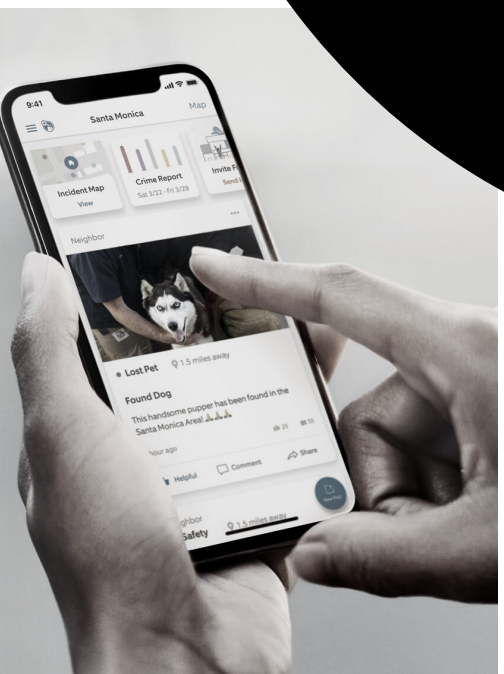
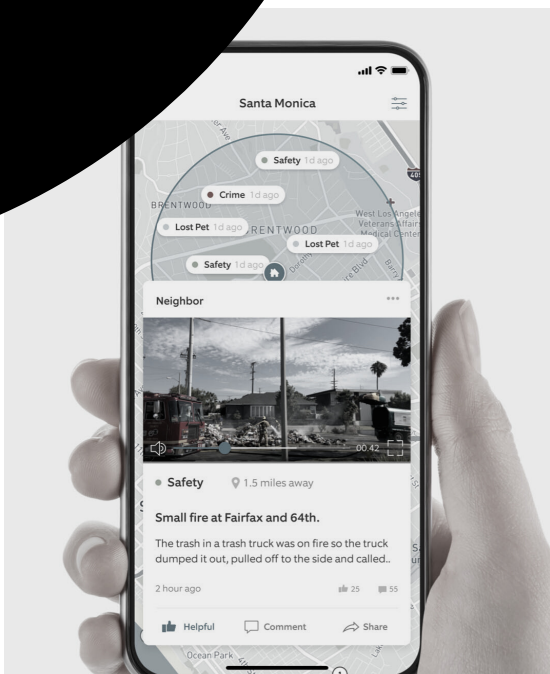
RING NEIGHBORS & NEIGHBORS PUBLIC SAFETY SERVICE

A CIVIL RIGHTS & CIVIL LIBERTIES AUDIT

Policing Project
NYU School of Law





About the Policing Project

The Policing Project at New York University School of Law partners with communities, policymakers, police, and technology companies across the country to bring democratic accountability to policing so that it better matches American ideals and community needs. Our work is intended to help center a community-driven vision for public safety, one that is equitable, non-discriminatory and respectful of public values.

For more information, visit www.PolicingProject.org.

This report was written by Policing Project Founder and Faculty Director Barry Friedman, Executive Director Farhang Heydari, Staff Attorney Max Isaacs, and Policing Fellow Julian Clark.

Table of Contents

Executive Summary

Ring is one of the nation's largest home security companies, best known for its smart video doorbell. Tens of millions of U.S. households own a smart doorbell sold by Ring or one of its competitors. Consumer spending on home security is expected to grow to nearly $10 billion by 2023. Because Ring and other companies in the private security market facilitate sharing of surveillance information with the police, the growth of this market has and will continue to have a profound impact on how communities are policed.

Ring also offers a free app called "Neighbors" and an analog exclusively for public safety agencies called "Neighbors Public Safety Service" (NPSS). Members of the public – whether they own a Ring doorbell or not – can use Neighbors to share information about local crime and safety issues with others in their neighborhood, and to receive information from local public safety agencies. Neighbors has more than 10 million monthly active users across the country. At present, there are approximately 2000 policing agencies and 400 fire departments on NPSS.

Police and other public safety agencies use NPSS to share crime and safety information with their communities through Neighbors. Importantly, police also use the "Request for Assistance" ("RFA") feature of NPSS to request information, including videos, from users within a specific geographic area. RFAs make it easier for police to solicit such information from the public to use in their investigations.

We undertook this audit to examine how Ring allows policing agencies to use its products and services–with a particular focus on NPSS. The purpose of the audit was to provide an objective accounting of how Ring's products and services operate, to assess the possible civil rights, civil liberties, and racial justice harms that arise when a company facilitates the sharing of private surveillance information with the police, and to encourage changes within Ring that can mitigate any harms we identified. During the audit, Ring gave us access to information about NPSS that to this point has never been disclosed publicly, such as the amount of video accessed by police via NPSS and the types of crimes police use NPSS to investigate.

We considered several potential risks or harms that could follow from the relationship between Ring and policing. These include, among others, the possibility that Ring's services could increase overreliance on policing, engender bias, or impede democratic governance of police. We discuss these and others at length in Part II.

In response to the risks and harms we identified, Ring has implemented ***over one hundred changes*** to its policies and practices. We enumerate key changes in Part IV. Among the more notable are that:

- Ring now displays publicly every police request for information via NPSS, known as a Request for Assistance. In addition, Ring has created public profiles for every agency on NPSS and displays the full text of these RFAs on the agencies' profiles.
- Ring now is recruiting non-police government agencies onto NPSS with a specific emphasis on community safety and non-police response. At present, Ring is recruiting fire departments onto NPSS. Ring has ceased actively recruiting policing agencies to NPSS.
- Ring has committed not to onboard immigration and federal law enforcement agencies, because these agencies are not democratically accountable to their local communities.
- Ring has implemented design and moderation changes to fight bias, such as restricting the types of content that can be posted to Neighbors and creating procedures to suspend or ban users with a history of posting problematic content.

Although this audit is directed to Ring, one of our central conclusions is that it is time policymakers pay attention to and regulate the ways that policing agencies rely on commercialized private surveillance. Ring is one part of a growing, largely unregulated, market for "lateral surveillance" – private individuals surveilling one another. Police increasingly are leveraging privately-owned surveillance devices, from internet-connected cameras to automated license plate readers. Lateral surveillance may at times have security benefits, but it also has real costs, as this Report endeavors to make clear. In Part III, we indicate what regulation of lateral surveillance should look like.

About This Audit

From the popular media to the halls of Congress, Ring's products and its relationships with policing agencies have attracted considerable controversy and public scrutiny. In early 2020, Ring approached our organization, the Policing Project, to conduct an evaluation of the racial justice, civil rights, and civil liberties implications of Neighbors and NPSS as they relate to policing. We agreed, on the conditions set out below.

In this Part, we explain why we conduct these audits and why we agreed to audit Ring; then, we describe the process and conditions of our audit of Ring.

Why Conduct Technology Audits?

Much of the Policing Project's work focuses on policing technologies, from body-worn cameras to facial recognition. These technologies have the potential to make communities safer. Yet they also can threaten values we hold dear – around privacy, racial justice, democratic governance, and much more. Because of the potential harms, our view is that no policing technologies should be used for surveillance absent a democratically-accountable legislative framework. Unfortunately, this sort of democratic accountability around policing technologies is all too rare. It is for that reason that we conduct audits of technology companies.

Our audits should not be taken as an endorsement of any sort. Our reports are not a seal of approval. Rather, the audits have two overarching goals:

First, our audits seek to make policing technologies more transparent. Transparency is the foundation of democratic governance, and its absence in many areas of policing stands in the way of public awareness that might motivate substantive regulation. Our audits involve extensive factual research into how policing technologies are designed and used, and culminate in public reports which give communities and policymakers the information they need to make informed decisions. Our report on Baltimore's

Aerial Investigation Research (AIR) Program, for example, provided information in litigation over the program that otherwise was not public.[1]

Second, our audits seek to influence vendors to design their products in a way that reduces civil rights and civil liberties harms. This applies not just for the immediate company being audited, but for any other vendors in that space. Nudging these companies can impact the entire country and can have a dramatic impact on police surveillance. For example, the Axon AI Ethics Board, which the Policing Project staffs, convinced Axon not to put facial recognition technology on its body-worn cameras out of concerns regarding racial disparities in the algorithm.[2]

The Policing Project Audit Process with Ring

When Ring approached us about conducting an audit, offering unconditional and unfettered access, we understood that Ring had its motives. But in pursuing them, Ring opened itself up to our evaluation, without any real control over its outcome. We saw this as a rare opportunity to learn about and influence a company with considerable reach – over 10 million monthly users on Neighbors, over 2000 policing agencies on NPSS sending about 2000 RFAs a month. We also hoped to gain insight into how society should deal with the increasing challenge of "co-veillance" or "lateral surveillance:" private individuals surveilling one another, and often reporting what they learn to the police.

Our engagement with Ring proceeded in five stages.

Stage 1 – Defining the Scope of the Audit

Consistent with the Policing Project's mission, we agreed to focus on racial justice, civil rights, civil liberties, and democratic accountability issues relating to law enforcement's use of Neighbors and Neighbors Public Safety Service and Ring's practices regarding law enforcement requests for information. The scope of this audit necessarily meant we omitted certain issues that might be of importance to the average consumer, such

as a review of Ring's products themselves and data security.[A]

Stage 2 – Information Gathering

By March 2020, we had begun the lengthy process of understanding the details of Neighbors and NPSS, as well as Ring's internal policies and operations. Given pandemic-related travel restrictions, we conducted this audit remotely. Over the course of this phase, Ring shared hundreds of pages of internal documents, including three full months of video requests. We also conducted dozens of employee interviews at various levels, including Ring's president, its general counsel, the general manager of Neighbors, and many others.

Stage 3 – Recommendations

We next presented Ring with a detailed set of recommendations on how to improve its operations and technology from a civil rights, civil liberties, racial justice, and democratic accountability perspective. We solicited feedback from Ring on the aptness and feasibility of these recommendations but retained ultimate discretion as to their content.

Stage 4 – Implementation

Ring then embarked on the complex task of implementing our recommendations. We

---

[A] Although our audit required understanding Ring's devices, the focus of our efforts was on law enforcement's use of Ring services and data, not the devices themselves. This means that we did not conduct any deep dive into how the devices operate. Nor did we study certain new products that Ring announced during this audit, such as in-home security-camera drones and vehicle dash cams. We have, however, encouraged Ring to think through its policies and ensure that it approaches each new product with the thought that has gone into its responses to this audit.

Our audit also does not address data security issues, including those policies and practices meant to protect a customer's digital information from unauthorized access. In the case of smart-home products, data security issues include unauthorized access to stored videos and live video feeds. Ring has faced significant public criticism for its data security practices. *See, e.g.*, Neil Vigdor, *Somebody's Watching: Hackers Breach Ring Home Security Cameras*, N.Y. TIMES (Dec. 15, 2019), https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html; Zack Whittaker, *Amazon's Ring Neighbors App Exposed Users' Precise Locations and Home Addresses*, TECHCRUNCH (Jan. 14, 2021), https://techcrunch.com/2021/01/14/ring-neighbors-exposed-locations-addresses. Over time, Ring has taken steps to improve its practices, such as requiring two-factor authentication and implementing end-to-end encryption. We did not assess whether such steps are adequate and express no view on the matter. Simply put, these issues were not within the scope of our audit.

provided assistance throughout this process, answering questions and providing additional guidance when issues arose. We estimate this part of the process took thousands of hours of Ring personnel time, from executives to software engineers.

Stage 5 – Public Report

Finally, we drafted this public-facing report. As with every other stage of the audit, the Policing Project retained final control over the substance and contents of this report. At our request, Ring reviewed the report for factual errors and gave substantive feedback.

We agreed at the outset that that we would accept $25,000 to partially defray the costs of the audit. During the course of the engagement, however, we decided to donate the full amount to a non-profit charitable organization.

Confidentiality & Transparency

At the outset, Ring agreed that we would be free to publish a report summarizing our findings. To facilitate a free exchange of information from the company, we agreed to a limited Confidentiality Agreement that allowed Ring to share confidential information with us to aid in our audit, but that we would not publish in our final report. With this agreement in place, Ring has been quite transparent in providing us with information throughout this audit process.

Although we made our recommendations based on our full understanding of the facts, in rare instances, we have disagreed with Ring's assessment about what information should remain confidential. To be clear, Ring is under no legal obligation to publish this data. Companies closely guard much of their internal data out of competitive concerns. Still, as we explain through this report, we believe companies that operate in the policing and public safety space have a distinct obligation to be transparent. Many of the changes that Ring has made in response to this audit exhibit just this sort of transparency.

Summary of Key Concerns & Changes by Ring

Ring is a private company selling products to private individuals, but it positions itself as a *neighborhood safety* company. By doing so, Ring obligates itself to consider the wider impact of its products and services on the neighborhoods and communities it endeavors to keep safe. In this regard, Ring, and all companies in this space making similar claims, should make decisions based on an understanding that the community itself – the inhabitants, and not the police – is the ultimate customer.

At times in its evolution as a company, Ring marketed in partnership with policing agencies in ways that may have seemed to elevate law enforcement's needs above other concerns. To the extent that was true, it was upside-down, and Ring has – both before our audit and in response to it – made many changes to the way it does business to address this. Recognizing the community as the customer means being responsive not only to the concerns of device owners and law enforcement, but to the concerns of those people who are impacted by the choices of those who have Ring devices or use Neighbors or NPSS.

A community-centered approach also means proactively addressing civil rights and civil liberties issues, whether they impact the device owner or communities at large. Part II includes a full discussion of potential civil rights, civil liberties, and racial justice issues arising out of police use of Ring device data, Neighbors, and NPSS. We discuss a number of concerns that are present with many surveillance tools, public or private, including potential invasions of privacy (including the risk of self-surveillance), surveillance of First Amendment activities, coercion, the risk of self-surveillance, and data integrity and evidentiary risk.

As a preview, in this Part, we briefly discuss four primary risks: (1) Overreliance on Policing, (2) Bias, (3) Transparency, and (4) Democratic Governance. We summarize the nature of our concern, the changes made by Ring to mitigate those risks, and issues that remain unmitigated. For our full accounting, the reader must turn to Part II.

Over-Policing

Police have become society's de facto responders to a broad swath of social problems, from drug addiction to homelessness. But given their authority to make arrests and use force, there are inherent risks every time police become involved. These risks may be justified in addressing more serious offenses, but in lesser situations, even if behavior technically is "criminal," a police response may do more harm than good.

Our audit explored whether Ring contributes to overpolicing of low-level offenses. We found that with regard to police requests for video, the most common crimes were thefts from vehicles (25%), shootings (16%), and thefts from homes (11%). A relatively small number of requests pertain to minor offenses such as vandalism (4%). There also were a significant number of video requests where the underlying crime was unclear (15%) – a problem that Ring has corrected during this audit.

The story was somewhat different with regard to the offenses Neighbors users posted about, and thus potentially bring to the attention of the police. Neighbors users sometimes post about issues such as graffiti, public urination, drug use, vandalism, and public intoxication. We have no data showing how police are using Neighbors. Only police themselves have this data, and no agency we are aware of collects or publishes this information.

Ring alone cannot correct our national problem of overreliance on police, but it has made important commitments. During this audit, Ring redefined its post categories to prohibit posts about certain low-level criminal activity that does not pose a threat to safety and property and prohibiting certain posts regarding conduct that may have innocent explanations. Ring also has committed to invest resources in identifying and onboarding local government agencies other than police, with a specific emphasis on holistic community safety. Currently, Ring is recruiting fire departments to join the platform and says that it will expand its outreach to other agencies in the future (e.g., mental health services, homeless outreach). Time will tell.

Bias

Policing disproportionately affects certain communities in this country, in particular, Black and brown communities. This occurs for systemic reasons, but also because of individual implicit, and even explicit, bias. Although Ring has implemented safeguards that many social platforms have not—like human moderation of all original posts—bias

still is a concern.

In response to this audit, Ring has implemented important design and moderation changes to further minimize such harms, such as eliminating post categories that create greater opportunities for racial profiling, and implementing procedures to suspend or ban Neighbors users with a history of posting problematic content. We also encouraged Ring to do more by engaging with outside experts in content moderation, which Ring continues to do.

These guardrails are important, but they are not a panacea. The very nature of implicit bias makes it difficult to address through content moderation. A post may not evidence racial prejudice; yet racial bias may be a reason why the poster identified the conduct as worth reporting. We should not fool ourselves into thinking that profiling and prejudice can be eradicated from social media platforms.

Transparency

At the outset, we identified the lack of transparency around police use of NPSS as a key problem. There was a time, for example, when Ring did not even publish the number of law enforcement agencies on NPSS.

Ring has done much to address our concerns. It has become much more transparent around its internal policies. And it has taken significant steps to bring more transparency to how policing agencies use its platform. Ring created public profiles for every agency on NPSS. It now requires all police requests for video to occur via public posts (RFAs). And it includes the full text of every RFA that an agency makes on the agency's profile.

Democratic Accountability

Our core principle is that the public – and not the police – should decide how policing occurs. That occurs too seldom today because legislators largely have abdicated their role. The problem is particularly acute with regard to lateral surveillance technologies, which can enable law enforcement agencies to leverage a network of surveillance devices that police would not be able to create on their own. Absent legislative regulation, police reliance on lateral surveillance can further insulate police from democratic checks.

In response to this issue, Ring agreed to exclude private security companies, immigration enforcement agencies, and federal law enforcement from NPSS because these entities and agencies are not democratically accountable to their local communities.

Advocating for democratic accountability requires understanding the precise nature of the technology at issue and its impact. Although lateral surveillance can facilitate continuous, bulk transfer of data from private devices to police, the data we obtained from Ring suggests that not to be the case with NPSS. In 2021, year to date, the nearly 2000 policing agencies on NPSS downloaded less than 100 total hours of the videos shared with them by members of the public. At 45 seconds per video, this would come out to fewer than 8000 video clips downloaded by police. To put this figure in perspective, the agencies on NPSS sent out over 20,000 requests during this same period. To be clear, members of the public shared many more videos with the police via NPSS—this is a number Ring would not allow us to publish. Police can view these videos within NPSS, but if the videos are not downloaded within 30 days—as the vast majority have not been—they are deleted and unrecoverable.

Of course, just because police do not use Ring footage for continuous surveillance does not mean the videos they download have no impact. A single video frame can indicate a person or vehicle of interest. Police then might use their own facial recognition or license plate reader software to identify a suspect. We have no data on these possibilities, but these are precisely the sorts of questions that democratically-accountable representatives should be asking of the police, and regulating if appropriate – an issue we discuss in detail in Part III.

Which brings us to a final critical point.

Citizen-on-citizen surveillance is nothing new, but emerging technologies have transformed our ability to surveil our surroundings and one another. There is now a burgeoning market for these products– from cell phone cameras to drones to license plate readers. There are hundreds of millions of privately-owned surveillance devices in use across the country. And much of this private surveillance can become available to the police.

Conducting this audit has sharpened our conviction that it is past time for policymakers to pay attention to and regulate the ways in which law enforcement relies on, and gains access to, private surveillance. As our nation grapples with the proper role and scope of policing, the role of lateral surveillance in achieving public safety must be part of the conversation.

I. Ring's Products and Services

This Part describes Ring's devices and services, with particular attention to those that have the greatest impact on policing. In the course of describing Ring products, we also touch on key changes Ring made during this audit.

A. Ring's Devices, Including its Video Doorbell

Founded in 2014, Ring is a home security company that offers various "smart" (internet connected) security products and services. Ring's devices are part of the growing smart home-security industry. By 2023, consumer spending in the smart home-security market is expected to grow to nearly $10 billion.[3] Ring alone has well over 10 million device users.

Ring's flagship product is a smart video doorbell. The doorbell comes equipped with a high-definition camera, motion sensors, a microphone, and a speaker for two-way audio communication. Ring device owners set up, manage, and operate their devices via the free Ring App. When the doorbell is rung or the camera detects motion, the device owner receives a real-time notification, and can see, hear, and speak to anyone at the door directly from their smartphone. Many Ring products can detect motion from up to thirty feet away; certain devices allow users to customize this sensitivity by creating geometric "motion zones," within which any detected activity will trigger recording. Doorbell owners also can set their doorbell to take a photograph at certain set intervals, from every 30 seconds to one hour, even without any detected motion. Most Ring devices (and all devices the company currently sells) have Privacy Zones, a feature that allows customers to block recording of areas they do not want to film. Users also can turn audio recording on or off.

In addition to video doorbells, Ring sells a full complement of other smart-security products meant to support and interact with one another. For example, Ring sells cameras for both indoor and outdoor use, and smart lights that turn on when the cameras detect motion. Ring also offers an alarm system that can alert the owner when triggered; for an additional fee, customers can purchase professional monitoring services to receive alerts and contact emergency services if necessary. The company

also offers items such as solar panels, battery packs, and transformers to power its products. More recently, Ring announced an in-home security-camera drone and devices for cars, including a dash cam and car alarm.[4]

Ring's video-enabled products come with the option for the owner to purchase a storage plan that gives the user the ability to review, share, and save videos. Without a storage plan, videos are not retained for any length of time, though a user still can view the live stream. With a storage plan, users have access to videos for up to 60 days.[5] During this audit, Ring gave device owners the option to reduce the duration of storage (and to encrypt their videos end-to-end). Once the retention period for a video elapses, the video is deleted permanently from Ring's servers and is not recoverable.

Although Ring holds a patent relating to facial recognition technology, the company does not currently offer any type of face identification or recognition capabilities, including any sort of interface with Amazon's Rekognition software. Nor has Ring disclosed any current plans to add such features. This is in contrast to some of Ring's smart home-security competitors, which already include facial recognition capabilities to differentiate between familiar and unfamiliar faces. Ring has taken the following public position on facial recognition: "Ring does not use facial recognition technology in any of its devices or services, and will neither sell nor offer facial recognition technology to law enforcement."[6]

B. The Neighbors App

In 2017, Ring launched a U.S.-only social media platform called "Neighbors." Neighbors is available to everyone, not just Ring device owners, and allows members of the public and local public safety agencies to communicate about crime and public safety issues in their geographic community. When it first was launched, Ring described Neighbors as a "Neighborhood Watch for the Digital Age" or "New Neighborhood Watch." Today, the app is branded "Safer Neighborhoods, Together."

As of September 2020, Neighbors had approximately 10 million monthly active users. Ring does not publicize precise figures for competitive reasons.

People join Neighbors in one of two ways: First, when a Ring device owner creates a Ring account, Neighbors automatically appears in the app. (During this audit, Ring provided device owners the ability to opt out of Neighbors entirely.) Second, interested individuals without a Ring device can download Neighbors as a standalone app for their smartphone.

Upon signing up for Neighbors, each user first must define the "neighborhood" for which they want to receive information. The user's "neighborhood" is an area—up to a 5-mile radius—around the user's chosen home location. Neighbors users can receive push notifications for alerts in their neighborhood based on their preference. Users can control which categories of information they want to see in their feed or for which they wish to receive push notifications.

Neighbors users receive crime and safety information about their neighborhood in three different ways: First, users see a Timeline—a feed of crime and safety incidents posted by anonymized Neighbors users, Ring's content team, local public safety agencies (such as police), and certain trusted national entities (e.g., U.S. Geological Survey, National Weather Service, and the Environmental Protection Agency). Ring also will send out regional alerts for a limited number of reasons (e.g., Red Cross alerts, National Center for Missing and Exploited Children [NCMEC] alerts, natural disaster alerts, or when a public safety agency joins NPSS). Second, users see an Incident Map of all posts in their Timeline that have a specific location. Finally, users can view a weekly "Safety Report"—a report created by Ring that summarizes local crime and safety incidents reported to law enforcement in a user's zip code over the last week.[7]

C. User Posts on Neighbors and Content Moderation

In addition to receiving crime and safety information, Neighbors users can post information to the app.[B] A *user post* can contain images or video. Users' posts are added to the neighborhood's Timeline and Incident Map. In addition to creating

[B] There was a time when Ring employees commented directly on user posts asking for police case numbers or asking whether users had contacted the police. Ring would then, with the user's consent, post ads on Facebook with the user's photo or video and encourage anyone with information to contact police. Ring ended this practice in July 2019 and during our audit committed to not reviving it.

original posts, users also can *comment* on other users' posts.

- ***User Anonymity***

User posts and comments are anonymized in two ways. First, Neighbors users are not listed by their name or handle. Instead, they appear as anonymized "Neighbors." Second, the location of a user's post is not mapped precisely. Neighbors uses a geographic obfuscation logic to hide the precise location of a user's post, while still providing the user's general area. For users in rural areas, where providing even a general area might be enough to pinpoint a user's location, Ring does not map the location at all.

Despite these steps, complete anonymization is impossible. First, when individuals have Ring doorbells or other devices on their home, these are visible to the public. Although somewhat inconspicuous, it often is possible to identify homes with these devices (indeed, Ring sells signs and stickers stating that a home is "Protected by Ring"). Second, when users post photos or videos captured by their doorbell, that image, combined with the general location of the post, often makes it possible, with great effort, to identify the precise location.

- ***Neighbors Community Guidelines & Content Moderation***

Ring limits the subject matters of posts that are permitted on Neighbors.[8] To enforce these limits, Ring moderates all Neighbors content, including human review of all Neighbors posts before they go live.

As of December 2, 2021, all original user posts must fall within one of the following categories:

- ***Safety***: General environmental awareness and potentially dangerous incidents.
- ***Crime***: Criminal activity involving theft, damage, illegal entry, or violence.
- ***Animals***: Missing and found pets.
- ***Environmental***: Severe weather and local environmental conditions that present safety concerns, such as wildfires, floods, or air quality.
- ***Community***: Community-building moments, events, and acts of kindness.

- *"I'm not sure"*: Explain what happened with as much detail as possible.

The category names and definitions have evolved over time. Ring eliminated the "Stranger" and "Suspicious" categories to address concerns about overcriminalization and bias. Some posts that would have fallen into these categories were shifted to other categories, such as "Safety"; others are no longer permitted. In 2020, 27% of posts were for lost pets, 26% were Safety, and 30% were Crime. As of October 2021, after Ring eliminated the "Stranger" and "Suspicious" categories, 43.5% of posts were Safety, 27.4% were for lost pets, and 20.1% were Crime. As discussed in further detail below, Ring made additional changes after consulting outside content moderation experts, including prohibiting posts about certain actions that may have innocent explanations, such as opening a screen door or mailbox.

Ring moderates all Neighbors content. *Posts* always are reviewed by a human moderator before they go live. Moderators review both the text and any attached media, such as videos. Moderators are trained to reject any posts that violate the Community Guidelines—for example, because the post does not meet the Neighbors definition of Crime or Safety, is abusive, or engages in racial profiling. *Comments* first are evaluated by a machine learning system that automatically approves a comment if it has a high confidence that the comment abides by the Community Guidelines—examples include simple comments such as "great"—and automatically rejects a comment if it has a high confidence that the comment violates the Community Guidelines—examples include comments with specified words or phrases that constitute hate speech, are political in nature, or are prejudicial, inappropriate, rude, or violent.[C] If this system cannot quickly approve or reject the comment, the comment is sent to a human moderator in much the same way as original user posts.

Neighbors users also can flag a post or comment as inappropriate or in violation of Ring's Community Guidelines.[D]

[C] In order to minimize the chance that users will circumvent the auto-moderation system, Ring keeps the list of banned terms confidential.

[D] If a post is flagged three times, the moderation team will review it again. If a comment is flagged once, the moderation team will review it. According to Ring, the most common user flags are "unneighborly" (i.e. inappropriate or insulting) and "unhelpful." These two flags make up a majority of total flags.

D. NPSS & Ring's Relationship with Police

In the past, Ring — through a range of initiatives — worked directly with policing agencies and municipal governments, in ways that engendered criticism. In 2018, Ring provided the Aurora Police Department with free Ring devices in support of a police operation targeting package thefts.[9] In May 2015, LAPD and Ring launched a program to provide doorbell cameras to residents of the Wilshire Park neighborhood in Los Angeles. In 2018, Ring launched a similar program in Newark, New Jersey, donating several hundred devices.[10] Ring also has matched municipal subsidies, up to $100,000, to reduce the cost of Ring cameras for their residents.[11] These programs have been criticized for their lack of transparency, for using law enforcement agencies to market Ring devices, and for promoting the crime-fighting capabilities of Ring and Neighbors without clear evidence.[12]

Prior to and during our audit, in response to these criticisms and our suggestions, Ring made a range of changes to these practices. For example, Ring will no longer participate in police sting operations. Ring stopped sharing non-public information regarding general location, density, or number of users in a jurisdiction. Ring also implemented new protocols around device donation programs that strictly limit the sharing of user data with agencies and committed not to donate devices to policing agencies in the future.

▪ *Neighbors Public Safety Service (NPSS)*

Most of Ring's contact with policing agencies comes through Neighbors Public Safety Service—a version of the Neighbors app designed specifically for public safety agencies. Via NPSS, public safety agencies can view and comment on public posts and can post their own crime and safety information. Unlike a regular user, an NPSS user's post is visible to the entire region within the agency's jurisdiction, not just a single neighborhood. Finally, as part of NPSS, a public safety agency can request that local Ring users voluntarily share their videos with the agency, as discussed in detail in the next section.[13] The total number of agencies on NPSS was not always public, but Ring now publishes an Active Agency Map that lists all of the government agencies using NPSS.[14]

Use of NPSS has burgeoned. Sixty-two agencies joined NPSS in 2018; 696 agencies joined in 2019; 913 agencies joined in 2020. As of December 1, 2021, there were about 2000 policing agencies on NPSS, including some of the country's largest agencies, such as Austin, Chicago, Dallas, Denver, Detroit, Houston, Los Angeles, Miami-Dade, Philadelphia, Phoenix, and St. Louis. During the course of our audit, Ring opened NPSS to fire departments, and since has onboarded nearly 400 to date. At our suggestion, Ring also is looking into onboarding government social service agencies.

Today, to gain access to NPSS and to use it to post to Neighbors, public safety agencies agree to the NPSS Terms of Service. These Terms, many of which were amended during this audit, include (but are not limited to):

- That NPSS is being used for a legitimate public safety purpose;
- That the agency maintains appropriate access controls on NPSS credentials;
- That the NPSS user will not post deliberately false or misleading information;
- That the NPSS user will only use an official NPSS account (not a personal Neighbors account) when using Neighbors in their capacity as a public safety official;
- That the NPSS user will include their real name, title, and agency contact information; and
- That Ring has the right to take disciplinary action, such as temporarily suspending or permanently banning any user or agency, for any conduct that Ring determines to be inappropriate or harmful.

These public terms of service replace earlier Memoranda of Understanding ("MOUs") that Ring asked public safety agencies to sign. The MOUs were criticized for including a number of provisions that gave Ring some say over the content of police department communications. For example, the MOUs included confidentiality provisions.[15] Ring told at least one policing agency that "[NPSS] back-end features should not be shared with the public, including the law enforcement portal on desktop view, the heat map, sample video request emails, or the video request process itself as they often contain sensitive investigative information."[16] These agreements also included provisions relating to press, social media, and community outreach.[17]

Ring no longer uses these MOUs and has communicated to agencies that these terms no longer are in force. As part of this audit, Ring also has agreed not to include

confidentiality provisions in any agreements with public safety agencies.

Although Ring does not receive a direct financial benefit from its law enforcement partnerships, there is no question that these partnerships set Ring apart and that Ring believes the partnerships benefit it.[18] No other smart home-security company provides a neighborhood-based crime and safety app like Neighbors. Of the other online platforms that focus on neighborhood safety and security, only Nextdoor appears to have a greater number of law enforcement partnerships.[19]

- ***Requests for Assistance (RFAs)***

NPSS includes a unique feature that allows public safety agencies, including police, to solicit videos from Ring device owners in furtherance of an ongoing investigation.

When this audit began, the process was known as "Video Request." Police would initiate and draft the request. Ring then would send an email to device owners in the request area. Only device owners with stored video recordings from the date and time requested would receive a Video Request. The request email asked, on behalf of the policing agency, if the device owner would like to share video to assist the investigation.

During this audit, Ring overhauled the Video Request process, renaming it "Request for Assistance," or RFA. RFA has many of the same characteristics as Video Request, but now instead of Ring sending requests to device owners by email, the posts are made publicly and transparently. All Neighbors users in the relevant area will see the request as a post in their Timeline. Ring also includes every RFA on the agency's public profile.

Ring reports that policing agencies have not raised objections to this change to NPSS, and the volume of RFAs and the number of individuals seeing the requests is essentially level. Ring has rejected more police requests as agencies adjusted to the new specificity requirements (discussed below). Finally, since the switch to RFA, both the total number of videos shared with police and videos downloaded by police have decreased—although the percentage of shared videos that police choose to download has increased.

- ***The RFA Process***

The first step in the RFA process is for the NPSS user—usually a police detective or crime analyst—to create the request that eventually will become a public post. Ring personnel review all RFAs before they are posted to ensure that they comply with Ring's Request for Assistance policies ("RFA Policy").[20]

This RFA Policy, like the NPSS Terms of Service, was updated substantially during the course of this audit. It currently includes a number of requirements, including that the RFA has a specific case number, an address associated with the incident under investigation, a time range for the video request (up to twelve hours), and the geographic boundaries for the request area (a minimum of .025 square miles, and up to .5 square miles). The request also must include a brief description of the basis for the request—such as the type of incident the officer is investigating—as well as contact information to reach the agency directly.

Unless they opt out, Neighbors users receive a notification that an RFA has been posted to their Timeline.

Previously, users could opt out of receiving VRs entirely only through an unsubscribe link in a VR email or by calling customer service. Now users also can opt out of seeing RFAs entirely through the Ring App.

When users see an RFA post, they can ignore it or decide to respond. Policing agencies are not told if any (or how many) Neighbors users or Ring device owners receive the post, nor how many choose to view it, and Ring never has received a legal request from law enforcement for that type of information. This was the case for the Video Request process as well.

If a user chooses to respond to the RFA and the user has stored video from the specific time frame, the user will be prompted to review recordings and select which, if any, to share. If the user chooses to share a video, the requesting police officer receives the selected user video, as well as the physical address and email address associated with the Ring device and account—this information is shared with the agency to facilitate further communication between the agency and the Ring customer.

Videos shared with police automatically are saved in the agency's NPSS account and filed by case number. The videos are available for agency personnel to review and/or download for the next 30 days and then are permanently deleted from the agency's account.

Once a video is downloaded, it no longer is within Ring's control. The agency can store or share the file according to its own policies. Some advocates have charged that Ring was not transparent with its customers about how videos they share via NPSS may be retained and used by law enforcement. If these facts were not clear already, then changes to Ring's RFA process, as well as public FAQs, now make clear what happens up to the point that an agency downloads the video. After that point, the retention and use of NPSS-sourced videos depends on the policies of the particular agency. Neither Ring nor Ring device owners have that information.

During the course of the audit, Ring disclosed that in 2021, year-to-date, the nearly 2000 policing agencies on NPSS downloaded less than 100 total hours of the videos shared with them by members of the public. At 45 seconds a video, this would come out to fewer than 8000 video clips downloaded by police in 2021. Although these are the number of videos *downloaded*, members of the public *shared* many more videos with police via NPSS. (Ring requested we not publish the precise number.) Police may view these videos in NPSS, but if police do not download a video within 30 days, the video is automatically deleted and unrecoverable.

E. Law Enforcement's Use of Legal Process to Access Ring Customer Data

NPSS's Request for Assistance feature is one way that law enforcement agencies can obtain videos from Ring device owners, but it is not the only way. As with any company that provides remote computing (i.e. cloud) services, Ring can be compelled legally to disclose its customers' data to government entities conducting criminal investigations.[21] Legal compulsion can take the form of warrants, subpoenas, court orders, and national security requests.

In 2020, Ring received about 1,600 search warrants from law enforcement (up from

536 in 2019) and provided a full response in about half of them.[22] Ring has no information on how often the information Ring provided was useful to a police investigation.

The circumstances under which Ring legally would be required to disclose customer information depends on federal and state law. Ring only will share "content information" – including videos generated by Ring devices – in response to a court-issued warrant based on probable cause (or exigent circumstances). With regard to non-content information–such as a user's name, address, email address, billing information, and certain purchase history and service usage information–Ring requires a valid legal request that compels disclosure in connection with a criminal investigation, but not a warrant.[23]

The only other instance in which Ring will disclose customer data to law enforcement is under certain exigent circumstances recognized under the Stored Communications Act. In particular, "Ring reserves the right to respond immediately to urgent law enforcement requests for information in cases involving imminent danger of death or serious physical injury to any person."[24] Such emergency requests must be sent in writing using an emergency request form.[25]

II. Benefits & Harms

The primary focus of this audit, as with all our audits, is on the civil rights and civil liberties issues raised by the use of a particular technology. We look at these from both a legal and ethical perspective. Where we are able, we also speak to the asserted benefits of the technology.

This audit differs somewhat from others that we conduct, in that most products we evaluate are sold to and used somewhat more directly and exclusively by policing agencies. Ring products are sold to private parties, and private parties have the ability to use the Neighbors App. But Ring has designed its product, and Neighbors, (a) with a link to policing agencies (through NPSS); and (b) in a way that implicates the interests of both users and the public more generally. That is our focus.

We use a straightforward framework to begin to analyze issues around policing technologies. The goal of this framework is to help us take account of the benefits of a technology, as well as the harms. Our framework considers these issues in three steps:

> ***Step 1:*** Ask what problems are the technology trying to address? What are the real or potential benefits? What is the likelihood and distribution of those benefits?
>
> ***Step 2:*** Identify the harms associated with use of the technology, including not only hard monetary costs but also social harms – from inaccuracy and racial bias, to invasions of privacy and the chilling of First Amendment freedoms, to exacerbating disparities in how different communities are surveilled and policed.
>
> ***Step 3:*** Determine *if* there is a regulatory framework—i.e., a set of legal requirements or internal guardrails governing law enforcement use—that can eliminate or substantially mitigate the costs, so that any benefits can be obtained. (We emphasize the word *if* so as to signal and leave open the possibility that the costs of a particular technology are so high, and cannot be mitigated sufficiently, that the particular use of the technology should be

banned entirely. Even in this case, some uses may be permissible, and others not.)

Our audits for the most part look at potential benefits and harms, as a full empirical assessment of the technology's actual efficacy (as to its stated goal) would be quite labor intensive and beyond our capabilities. And, in particular, our goal is to evaluate closely possible harms, in order to offer ways to mitigate or eliminate those harms.

Potential Benefits

Ring's mission is to "help make neighborhoods safer." We evaluate this mission here, while recognizing that most people buy Ring products because they believe it will make them and their families, in particular, safer.

One aspect of this stated mission is to contribute to solving and reducing crime. Indeed, Ring's previous stated mission was to "reduce crime in neighborhoods." In past marketing materials, the company has claimed: "With Ring, you can stop crime before it happens—no matter where you are. Because with Ring, you're always home." Although it may be true that Ring cameras can act as a deterrent to crimes being committed against Ring device owners, it is not clear whether Ring devices reduce crime in neighborhoods overall.

When it comes to surveillance cameras generally, a number of studies have found that closed circuit television cameras (CCTV) can be highly effective at reducing crime in parking lots and also may deter crime in residential areas.[26] Yet CCTV has only minimal impact in city centers or in public housing.[27] Studies that have found a significant impact on crime have found reductions in vehicle thefts, but not violent crime.[28] It is not clear how these studies apply to Ring devices and Neighbors.

We have seen (and Ring has provided) anecdotal examples of Neighbors and Ring devices being used to deter criminal activity or solve crimes.[29] The company's "RingTV" webpage features dozens of videos in which would-be thieves have been deterred by a Ring Video Doorbell.[30] The Neighbors home page also includes a story about a community using Neighbors to identify a prolific package thief. Ring devices have

captured footage of serious, violent crimes; for example, a Ring device recorded video of suspects leaving the scene of a murder.[31]

But there are no robust studies measuring the impact of Ring devices or Neighbors. No agency (at least none that we know of) keeps statistics regarding the number of crimes solved via Ring devices or Neighbors. A statistic that Ring frequently cited boasts that after a Los Angeles neighborhood was equipped with Ring Video Doorbells, the number of burglaries dropped by 55%.[32] But a report by the MIT Technology Review was unable to verify the results of Ring's Los Angeles study and noted that the following year, burglaries in the neighborhood hit a seven-year high.[33] Public analysis of Ring public safety benefits have found "minimal impact" or "little concrete evidence."[34]

During this audit, Ring agreed to stop citing data regarding Ring's impact on crime until such data has been verified through independent study. Ring also reviewed all of its marketing and social media materials to remove any claims about crime reduction.

There are other possible benefits from the use of Ring's products and services. In recent years, Ring advertising has featured a broader conception of safety. Neighbors users can post about issues such as missing persons, lost pets, and stolen property.

Public safety agencies also have used Neighbors to inform citizens about fires, extreme weather, and other hazards. It is not difficult to imagine situations in which timely, geography-specific notifications—for example about tornadoes or wildfires—could make the difference between life or death.

Quite obviously, there is a substantial market for Ring products and for Neighbors. These users—law enforcement, fire departments, and members of the public—believe they obtain benefits from using the products or the apps. These benefits might be real, or they might be perceived—purchasing a Ring device, posting to Neighbors, and connecting with law enforcement and others about public safety issues might give people a sense of security and control. It is evident millions of users see some benefit in using Ring services and products.

Potential Harms

Over the course of our audit, we considered a range of potential civil rights, civil liberties, and racial justice issues arising out of police use of Ring device data, Neighbors, and NPSS. In each section below, we discuss the nature of the concern generally, and how it might apply to Ring. We then highlight changes Ring has made to address these concerns and what aspects of the risk remain. Because many of these risks are inherent to policing, mitigating them will depend on the actions of police and policymakers, not just tech companies.

1 *Overreliance on Policing*

Police today often are used as society's de facto responders to a host of complex social problems, such as mental illness, homelessness, substance abuse, eviction, and poverty. A great deal of attention of late has been paid to the fact that for these sorts of issues, police are not trained to be the ideal responders, and lack the capacity to solve the underlying problems.[35] In addition, whenever police respond, they bring with them the possibility of using force and making arrests.

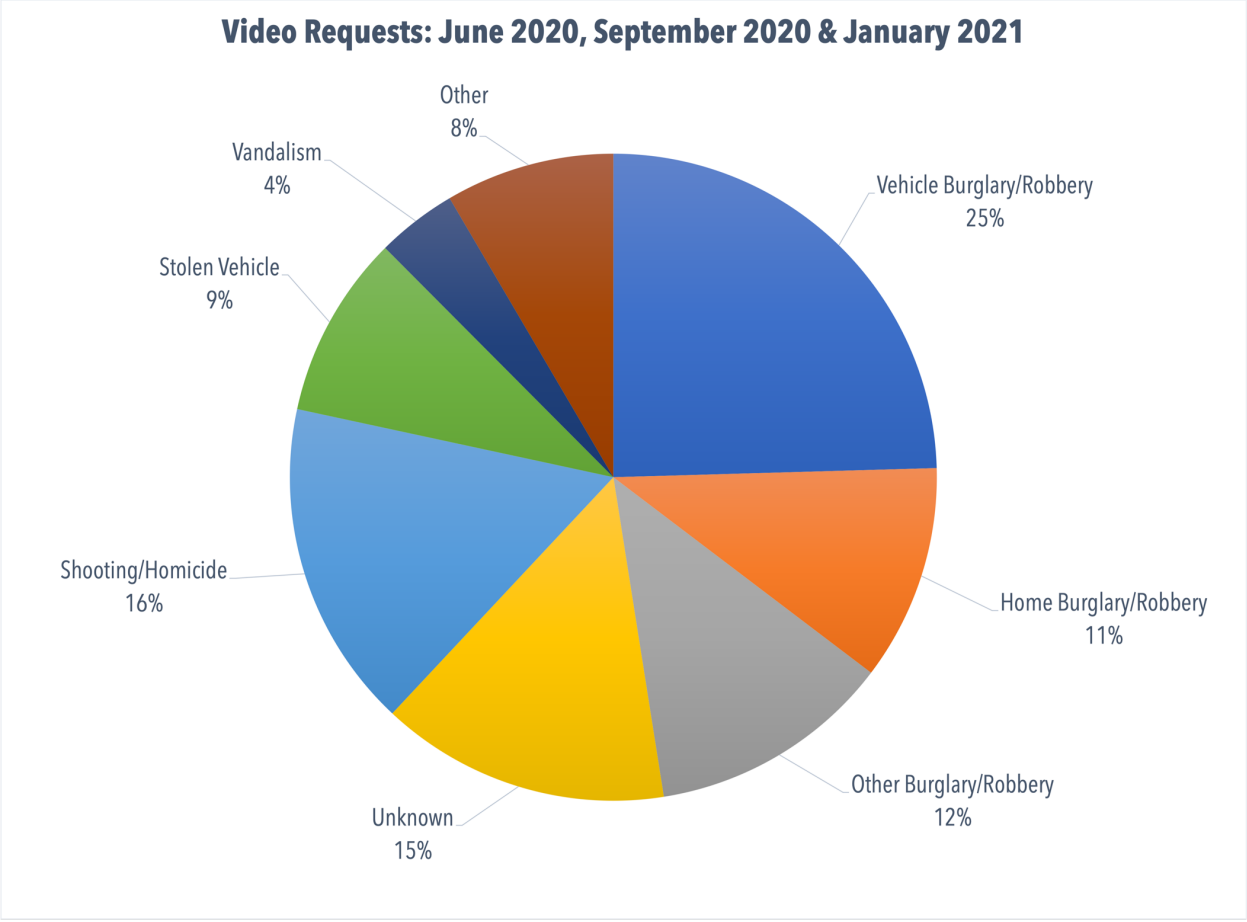
In some instances, a police response to criminal conduct is appropriate. But for certain "low level" offenses – minor drug possession being a paradigmatic example – the risks of police intervention may well exceed any benefits. Communities must draw their own lines as to what crimes warrant a police response, but social science research provides useful guidance. A recent study of misdemeanor prosecutions in Suffolk County, Massachusetts, for example, found that prosecuting people for low-level offenses makes it significantly *more* likely for people to reoffend.[36] Relatedly, a study in Baltimore found that the city's recent policy of declining to prosecute minor drug possession and sex work "led to fewer new low-level drug and prostitution arrests, almost no re-arrests for serious crimes for those who had charges dropped, and fewer 911 calls."[37] That is not to say that police never have a role to play. Rather, we must recognize that for some offenses, police enforcement does little to deter the behavior and nothing to address underlying causes.

A key issue we evaluated was whether Ring's devices and services contribute to the over-enforcement or counter-productive enforcement of low-level offenses. There are

two ways this might occur:

First, policing agencies might use NPSS to request video evidence of low-level offenses. There are anecdotal reports that policing agencies have used social media platforms to investigate such offenses. In one example, which garnered widespread attention earlier this year, an agency used Facebook to crowdsource information about a man who shoplifted baby diapers and wipes from a Walmart after his credit card was declined repeatedly.[38]

During the course of our audit, we reviewed several thousand NPSS video requests (the precursor to RFA). We found that most video requests from these months related to relatively serious property crimes and some violent crimes. The most common requests were for footage related to vehicle burglaries and robberies, shootings, home burglaries and robberies, and stolen vehicles.



We cannot say with certainty how often agencies have used video requests in connection with low-level offenses, because approximately 15% of police requests did not specify what type of crime was under investigation. A smaller subset of requests did not reference any incident under investigation at all and simply asked users to submit footage of suspicious activity.

To address concerns about over-enforcement of low-level offenses, Ring has begun rejecting RFAs that are not specific enough (for example, that do not contain information about the type of incident being investigated). Ring also is considering requiring the requesting agency to select an offense type (or types) from a dropdown menu. This information then could be collected and made public in aggregated form to an agency's profile. Doing so would provide communities with real insight into how their local agencies use NPSS.

Second, public posts on Neighbors might bring low-level offenses to the attention of police, which in turn might lead to police enforcement. Police might learn about low-level offenses directly through the app. When we first reviewed content on Neighbors, we saw crime-related posts reporting relatively petty conduct, such as verbal disputes, graffiti, public urination, drug use, vandalism, and public intoxication.[39] But the ways in which users respond to content on the platform might also drive a police response. The fact that footage of an offense exists — even a low-level one — can make it more likely that individuals will consider the incident a police matter.[40] Moreover, social media platforms that focus on crime and safety can cause individuals to overestimate the level of crime in their neighborhoods, leading to more reliance on police.[41] One post, which illustrates our concerns about these escalating effects, claimed that two individuals used a knife to enter buildings so that they could use drugs (the video only depicted a Black man and woman walking up a stairwell). A commenter urged the poster to tell the police that the couple was armed and dangerous so that they would respond quickly.

We cannot answer whether or how often this *potential* risk translates into real-world consequences. Ring lacks the necessary data to evaluate police response to posts— Ring does not know how often officers encounter posts about low-level offenses on Neighbors, or how often they take follow-up enforcement action. Nor does Ring know how often Neighbors posts result in escalation and police contact. Even when it comes

to video requests and RFAs, Ring does not know how often potential evidence translates into enforcement, arrests, or prosecutions, or for what type of crimes. These answers are in the hands of the policing agency and should be captured by data that police report to their communities.

Ring has taken some important steps to address the potential risks of overpolicing. By making all RFAs public posts and requiring police to disclose the nature of the investigation, communities will be able to see if police are investigating crimes that are not high priorities. Ring also redefined its post categories to prohibit posts about certain low-level criminal activity that does not pose a threat to safety and property, including drug use and public urination. Ring also has added community resources to Neighbors—for example, contact information for local suicide prevention services, homeless outreach, mental health services—so that users will have a clear source of information about non-police options. In addition, Ring has ceased actively recruiting new policing agencies to NPSS and has committed to onboarding local government agencies with a specific emphasis on community safety. Doing so will allow these non-police agencies to provide a wider range of safety information to communities and might encourage Neighbors users to consider a broader range of non-police responses when they encounter safety issues. At present, Ring is focused on adding fire departments, but we hope in the future Ring might expand to emergency management, public health departments, and animal services.[E]

Ring's actions in response to our audit are a first step toward transparency and limiting police responses in situations in which they would be counterproductive. But as we explain below, ultimately what is needed is greater regulation of police reliance on lateral surveillance.[42]

2 *Bias*

Bias in policing is a structural problem. A wealth of research and lived experience demonstrates that every aspect of law enforcement — from stops to arrests — disproportionately impacts people of color.

[E] We recommended to Ring that they also onboard more community-based organizations in the hope that these organizations might broaden the safety conversation on Neighbors.

Knowing this, we considered the risk that Ring's devices and services might be used to disproportionately target people of color and other vulnerable populations. Bias is a well-documented problem on social media platforms.[43] Some have criticized Neighbors for disproportionately depicting people of color engaging in harmless activity.[44] This may result from implicit bias – for example, a wealth of literature shows that people often view Black men as more threatening or more likely to be engaged in suspicious behavior.[45] There also is an unfortunate history of *explicit* bias – people reporting Black individuals to the police with malicious intent.[46] A prominent recent example was a woman's racially-motivated call to 911 to report a Black bird-watcher in Central Park.[47]

Ring mitigates potential racial bias on Neighbors through content moderation. As discussed above, it moderates all content on the platform, including removing and banning hate speech. Overall, Ring's content moderation process rejects a substantial portion of posts.[F] In this respect, Ring is far ahead of many other social media platforms. Neighbors moderators also apply specific rules around the mentioning of race. Race only may be mentioned if (1) it is relevant to the incident and is part of a larger description to identify the subject of the post, (2) it is in the context of discussing how the subject of the post was treated, or (3) it refers to the poster's own race. During our audit, Ring also updated the training it provides its content moderators in order to minimize profiling and prejudice on the platform. Ring also implemented procedures to suspend or ban Neighbors users with a history of posting problematic content. Still, bias can be difficult to weed out – a post may not evidence racial prejudice, yet bias may be the reason why the poster identified the conduct as worth reporting.

Ring's most important changes in this vein have been to eliminate certain categories of posts that created greater opportunities for racial profiling. For example, Ring eliminated the post categories of "Stranger" and "Suspicious" in order to encourage users to describe activities instead of people. Ring also prohibited certain posts about behavior that may have an entirely reasonable explanation (e.g., off property suspicious behavior, shortcuts, and hiding from police) and other subcategories that

[F] Ring considers the precise percentage confidential. According to Ring, by far the most common reason for a post to be rejected is that it is not "crime and safety" related. For example, in one denied post, a user asked: "Who is this guy walking down the street at 2am?"

are uncertain or speculative in nature (e.g., potential crime, potential suspect, attempted crime). Similar problems can arise when policies agencies seek footage of "suspicious" individuals without a description of the suspect or crime under investigation. To address this, Ring's RFA guidelines now require that RFAs contain specific pieces of information, including "information referencing an active investigation, specifically, the type of incident being investigated."[48]

We encouraged Ring to work with outside experts in content moderation to continue to strengthen its moderation practices. In response, Ring has engaged the Center for Democracy and Technology (CDT). CDT contributed substantially to Ring's recently updated Community Guidelines, though there are additional improvements that Ring may well want to consider in the future.[G]

3 *Transparency*

Transparency is the foundation of democratic governance. Without adequate information, the public cannot have informed opinions, and legislatures cannot make informed decisions. Technology companies can both hinder and facilitate transparency. In the policing context, there are too many examples of the former — companies sign secret agreements with policing agencies, require non-disclosure clauses, or refuse to provide information to the public. But companies also can foster transparency between public safety agencies and their communities.

Many critics of Ring and NPSS pointed to problems of transparency.[49] There was a time, for example, when Ring did not even publish the number of law enforcement agencies on NPSS. Ring required agencies to sign agreements with confidentiality provisions

[G] For example, Ring might consider requiring posters to corroborate claims about crime, so that individuals are not falsely accused on the platform. In our review of Neighbors posts, the vast majority of crime-related posts showed the subject of the video committing the offense described in the post. But there were rare posts in which the user accuses the individual depicted of a serious crime without any corroboration.

Ring might also explore whether to follow platforms such as Nextdoor and Facebook in requiring posters to use their real names, in light of studies showing that this holds users accountable, reducing bias and increasing civility. *See* Keum & Miller, *supra* note 56; Kelly P. Dillon, Rachel L. Neo & Natalee Seely, *Civil Keystrokes: Examining Anonymity, Politeness and Civility in Online Newspaper Forums* (2015).

and wrote or approved statements issued by policing agencies without disclosure of this important fact.

Prior to and during this audit, Ring implemented a litany of policy changes to improve its transparency. Ring no longer ask will agencies to sign agreements with non-disclosure or confidentiality provisions (and has officially released agencies from all such previous restrictions). Ring also has committed to publishing all materials it provides to NPSS users (e.g., Terms of Service, training materials, and press resources) and will disclose all device donation initiatives involving government agencies.[50] Ring also has brought greater transparency to how policing agencies themselves are using NPSS. Ring has created a public profile for each agency using NPSS, which includes a range of information about how the agency uses NPSS, including the full text of the agency's posts and RFAs. Ring also generates periodic usage reports for each NPSS agency and shares that report with the agency's NPSS coordinator.[H] Finally, Ring will publish a bi-annual report with information about the number of law enforcement requests Ring received (e.g., warrants, subpoenas), the number of customers Ring notified about the law enforcement requests, and a breakdown of how often Ring disclosed content and non-content information.

These are important changes, but much is still unknown about how police use images and videos they obtain via NPSS. Some agencies might use the data in conjunction with advanced analytics like facial recognition and license plate recognition. The scope and extent of these efforts, however, is presently unknown, outside of press reports.[51] Once again, the only way to ensure transparency around these issues is through direct regulation of law enforcement.

4 *Lateral Surveillance and Democratic Governance*

If a policing agency sought to create a network of cameras or license plate readers throughout its community, it would be the subject of much political debate. Regulatory and budgetary constraints might force the agency to justify the program to policymakers. But when police crowdsource from private devices, they can achieve surveillance with no cost, no public debate, and no public approval. In this way, lateral

[H] Because Ring shares the report with the agency's NPSS coordinator, it is available for public records requests.

surveillance can undermine the ability of community to have a say in how they are policed.

This point is not restricted to Ring; as we discuss in Part III, lateral surveillance is a wide reaching and complicated issue, with many gradations. There is little concern about democratic governance when individuals reach out to police to share information, whether via 911 or via social media. At the other extreme, there are real governance concerns when businesses set up CCTV cameras by the hundreds or thousands and provide police with direct access – as has happened in cities across the country.[52]

Neighbors and NPSS fall between these two extremes. Ring does not facilitate direct police access to customer cameras. Sending out an RFA is far easier for police than going door to door seeking information, but private individuals must take affirmative action to share in response. This is not the kind of continuous, bulk, and directly accessible surveillance that concerns us the most.

There have been a few reports of police side-stepping some of NPSS's protections. For example, there are reports of agencies subsidizing Ring cameras on the condition that users submit all requested footage.[53] One agency "loaned" Ring devices to users, retaining ownership of the resulting data. Another piloted a program enabling local Ring users to share their cameras' video streams with the agency around the clock.[54]

We recommended that Ring update its NPSS Terms of Service to prohibit policing agencies from enacting programs that provide direct access to Ring customer videos or devices, and to ban departments who violate these terms. In response to our recommendation, Ring noted that jurisdictions may decide to authorize direct access to user devices.[55] This is a fair point. Still, Ring should prohibit agencies from directly accessing customer devices *unless* such access has been authorized democratically. We understand that it will be difficult for Ring to enforce this requirement, but reserving the right to terminate users and/or agencies on this ground will at least create a disincentive for policing agencies to overstep.

Ring has made other changes that facilitate democratic governance: Many of the transparency changes discussed above make it easier for the public (including advocacy organizations) to hold their agencies accountable. Ring also has committed

to not onboarding private security companies, immigration authorities, or federal law enforcement onto NPSS precisely because these entities are not democratically accountable to local communities.

Ultimately, whether communities choose to do more to govern police use of technology is a choice for policymakers. We discuss this in greater detail in Part III.

5 *The Coerciveness of Police Requests for Video*

A central claim of NPSS's Video Request (VR) and Request for Assistance features is that everyone is free to choose whether to share videos with the police. But some have argued that "[m]any people are not going to feel like they have a choice when law enforcement asks for access to their footage."[56]

We examined the voluntariness of VR and found no evidence that these requests are coercive. During this audit, prior to the release of RFA, Ring further edited the request template to make clear that individuals are not obligated to share video. More generally, we suspect that an electronic request is far less intimidating than being confronted by an officer going door-to-door in person. In addition, Ring's change from VRs (sent via email) to RFAs (via public posts and push and email notifications for those posts) likely will make the process even less coercive.

Still, coercion and inappropriate police requests can enter the process at other points. First, we think it essential that police not use NPSS to trick anyone into providing information. To help ensure this, Ring now requires police users to commit not to post false or misleading information on the platform, and reserves the ability to remove agencies that break this rule. Second, it is possible that police could bypass NPSS and request footage directly from Ring users. One police captain noted that when device owners aren't responding to VRs, officers will knock on doors asking for Ring footage in person.[57] (Importantly, officers do not know who receives an RFA; likewise, under the old VR process, officers did not know who received a video request.) Some agencies have created camera registries to easily contact camera owners who might have data relevant to investigations.[58] There are reports of agencies requiring Ring users who received subsidies to submit videos upon police request.[59]

Ring does not facilitate these programs and Ring cannot prevent them through design choices—only regulation can do that. But Ring has taken some steps to mitigate the chances that police will use coercive methods to obtain Ring data. Ring no longer donates devices directly to police. Ring has implemented stricter controls around its remaining donation programs, prohibiting donors from requiring Ring users to share footage or access to their devices. Ring also has committed not to provide agencies with location information regarding Ring users absent a warrant or subpoena (or exigent circumstances).

6 *Surveillance of First Amendment Activity*

Police surveillance of political or expressive activity gives rise to the concern that individuals will be targeted for enforcement based on their political beliefs, and that people might be deterred from exercising their First Amendment rights as a result. These concerns came to the fore when it was reported that the Los Angeles Police Department requested Ring footage related to offenses that occurred during protests over police abuses.[60]

The issue is complicated. On the one hand, although the overwhelming majority of demonstrations are peaceful, some do devolve into violence or property damage, leading to injuries and even death. This was certainly true in the Charlottesville confederate statute protest, the march on the Capitol, and some of the demonstrations in the immediate aftermath of George Floyd's murder. Police should be permitted to enlist the public's help in investigating serious crimes that occur at a protest. On the other hand, the long history, in the United States and abroad, of law enforcement agencies intentionally subverting political movements – and enlisting the public's help to do so – demonstrates the validity of protestors' concerns.

To determine whether police use NPSS to request video of protests or other First Amendment activities, we reviewed all Video Requests from June 2020 (coinciding with nationwide protests over police abuses). We found no evidence that this occurred. Ring rejected one video request seeking that "the public share any video that may help us identify crimes committed or suspects involved in the incidents that occurred on" a date coinciding with police protests because the request lacked a case number. Agencies did send requests related to crimes that occurred during protests – including

one incident in which a vehicle intentionally struck pedestrian demonstrators – although these were quite rare.

Minimization policies can help strike the right balance when police seek protest-related footage. The LAPD's June 2020 request was broadly worded, seeking videos related to unspecified injuries, looting, and property damage and destruction during recent protests. If agencies want video, they should focus their requests on *specific* committed offenses and carefully limit their requests to times and locations in which evidence of those offenses might be found. Ring has already implemented geographic and temporal limitations on RFAs, as discussed above – an important step.

7 *Invasion of Privacy*

All surveillance technologies impact personal privacy. Some do this by over-collecting information that is revealing and intimate, including the contents of our phone conversations or emails. Others impact privacy by aggregating vast amounts of information, such as license plate readers and data-broker dossiers. The widespread use of surveillance technologies can change the way that the populace engages with the world at large, chilling people's willingness to say, write, or do certain things. Information collected can be used against individuals and shared in various ways.

Because they are trained on people's front porches or the area in front of their homes, most Ring videos do not capture particularly sensitive information. Most of the activity captured on Ring devices occurs in public view – either on one's own property, on the street, or perhaps in a neighbor's yard.[l]

Depending on the area and device positioning, however, even surveillance of public spaces can potentially implicate privacy. Ring cameras can capture nearby pedestrians and vehicles, as well as the driveways, yards, and homes of nearby neighbors. And, because Ring cameras are stationary, they can capture these images over an extended

[l] The use of Ring devices in conjunction with camouflage cases (cases that cause Ring devices to appear to be something else – such as bird feeders or potted plants) or in locations where they are not clearly visible may well violate some state wiretapping laws. Under Massachusetts law, for example, it is a crime to record wire or oral communications unless the subject is on notice that they are being recorded. *See* MASS. GEN. LAWS ch. 272, § 99(C)(1); *Glik v. Cunniffe*, 655 F.3d 78, 87 (1st Cir. 2011).

period of time, revealing potentially personal information. A camera recording the outside of a home might, for example, capture "images of our children playing outside in our yards, our friends coming to meet us where we live, and our guests arriving for gatherings of a religious or political nature, to mention only those of life's privacies around the home that are least likely to cause us embarrassment or even shame."[61] A U.K. court recently held that a Ring user's surveillance of a neighbor using a Ring device violated U.K. law.[62]

Law enforcement knows the value of this type of information. One law enforcement agency offered larger subsidies to homes that had "optimal viewpoints" – that is, views of the block and nearby residences.[63] (Ring had nothing to do with this subsidy program.) In places where cameras are ubiquitous, it would be easy for law enforcement to gather videos en masse. As one New Jersey commander said: "Our township is now entirely covered by cameras . . . . Every area of town we have, there are some Ring cameras."[64]

Ring has built safeguards into NPSS that mitigate the chance of bulk collection or extended surveillance occurring. First, the process relies on obtaining consent from individual users, which limits indiscriminate collection of videos. (As discussed above, we do not find NPSS to be coercive.) Second, NPSS's 12-hour limit on requests for footage prevents agencies from using the platform to conduct long-term surveillance of private residences. Third, the geographic restrictions on requests for footage significantly restrict the scope of police surveillance through the platform. We recommended Ring investigate ways to deny automatically any attempt to skirt these requirements. During the course of the audit, Ring implemented a policy permitting police to use the same case number a maximum of two times on an RFA. Ring also allowed users to customize the period of time that they retain videos, making it easier to routinely delete videos. Ring also has deleted personal information gathered in connection with past donation/subsidy programs, ensuring that information will not be shared. In addition, Ring has drawn a firm line against granting law enforcement live streaming or direct access to a Ring device through NPSS, although at present Ring does not prohibit customers from granting police direct access to Ring devices outside of NPSS.[J]

[J] During the course of the audit, we learned the total amount of video footage downloaded by police

8 *Risks of Self-Surveillance*

As smart home devices with cameras, microphones, and other sensors become more and more ubiquitous, they collect information that can be used against customers and their families. We call this the risk of "self-surveillance." In recent years, it has become clear that the risk of self-surveillance is far from speculative – there now are examples of data from smart home devices being used as evidence in criminal prosecutions.[65] One agency noted that smart devices may contain "valuable data regarding device owners' movements in real-time and on a historic basis, which can be used to, among other things, confirm or contradict subject alibis or statements."[66]

The idea of self-surveillance as a civil liberties risk may seem a little counterintuitive. After all, it is the person being surveilled who installed the cameras in the first place. It also can be difficult to understand why society should be concerned about people providing evidence of their own crimes.

Still, police access to smart home devices can have profound privacy implications. The home is the "area where privacy interests are most cherished in our society," *California v. Ciraolo*, 476 U.S. 207, 226 (1986) (Powell, J., dissenting), a place where we have our most personal conversations and intimate moments. Balancing law enforcement's need for evidence with individuals' privacy interests is an especially delicate task in the context of the home, and depends on what type of data is being accessed, for what reason, and what safeguards are in place to minimize the collection of non-evidence.

Ring's policies regarding law enforcement requests for user data are consistent with the requirements of the Stored Communications Act and other applicable law. Absent exigent circumstances, the company only will share a user's video with law enforcement upon issuance of a warrant based on probable cause.[67] In response to subpoenas, Ring will provide only non-content information, such as the device owner's name, email address, and number of devices. Ring also updated its guidelines to clarify that Ring will notify users before disclosing their information, including video, absent established

via NPSS. Although Ring has insisted we not publish the total number, we can say that the data suggest agencies generally are not downloading videos en masse (although it is possible that some agencies are downloading significantly more than others).

exceptions.[68] Moreover, Ring device owners can choose to enable end-to-end encryption, which prevents Ring from accessing or sharing the content of the owner's videos.

These important policies do not, however, obviate the need for regulation of how police access smart home devices and under what circumstances. Nearly 70% of homes have a smart home device. It is long past time for policymakers to determine what circumstances justify seeking a warrant to search smart home devices, and how resulting privacy intrusions can be minimized. For example, legislatures might consider limiting searches of smart home devices to investigations of serious offenses, and could implement minimization requirements – for example, restricting searches to times and locations where there is cause to believe that relevant evidence may be found. And special rules may be necessary where an agency seeks direct access to a user's account.

9 *Data Integrity & Evidentiary Risks*

Only Ring device owners can share video directly with police via NPSS. By limiting RFAs to Ring devices only, Ring ensures the video has not been edited or manipulated by the user in any way. This mitigates a serious potential problem around the use of private surveillance footage, a problem that only grows more serious with the emergence of highly realistic "deep fakes."[69]

Although Ring has mitigated the deep-fake problem, there are other evidentiary problems it cannot yet address. For example, once an NPSS agency downloads a video, it is entirely outside of Ring's hands. Ring has no way of verifying that the video in the agency's possession is in its original form – in other words, Ring has no way of confirming the video's chain of custody.

We see two options for addressing this: (1) Technical changes – for example, embedding hashes, either at the point that a video is uploaded to the cloud or shared through NPSS; or (2) Outside partnerships – for example, an integration with an external evidence management system that would keep chain of custody information and ideally a full audit trail of the agency's interactions with the video (e.g., when it was downloaded by the agency, by whom, whether it has been edited, and with whom it

has been shared). From a societal perspective, the latter option might raise its own civil liberties concerns — particularly as digital evidence management systems evolve to include advanced analytics capabilities such as transcription and computer vision. Moreover, agencies may use such systems to store data for months and even years, resulting in massive accumulations of data. Ring has committed to exploring solutions to this problem, but at present it remains unresolved.

III. Regulation of Police Use of Lateral Surveillance

Public safety is a collaborative enterprise; all members of society can play a role in protecting our communities. But *how* we do it matters.

Lateral surveillance — private individuals observing, recording, and disseminating information about other private individuals — has long existed. Nosy neighbors spy on neighbors. Witnesses and informants provide information to the police. Law enforcement agencies, especially after September 11, have cultivated a culture of "if you see something, say something."[70]

These practices have both benefits and harms. On the one hand, serious criminal investigations rely on people being willing to come forward and cooperate with police. On the other hand, something profound is lost when citizen spying becomes a routine part of community life, creating fear and distrust with profound real-world consequences. Witness, for example, the residents of a college town who called the police on a student who was carrying a rice cooker on campus, or the mobilization of thousands of online vigilantes against an individual who was (incorrectly) believed to have committed the Boston Marathon bombing. (Or think, for that matter, of any totalitarian society that encouraged its residents to spy on one another.[71])

Regardless of what one thinks about this tradeoff, the reality is that we as a society accept a bit of spying as a routine fact of life. But even if we accept analog lateral surveillance — witnesses reporting a crime — the digitization of lateral surveillance has created something altogether different.

Emerging technologies have transformed our ability to keep tabs on our surroundings and on one another. Ring is only one part of this growing industry. Ordinary individuals have access to sophisticated surveillance tools to an extent that would have been unimaginable only years ago. Cell phone cameras are in every pocket. Cameras also can be found on tens of millions of homes; drones and license plate readers are readily available; a trove of information about each of us is only a few clicks away. When law enforcement taps into these networks, it expands their capabilities massively.

The simple fact is that law has not kept up with the technological expansion of lateral surveillance. In fact, police reliance on digital lateral surveillance remains largely unregulated.

We cannot wait for industry to self-regulate. Ring opened itself up to an outside audit, but most such companies have not. More fundamentally, audits cannot stand as a substitute for direct regulation of police. And many of the harms identified above cannot be fully addressed absent such regulation.

At the least, policymakers should enact sensible regulation of law enforcement's use of lateral surveillance tools. The sooner the better. And given the unique risks that arise when police have full and direct access to lateral surveillance, such access should be permitted only when democratically authorized – i.e. authorized through legislation or rules after ample public opportunity to comment. This regulation should include both *substantive* and *procedural* protections.

On the ***substantive*** front, every community must decide whether and how police are permitted to use information gathered from lateral surveillance. Examples of this type of regulation might include:

> ***Threshold Limitations:*** At a minimum, regulators should make illegal any use of lateral surveillance for non-legitimate law enforcement purposes, such as for personal use queries; to harass or intimidate an individual or group; to identify persons engaged in constitutionally-protected activities or participating in a noncriminal organization; or to identify persons based on their religious, political or social views, race, ethnicity, place of origin, age, disability, gender or gender identity, sexual orientation or other classifications protected by law. Given the risk that lateral surveillance can lead to overpolicing of low-level offenses and divert officer resources from preventing serious crime, jurisdictions may well decide to limit the types of offenses that lateral surveillance may be used to investigate.
>
> ***Prohibited Uses:*** Jurisdictions might decide to prohibit police reliance on certain types of lateral surveillance – such as private individuals aiming license plate readers at public roads. Why, after all, should private individuals be free to

use advanced technologies to track the comings and goings of others and turn that information over to authorities? Jurisdictions might prohibit police use of certain categories of lateral surveillance, except to investigate only the most serious of crimes. Jurisdictions around the country have done this with facial recognition technology, familial DNA searches, and wiretaps.[72] Jurisdictions also may choose to impose more specific restrictions, such as prohibiting certain types of real-time or extended surveillance.

In addition to these substantive limits, lawmakers should also consider enacting ***procedural*** protections on police use of lateral surveillance. Again, the details are up to communities and policymakers to decide, but here are a few examples of what might be considered:

Warrant Requirements: Short of prohibiting certain uses, jurisdictions can require agencies to obtain a warrant before accessing certain types of data (such as real-time or extended video data) or to obtain a court order before using the data they obtain in certain ways (e.g., using camera data for facial recognition). Similar requirements exist in other contexts (e.g., wiretaps), providing additional protection where police surveillance poses special risks. Warrants could require case-specific facts establishing probable cause to believe that the methods sought to be used, in the particular times and locations specified, will yield evidence relevant to the crime under investigation.

Mandatory Use Policies: Jurisdictions can require agencies to create and make available for public comment a use policy that defines how they will use the product or service. That policy should be available to the public. It should include:

- prohibiting employees, when acting in their official capacities, from using products and services not officially authorized by the agency,
- disclosure of how the authorized products and services function,
- authorized uses and users,
- training requirements,
- standard procedures, such as requiring officers to inform people of their right to refuse to share information, to obtain written consent, and to enable people to withdraw their permission (this may include prohibiting

subsidy or donation programs that require users to turn over their data to police),

- specificity requirements, so as to prevent overbroad requests (e.g., requests for videos of "suspicious" activity or persons),
- prohibiting officers from obtaining information except for public use,
- internal oversight mechanisms, such as supervisor approval for certain uses and an audit process to ensure officers are complying with the policy,
- privacy protections, including protocols for data retention and data purge,
- data security requirements, including protocols to prevent and mitigate harm from data breaches, and
- penalties for misuse.

Accountability by Design: Jurisdictions can require agencies to use products and software that have audit trails built in so that agencies can track:

- the name(s) of officer(s) conducting the search;
- case number and date/time of incident;
- type of incident under investigation;
- type and purpose of the search;
- search results, including any surveillance information viewed or downloaded by the officer(s); and
- whether the search produced useful investigative results.

Transparency & Reporting: Jurisdictions can require agencies to be transparent with the public about how they are using information obtained from lateral surveillance, including through periodic public reports that show how often and how much lateral surveillance information was accessed, and how that information contributed to criminal investigations. These periodic public reports should aggregate and anonymize the information tracked for individual cases and also should include summary statistics on the number of searches conducted, the type of crime or incident associated with the search, and investigation outcomes.

Enforcement: Regulation must come with enforcement mechanisms. In this

context, enforcement should include internal disciplinary consequences, rules about what happens to illegally-obtained evidence, and redress procedures for individuals who are inappropriately subjected to surveillance. There should also be consequences for agencies that allow repeat violations of applicable lateral surveillance laws or policies.

The size and consequences of lateral surveillance are too solemn to be addressed through the good will of companies. The time is now for policymakers to set sensible rules guiding police use of lateral surveillance technologies, lest we create the infrastructure ripe for government abuse.

IV. Summary of Ring's Changes During This Audit

During the course of this audit, Ring has made over 100 changes. In this Part, we recount some of the most significant.

Transparency

Transparency is the foundation of democratic governance. Without adequate information, the public cannot have informed opinions, and legislatures cannot make informed decisions. During the course of the audit, Ring implemented several changes to facilitate greater transparency around police use of NPSS. Among these are:

- Ring made it clearer that law enforcement uses Neighbors in various ways, including through posts on the Neighbors app and the Active Agency Map.
- Ring now publishes publicly NPSS training materials, press resources, and terms of service and discloses all donation initiatives involving government agencies.
- All agencies on NPSS now have an agency profile which includes the full text of an agency's posts and Requests for Assistance, among other information.
- Ring now requires all RFAs to specify the type of offense(s) under investigation and takes measures to ensure agencies provide accurate case numbers for each request.
- Ring has created audit trails for each Request for Assistance which include the user's name and the incident number.
- Ring now generates usage reports for each agency which includes details about the communications of each of the agency's NPSS users. Because Ring shares the report with the agency's NPSS coordinator, it is available for public records requests.

- Ring now publishes a bi-annual law enforcement request report with details about subpoenas and warrants Ring received, whether they were accompanied with non-disclosure orders, and how Ring responded.

- Ring has banned the posting of false or misleading information by NPSS users and now requires that police use official NPSS accounts.

- Ring will encourage policing agencies to adopt a formal internal policy governing NPSS by providing those agencies with a model policy drafted by the Policing Project. (We expect this model to be available in early 2022.)

- Ring has agreed to stop citing data regarding Ring's impact on crime until such data has been verified through independent study. Ring also reviewed all of its marketing and social media materials to remove any claims about crime reduction.

Overpolicing

Police today often are used as society's de facto responders to low-level offenses rooted in complex social problems, such as mental illness, homelessness, substance abuse, eviction, and poverty. A great deal of attention of late has been paid to the fact that for these sorts of issues, police are not trained to be the ideal responders, and lack the capacity to solve the underlying problems. In addition, whenever police respond, they bring with them the possibility of using force and making arrests. Thus, even if behavior is "criminal," in some circumstances having police respond with force and arrests causes great harm and does little to address the underlying problem. During the course of the audit, Ring implemented several changes to mitigate the risk that its platform will contribute to overpolicing, including:

- Ring temporarily has stopped actively recruiting policing agencies to join Neighbors and shifted to recruiting fire departments. Ring states that in the future it will try to onboard other government agencies such as public health departments, animal services, and agencies that address homelessness, drug addiction, and mental health.

- Ring no longer will donate devices to policing agencies or accept or provide financial contributions from policing agencies.

- Ring no longer will permit its employees to bring Neighbors incidents to law enforcement's attention, nor encourage users to file police reports.

- Ring no longer will participate in police sting operations.

- Ring has changed its guidelines to not allow users to post incidents about activity that may have innocent explanations – such as opening a screen door or mailbox.

- Ring has implemented a "Stop and Think Screen" which directs users, before a post is completed, to consider whether there is an innocent explanation for the activities they are reporting, and to ask them to think twice whether the issue even warrants neighborhood attention.

- Ring has given users the ability to turn off comments on their posts.

We have recommended that Ring onboard more government agencies, beyond policing agencies and fire departments, and that Ring onboard established non-governmental community organizations dedicated to public safety. Both present logistical challenges in terms of identifying and vetting organizations. Ring continues to explore these recommendations.

Bias

Bias in policing is a structural problem. A wealth of research and lived experience demonstrates that every aspect of law enforcement – from stops to arrests – disproportionately impacts people of color. This often results from implicit bias – for example, perceiving members of a certain race as more dangerous or threatening. There is also an unfortunate history of *explicit* bias – reporting individuals to the police with malicious intent. During the course of the audit, Ring implemented several

important changes to reduce the risk of bias on its platform. These include:

- Working with the Center for Democracy and Technology, to strengthen and update it content moderation practices. Ring's updated Community Guidelines reduce the possibility of profiling by, among other things, prohibiting speculative posts about merely suspicious activity, setting clearer guidelines regarding what kind of conduct can be reported, and eliminating certain types of posts (e.g., "Suspicious" or "Unexpected Activity").

- Ring updated the training of its moderation team to be sensitive to issues of bias – they are instructed to reject posts that engage in profiling, make negative judgments about a person based upon protected attributes, or that call attention to such attributes when they are irrelevant.

- Ring is implementing procedures to suspend or ban Neighbors users with a history of posting problematic content.

Coercion

Although some have claimed that individuals may feel coerced to share video with police, there is little evidence that this occurs in the context of Neighbors and NPSS. Still, Ring has made changes to reduce the possibility of coercion on its platform. Among them are:

- Ring makes clear through the Requests for Assistance process that individuals are under no obligation to share video.

- Ring has updated its NPSS Terms of Service to include a number of terms banning coercive tactics, including requiring the agency to maintain appropriate access controls on NPSS credentials and requiring NPSS users include their real name, title, and agency contact information.

- Ring no longer donates devices to policing agencies. Regarding other entities that receive donations, Ring prohibits entities from requiring individuals to:

- Share their Ring video footage with a third-party;
- Share access to Ring devices with a third-party;
- Share information captured by their Ring devices with a third-party;
- Register their Ring device with a third-party;
- Provide proof or confirmation of Ring device installation;
- Purchase a Ring video recording subscription or make a purchase of any kind.

- Ring has committed to not providing agencies with maps or location information regarding device owners, and has strengthened its obfuscation of the locations of posts.

Privacy

There are some circumstances in which surveillance, even of conduct occurring in public view, can potentially implicate individuals' privacy interests. Extended surveillance, especially surveillance of sensitive locations such as the home, can potentially be invasive. So too can bulk or "dragnet" surveillance, where police collect data on individuals indiscriminately and without constraint. In light of these concerns, Ring has implemented several important changes to mitigate the privacy risks resulting from police use of its products and services, including:

- Ring has made the retention period for videos customizable to give users greater control over their data.

- Ring has deleted all personal information it gathered in connection with past donation or subsidy programs.

- Ring updated its Law Enforcement Guidelines to clarify that Ring will always require a warrant or user consent before turning over stored user videos (absent exigency exceptions) and that Ring will notify users before disclosing their information (absent established exceptions). Ring also clarified that it will only provide non-content information in response to subpoenas.

- Ring device owners can now choose to enable end-to-end encryption, which prevents Ring from accessing or sharing the content of the owner's videos. (The company began this effort prior to engaging with NYU, but we mention this change here as it relates to concerns over privacy and self-surveillance.)

We have recommended Ring consider whether and how to revise its terms of service to prohibit users from granting police direct access to their cameras, absent democratic authorization.

Democratic Accountability

As discussed, the growth of networked lateral surveillance has significant implications for democratic governance of policing. Although Ring does not facilitate direct access to customer cameras, sending out an RFA is far easier for police than going door to door, and in that way, can serve to expand police surveillance capabilities without having to go through any democratic process. Ring has made important changes to enhance democratic accountability around police use of Ring devices. These include:

- Ring will not participate in device discount programs unless the program is authorized democratically.

- Ring will not onboard immigration and federal law enforcement agencies, because they agencies are not democratically accountable to their local communities.

- Ring has placed a moratorium on onboarding private policing agencies, with possible case-by-case exceptions for private agencies that are peace officers under state law and subject to constitutional restrictions.

Endnotes

[1] *See* POLICING PROJECT, CIVIL RIGHTS & CIVIL LIBERTIES AUDIT OF BALTIMORE'S AERIAL INVESTIGATION RESEARCH PROGRAM (2020), https://bit.ly/3pnWqkT.

[2] *See* AXON AI ETHICS BOARD, FIRST REPORT OF THE AXON AI & POLICING TECHNOLOGY ETHICS BOARD (2019), https://bit.ly/3Gah7HV.

[3] *See* T.J. McCue, *Home Security Cameras Market to Surpass $9.7 Billion By 2023*, FORBES (Jan. 31, 2019), https://www.forbes.com/sites/tjmccue/2019/01/31/home-security-cameras-market-to-surpass-9-7-billion-by-2023/#3f3bea523c2b.

[4] These devices were not the focus on this audit. *See supra* note A.

[5] Because of requirements under European law that are absent in the United States, Ring offers video retention for up to 30 days in some European countries.

[6] *Ring's Stance on Facial Recognition Technology*, RING (Aug. 20, 2020),

[7] *See Neighbors Safety Report*, RING, https://support.ring.com/hc/en-us/articles/360035191972-Neighbors-Safety-Report (last visited Dec. 1, 2021).

[8] *Neighbors by Ring Community Guidelines*, RING, https://support.ring.com/hc/en-us/articles/115004851266-Ring-Neighbors-Community-Guidelines (last visited Dec. 1, 2021).

[9] *See* Caroline Haskins, *How Amazon and the Cops Set Up an Elaborate Sting Operation that Accomplished Nothing*, VICE (July 1, 2019), https://www.vice.com/en/article/43jmnq/how-amazon-and-the-cops-set-up-elaborate-sting-operation-that-accomplished-nothing.

[10] *See* Steven Rodas, *'Tis the 'Porch Pirate' Season, but Hudson County Communities Are Fighting Back*, JERSEY JOURNAL (Dec. 1, 2019), https://www.nj.com/hudson/2019/12/tis-the-porch-pirate-season-but-hudson-county-communities-are-fighting-back.html.

[11] *See* Caroline Haskins, *US Cities Are Helping People Buy Amazon Surveillance Cameras Using Taxpayer Money*, VICE (Aug. 2, 2019), https://www.vice.com/en_us/article/d3ag37/us-cities-are-helping-people-buy-amazon-surveillance-cameras-using-taxpayer-money.

[12] *See* Haskins, *supra* note 12; Louise Matsakis, Cops Are Offering Ring Doorbell Cameras in Exchange for Info, WIRED (Aug. 2, 2019), https://www.wired.com/story/cops-offering-ring-doorbell-cameras-for-information; Alfred Ng, *Amazon's Helping Police Build a Surveillance Network with Ring Doorbells*, CNET (June 5, 2019), https://www.cnet.com/features/amazons-helping-police-build-a-surveillance-network-with-ring-doorbells.

[13] The canvassing area for a video request can be set between .025 and .5 square miles. *See Neighbors Public Safety Service Help Center - FAQ's*, RING, https://help.publicsafety.ring.com/hc/en-us/categories/360001506493-FAQ-s (last visited Mar. 4, 2021).

[14] *See Active Agency Map*, RING, https://support.ring.com/hc/en-us/articles/360035402811-Active-Law-Enforcement-Map (last visited Dec. 1, 2021).

[15] MEMORANDUM OF UNDERSTANDING, FERNDALE POLICE DEP'T, https://legistarweb-production.s3.amazonaws.com/uploads/attachment/pdf/400492/Ring_MOU_-_Ferndale_Police_Department_MI.pdf.

[16] Kate Cox, *Ring Asks Police Not to Tell Public How Its Law Enforcement Backend Works*, ARS TECHNICA (Aug. 21, 2019), https://arstechnica.com/tech-policy/2019/08/dont-call-our-surveillance-products-surveillance-ring-tells-police.

[17] *See* Caroline Haskins, *Amazon Requires Police to Shill Surveillance Cameras in Secret Agreement*, VICE (July 25, 2019), https://www.vice.com/en/article/mb88za/amazon-requires-police-to-shill-surveillance-cameras-in-secret-agreement.

[18] Ring publicizes its work with public safety agencies, as do the public safety agencies that use Neighbors and NPSS. *See, e.g.*, Ring, *How a Dallas Community Used the Neighbors App to Make Their Neighborhood Safer*, YOUTUBE (May 8, 2018), https://www.youtube.com/watch?v=F44O9hVuUVc.

[19] *See Get Updates from Public Agencies*, NEXTDOOR, https://nextdoor.com/agencies (last visited Mar. 4, 2021).

[20] *A Helpful Guide to Request for Assistance Posts*, RING, https://support.ring.com/hc/en-us/articles/360061496911-A-Helpful-Guide-to-Request-for-Assistance-Posts (last visited Dec. 1, 2021).

[21] *See* Stored Communications Act, 18 U.S.C. § 2703. Known colloquially as cloud computing or storage services, "remote computing services" means "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

[22] For 2020 data, see *Law Enforcement Information Requests in 2020*, RING, https://blog.ring.com/2021/01/20/law-enforcement-information-requests-in-2020 (last visited Mar. 10, 2021). For 2019 data, see *Law Enforcement Information Requests*, RING, https://blog.ring.com/2020/03/27/law-enforcement-information-requests (last visited Mar. 10, 2021).

[23] *See Law Enforcement Information Requests*, RING (Mar. 27, 2020),

[24] *Id.*

[25] *See Emergency Law Enforcement Information Request Form*, RING, https://support.ring.com/hc/en-us/article_attachments/360081269691/Ring_Emergency_Law_Enforcement_Request_Form.pdf.

[26] *E.g.*, Brandon C. Welsh et. al., *Effectiveness and Social Costs of Public Area Surveillance for Crime Prevention*, 11 ANN. REV. L. & SOC. SCI. 111, 117 (2015).

[27] *See id.*; Eric L. Piza et al., *CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis*, 18 CRIM. & PUB. POL'Y 135, 148–49 (2019).

[28] *See* Welsh, *supra* note 27, at 117.

[29] *See, e.g.*, Hollie Silverman & Artemis Moshtaghian, *How a Ring surveillance system and an alert couple helped lead to the capture of an escaped inmate in Tennessee*, CNN (Aug. 12, 2019), https://www.cnn.com/2019/08/12/us/tennessee-inmate-captured-monday/index.html.

[30] *See Caught in the Act*, RING, https://tv.ring.com/category/videos/caught-in-the-act (last visited Feb. 25, 2021).

[31] *See* David K. Li, *Doorbell Security Camera Captures Killers Leaving Mississippi Crime Scene, Family Says*, NBC NEWS (Feb. 26, 2020), https://www.nbcnews.com/news/us-news/doorbell-security-camera-captures-killers-leaving-mississippi-crime-scene-family-n1143501.

[32] *See* Mark Harris, *Video Doorbell Firm Ring Says Its Devices Slash Crime—but the Evidence Looks Flimsy*, MIT TECH. REV. (Oct. 19, 2018), https://www.technologyreview.com/2018/10/19/103922/video-doorbell-firm-ring-says-its-devices-slash-crimebut-the-evidence-looks-flimsy.

[33] *See id.*

[34] *See, e.g.*, Cyrus Farivar, *Cute Videos, but Little Evidence: Police Say Amazon Ring Isn't Much of a Crime Fighter*, NBC NEWS (Feb. 15, 2020), https://www.nbcnews.com/news/all/cute-videos-little-evidence-police-say-amazon-ring-isn-t-n1136026; Alfred Ng, *Ring's Work With Police Lacks Solid Evidence of Reducing Crime*, CNET (Mar. 19, 2020), https://www.cnet.com/features/rings-work-with-police-lacks-solid-evidence-of-reducing-crime.

[35] *See* Barry Friedman, *Disaggregating the Police Function*, 169 PENN. L. REV. 925 (2021); Emily D. Buehler, *State and Local Law Enforcement Training Academies, 2018 – Statistical Tables*, U.S. DEP'T OF JUSTICE, BUREAU OF JUSTICE STATISTICS (2021) (aggregating data regarding training hours dedicated to topics such as mediation, conflict management, and mental illness).

[36] *See* Amanda Y. Agan, Jennifer L. Doleac & Anna Harvey, *Misdemeanor Prosecution*, NBER Working Paper No. 28600 (2021), https://www.nber.org/system/files/working_papers/w28600/w28600.pdf.

[37] *See* Saba Rouhani, Catherine Tomko, Noelle P. Weicker & Susan G. Sherman, *Evaluation of Prosecutorial Policy Reforms Eliminating Criminal Penalties for Drug Possession and Sex Work in Baltimore, Maryland*, JOHNS HOPKINS (2021), https://publichealth.jhu.edu/sites/default/files/2021-10/prosecutorial-policy-evaluation-report-20211019.pdf. Moreover, enforcement is unlikely to solve the challenges posed by people who are unhoused, some of whom are arrested time and again with no change in status.

[38] *See* Cathy Free, *Police Posted a Photo of a Man They Say Stole Diapers from Walmart. Strangers Across the Country Came to His Defense*, WASH. POST. (Oct. 1, 2021), https://www.washingtonpost.com/lifestyle/2021/10/01/walmart-diapers-police-steal-facebook.

[39] Some of these posts would be prohibited under Ring's new Community Guidelines.

[40] *See* Chris Gilliard, *Caught in the Spotlight*, URBAN OMNIBUS (Jan. 9, 2020), https://urbanomnibus.net/2020/01/caught-in-the-spotlight.

[41] *See, e.g.*, Ethan Bauer, *Neighborhood, Watched*, DESERET NEWS (Aug. 31, 2021), https://www.deseret.com/2021/8/31/22643588/neighborhood-watched-nextdoor-ring-amazon-neighbors-crime-rate-safety-pew-research; Sue Frantz, *Availability Heuristic: A Nextdoor Example*, MACMILLAN LEARNING (Mar. 19, 2019), https://community.macmillanlearning.com/t5/psychology-blog/availability-heuristic-a-nextdoor-example/ba-p/6890; Gene Balk, *The 'Nextdoor Effect' in Bellevue: A Familiar Reaction to Crime*, SEATTLE TIMES (Feb. 11, 2019), https://www.seattletimes.com/seattle-news/data/the-nextdoor-effect-in-bellevue-a-familiar-reaction-to-crime.

[42] *See* Isidoro Rodriguez, *Can U.S. Policing Be Saved*, CRIME REPORT (May 17, 2021), https://thecrimereport.org/2021/05/17/can-u-s-policing-be-saved ("[A]ccording to a 2020 Gallup poll, 82 percent of Americans overall support a greater role for community-based alternatives to policing, with half of

Americans overall (50 percent) strongly or somewhat supporting the idea of eliminating officer enforcement of nonviolent crimes entirely, including majorities of Black (72 percent) and Hispanic (55 percent) Americans.").

[43] Ariadna Matamoros-Fernández & Johan Farkas, *Racism, Hate Speech, and Social Media: A Systematic Review and Critique*, 22 TELEVISION & NEW MEDIA 205 (2020). Social scientists note that this may result from a combination of factors — in particular, online anonymity creates disinhibition, enabling people to engage in biased conduct without fearing repercussions. Moreover, online environments tend to facilitate *group polarization* — that is, an inclination for individuals to seek out like-minded people who share similar beliefs. *See* Brian TaeHyuk Keum & Matthew J. Miller, *Racism on the Internet: Conceptualization and Recommendations for Research*, 8 PSYCH. OF VIOLENCE 782, 784 (2018).

[44] *See* Caroline Haskins, *Amazon's Home Security Company Is Turning Everyone Into Cops*, VICE (Feb. 7, 2019), https://www.vice.com/en_us/article/qvyvzd/amazons-home-security-company-is-turning-everyone-into-cops.

[45] *E.g.*, Anthony G. Greenwald & Linda Hamilton Krieger, *Implicit Bias: Scientific Foundations*, 94 CAL. L. REV. 945, 951 (2006); L. Song Richardson & Phillip Atiba Goff, *Self-Defense and the Suspicion Heuristic*, 98 IOWA L. REV. 293 (2012).

[46] Chan Tov McNamarah, *White Caller Crime: Racialized Police Communication and Existing While Black*, 24 MICH. J. RACE & L. 335 (2019).

[47] Jan Ransom, *Amy Cooper Faces Charges After Calling Police on Black Bird-Watcher*, N.Y. TIMES (July 6, 2020), https://www.nytimes.com/2020/07/06/nyregion/amy-cooper-false-report-charge.html.

[48] *A Helpful Guide to Request for Assistance Posts*, RING, https://support.ring.com/hc/en-us/articles/360061496911-A-Helpful-Guide-to-Request-for-Assistance-Posts (last visited Dec. 1, 2021).

[49] *See* Cox, *supra* note 20; Haskins, *supra* note 12; Zack Whittaker, *Ring Refuses to Say How Many Users Had Video Footage Obtained by Police*, TECHCRUNCH (June 8, 2021), https://techcrunch.com/2021/06/08/ring-police-warrants-neighbors.

[50] *See Neighbors Public Safety Service Help Center*, RING, https://help.publicsafety.ring.com/hc/en-us (last visited Dec. 2, 2021).

[51] *See* Caroline Haskins, *Ring Doesn't Have Facial Recognition — Some Police Want to Add Their Own*, BUZZFEED NEWS (Nov. 27, 2019), https://www.buzzfeednews.com/article/carolinehaskins1/ring-doesnt-have-facial-recognition-some-police-want-to-add; Alfred Ng, *Amazon's Helping Police Build a Surveillance Network with Ring Doorbells*, CNET (June 5, 2019), https://www.cnet.com/features/amazons-helping-police-build-a-surveillance-network-with-ring-doorbells.

[52] *See, e.g.*, Annie McDonough, *How New York City is Watching You*, CITY & STATE (Apr. 30, 2019), https://www.cityandstateny.com/policy/2019/04/how-new-york-city-is-watching-you/177409 (New York City); Kate Kaye, *Privacy Concerns Still Loom Over Detroit's Project Greenlight*, SMART CITIES DIVE (Feb. 1, 2021), https://www.smartcitiesdive.com/news/privacy-concerns-still-loom-over-detroits-project-green-light/594230 (Detroit); Jennifer Brett, *'Real-Time Crimefighting.' Around 11,000 Cameras Watch Over Atlanta*, ATL. J.-CONST. (Nov. 1, 2019), https://www.ajc.com/news/local/real-time-crimefighting-around-000-cameras-watch-over-atlanta/qlF76c7sgdwBvtIa3luX8H (Atlanta).

[53] *See* Sidney Fussell, *Amazon Ring Will Survive the Anti-Surveillance Backlash*, ATLANTIC (June 24, 2019), https://www.theatlantic.com/technology/archive/2019/06/police-offer-amazon-ring-free-exchange-

access/592243; Alfred Ng, *Amazon's Helping Police Build a Surveillance Network With Ring Doorbells*, CNET (June 5, 2019), https://www.cnet.com/features/amazons-helping-police-build-a-surveillance-network-with-ring-doorbells.

[54] *See* Caroline Haskins, *How Ring Transmits Fear to American Suburbs*, VICE (Dec. 6, 2019), https://www.vice.com/en/article/ywaa57/how-ring-transmits-fear-to-american-suburbs; Matthew Guariglia, *Police Will Pilot a Program to Live-Stream Amazon Ring Cameras*, EFF (Nov. 3, 2020), https://www.eff.org/deeplinks/2020/11/police-will-pilot-program-live-stream-amazon-ring-cameras.

[55] Ring also noted that users may well decide to give direct access to a neighbor, and that neighbor might coincidentally happen to be a police officer. To be clear, our recommendation is to require democratic authorization for direct access to Ring devices by law enforcement acting in an *official* capacity.

[56] *See* Sam Biddle, *Amazon's Home Surveillance Chief Declared War on "Dirtbag Criminals" as Company Got Closer to Police*, INTERCEPT (Feb. 14, 2019), https://theintercept.com/2019/02/14/amazon-ring-police-surveillance.

[57] *See* Ng, *supra* note 16.

[58] *See, e.g.*, *Fast-Growing Web of Doorbell Cams Raises Privacy Fears*, N.Y. POST (July 22, 2019), https://nypost.com/2019/07/22/fast-growing-web-of-doorbell-cams-raises-privacy-fears; Kim Norvell, *To Fight Crime, Des Moines Police Want Neighbors, Businesses to Register Their Private Security Cameras*, DES MOINES REGISTER (Oct. 8, 2019), https://www.desmoinesregister.com/story/news/crime-and-courts/2019/10/08/des-moines-police-private-camera-registration-ring-google-nest-watch-dsm-security-footage/3908234002.

[59] *See, e.g.*, Fussell, *supra* note 65.

[60] *See* Kevin Rector, *LAPD Sought Ring Camera Footage of Crime During Summer Protests, Riling Privacy Advocates*, L.A. TIMES (Feb. 16, 2021), https://www.latimes.com/california/story/2021-02-16/lapd-sought-private-ring-footage-as-they-investigated-crimes-around-george-floyd-protests.

[61] United States v. Moore-Bush, 963 F.3d 29, 56 (1st Cir. 2020) (Barron, J., concurring).

[62] *See* Dan Milmo, *Amazon Asks Ring Owners to Respect Privacy After Court Rules Usage Broke Law*, GUARDIAN (Oct. 14, 2021), https://www.theguardian.com/uk-news/2021/oct/14/amazon-asks-ring-owners-to-respect-privacy-after-court-rules-usage-broke-law. Although this case did not involve police, it illustrates the concern that persistent surveillance of one's activities at home can implicate individuals' privacy, even if such activities are technically in public view.

[63] *See* Haskins, *supra* note 55.

[64] *See* Ng, *supra* note 16.

[65] *E.g.*, Zack Whittaker, *Judge Orders Amazon to Turn Over Echo Recordings in Double Murder Case*, TECH CRUNCH (Nov. 14, 2018), https://techcrunch.com/2018/11/14/amazon-echo-recordings-judge-murder-case(recordings from an Amazon Echo); Kathryn Gilker, *Bentonville Police Use Smart Water Meters as Evidence in Murder Investigation*, 5 NEWS ONLINE (Dec. 28, 2016), https://www.5newsonline.com/article/news/local/outreach/back-to-school/bentonville-police-use-smart-water-meters-as-evidence-in-murder-investigation/527-e74e0aa5-0e2a-4850-a524-d45d2f3fd048 (data from home's smart water meter); *see also* Christine Hauser, *In Connecticut Murder Case, a Fitbit is a Silent Witness*, N.Y. TIMES (Apr. 27, 2017), https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-

silent-witness.html (data obtained from victim's Fitbit). *See generally* Ángel Díaz, *When Police Surveillance Meets the 'Internet of Things'*, BRENNAN CTR. (Dec. 16, 2020), https://www.brennancenter.org/our-work/research-reports/when-police-surveillance-meets-internet-things.

[66] *See* Sam Biddle, *Doorbell Cameras Like Ring Give Early Warnings of Police Searches, FBI Warned*, INTERCEPT (Aug. 31, 2020), https://theintercept.com/2020/08/31/blueleaks-amazon-ring-doorbell-cameras-police.

[67] Although the Stored Communications Act authorizes the disclosure of content data by remote computing services (such as Ring) in response to *subpoenas*, 18 U.S.C. § 2703(b), the Fourth Amendment may well require that police obtain a warrant in order to compel a service provider to produce user files stored in the cloud. *See* United States v. Warshak, 631 F.3d 266, 285–88 (6th Cir. 2010) (recognizing reasonable expectation of privacy in cloud-stored emails. *See generally* Riley v. California, 573 U.S. 373, 397–98 (2014) (acknowledging cell phone users' privacy interests in cloud-stored files).

[68] The exceptions to customer notifications are provided for under the Stored Communications Act. §2705.

Because content data is owned by the customer, we recommended notifying customers of preservation requests unless prohibited by law. By doing so, Ring would notify customers of data preservation requests that cause Ring to retain content information that a user would reasonably believe is not being preserved (such as a video that otherwise would expire). These types of notifications are not required by law and they are not the norm in the tech industry.

[69] Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1760 (2019).

[70] JOSHUA REEVES, CITIZEN SPIES: THE LONG RISE OF AMERICA'S SURVEILLANCE SOCIETY (2017).

[71] Andreas Lichter et al., *The Long-Term Costs of Government Surveillance: Insights from Stasi Spying in East Germany*, J. EUROPEAN ECON. ASSOC. 1, 2 (2020); Marcus Jacob & Marcel Tyrell, *The Legacy of Surveillance: An Explanation for Social Capital Erosion and the Persistent Economic Disparity Between East and West Germany* (2010), at 23; Jue Jiang, *The Eyes and Ears of the Authoritarian Regime: Mass Reporting in China*, J. CONTEMP. ASIA (Sept. 2020) at 3.

[72] *See, e.g.*, 25 M.R.S.A. § 6001(1)(I) (Maine facial recognition law); M.D. Code Crim. Proc. § 17-102(b)(1) (Maryland forensic genealogy law); 18 U.S.C. § 2516(1) (federal wiretap law).