7d706c. Accessed 4 Feb. 2020.

[27] Peralta, Jessica. "Ring's Neighbors App helps Westminster detectives in crime-solving efforts." *Behind the Badge*, 27 Feb. 2018. https://behindthebadge.com/rings-neighbors-app-helps-westminster-detectives-in-crime-solving-efforts/. Accessed 5 Feb. 2020.

[28] "Ring." *Owler*. https://www.owler.com/company/ring. Accessed 15 Feb. 2020.

[29] "Whole Home Protection." *SimpliSafe*. https://simplisafe.com/. Accessed 17 Feb. 2020.

[30] "Ring." *Owler.* https://www.owler.com/company/ring. Accessed 15 Feb. 2020.

[31] "SkyBell." *SkyBell*. http://www.skybell.com/. Accessed 17 Feb. 2020.

[32] "Ring." *Owler*. https://www.owler.com/company/ring. Accessed 15 Feb. 2020.

[33] "More than just a door intercom." *DoorBird*. https://www.doorbird.com/. Accessed 15 Feb. 2020.

[34] "Nest." *Owler*. https://www.owler.com/company/nest. Accessed 15 Feb. 2020.

[35] "Introducing Google Nest." *Google*. https://store.google.com/us/category/google_nest. Accessed 10 June 2020.

[36] Deahl, Dani. "Ring let employees watch customer videos, claim reports." *The Verge*, 10 Jan. 2019. https://www.theverge.com/2019/1/10/18177305/ring-employees-unencrypted-customer-video-amazon. Accessed 3 Apr. 2020.

[37] Chiu, Allyson. "She installed a Ring camera in her children's room for 'peace of mind.' A hacker accessed it and harassed her 8-year-old daughter." *Washington Post*, 12 Dec. 2019. https://www.washingtonpost.com/nation/2019/12/12/she-installed-ring-camera-her-childrens-room-peace-mind-hacker-accessed-it-harassed-her-year-old-daughter/?arc404=true. Accessed 3 Apr. 2020.

[38] Haskins, Caroline. "A Data Leak Exposed the Personal Information of Over 3,000 Ring Users." *BuzzFeed News*. 19 Dec. 2019. https://www.buzzfeednews.com/article/carolinehaskins1/data-leak-exposes-personal-data-over-3000-ring-camera-users. Accessed 6 Feb. 2019.

[39] Harwell, Drew. "Police can keep Ring camera video forever and share with whomever they'd like, Amazon tells senator." *Washington Post*, 19 Nov. 2019. https://www.washingtonpost.com/technology/2019/11/19/police-can-keep-ring-camera-video-forever-share-with-whomever-theyd-like-company-tells-senator/. Accessed 3 Apr. 2020.

[40] Molla, Rani. "Activists are pressuring lawmakers to stop Amazon Ring's police surveillance partnerships." *Vox*, 19 Nov. 2019. https://www.vox.com/recode/2019/10/8/20903536/amazon-ring-doorbell-civil-rights-police-partnerships. Accessed 3 Apr. 2020.

[41] "Senator Markey Investigation into Amazon Ring Doorbell Reveals Egregiously Lax Privacy Policies and Civil Rights Protections." *Senator Edward Markey*, 19 Nov. 2019. https://www.markey.senate.gov/news/press-releases/senator-markey-investigation-into-amazon-ring-doorbell-reveals-egregiously-lax-privacy-policies-and-civil-rights-protections. Accessed 3 Apr. 2020.

[42] "Senator Markey Investigation into Amazon Ring Doorbell Reveals Egregiously Lax Privacy Policies and Civil Rights Protections." *Senator Edward Markey*, 19 Nov. 2019. https://www.markey.senate.gov/news/press-releases/senator-markey-investigation-into-amazon-ring-doorbell-reveals-egregiously-lax-privacy-policies-and-civil-rights-protections. Accessed 3 Apr. 2020.

[43] Molla, Rani. "Activists are pressuring lawmakers to stop Amazon Ring's police surveillance partnerships." *Vox*, 19 Nov. 2019. https://www.vox.com/recode/2019/10/8/20903536/amazon-ring-doorbell-civil-rights-police-partnerships. Accessed 3 Apr. 2020.

[44] Fowler, Geoffrey A. "The doorbells have eyes: The privacy battle brewing over home security cameras." *Washington Post*, 31 Jan. 2019. https://www.washingtonpost.com/technology/2019/01/31/doorbells-have-eyes-privacy-battle-brewing-over-home-security-cameras/. Accessed 3 Apr. 2020.

[45] Biddle, Sam. "Amazon's Ring Planned Neighborhood 'Watch Lists' Built on Facial Recognition." *The Intercept*, 26 Nov. 2019. https://theintercept.com/2019/11/26/amazon-ring-home-security-facial-recognition/. Accessed 3 Apr. 2020.

[46] Collins, Dave. "'Predictive Policing': Big-City Departments Face Lawsuits." *Associated Press*, 5 July 2018. apnews.com/b11e4bca11e548d3af7a63f24e348c6f. Accessed 3 Apr. 2020.

[47] Johansson, Anna. "5 Lessons Learned from the Predictive Policing Failure in New Orleans." *VentureBeat*, 20 Mar. 2018. venturebeat.com/2018/03/19/5-lessons-learned-from-the-predictive-policing-failure-in-new-orleans/. Accessed 3 Apr. 2020.

Notes

FREDERICK A. & BARBARA M.
ERB INSTITUTE
UNIVERSITY OF MICHIGAN

The **Erb Institute** is committed to creating a socially and environmentally sustainable society through the power of business. Building on nearly two decades of research, teaching, and direct engagement, the Institute has become one of the world's leading sources of innovative knowledge on the culture, technologies, operations and governance of business in a changing world.
http://erb.umich.edu

WILLIAM DAVIDSON INSTITUTE
AT THE UNIVERSITY OF MICHIGAN

Established at the University of Michigan in 1992, the **William Davidson Institute** (WDI) is an independent, non-profit research and educational organization focused on providing private-sector solutions in emerging markets. Through a unique structure that integrates research, field-based collaborations, education/training, publishing, and University of Michigan student opportunities, WDI creates long-term value for academic institutions, partner organizations, and donor agencies active in emerging markets. WDI also provides a forum for academics, policy makers, business leaders, and development experts to enhance their understanding of these economies. WDI is one of the few institutions of higher learning in the United States that is fully dedicated to understanding, testing, and implementing actionable, private-sector business models addressing the challenges and opportunities in emerging markets.