WE CAN WORK IT OUT

THE FALSE CONFLICT BETWEEN DATA PROTECTION AND INNOVATION

CALLI SCHROEDER†, BEN WINTERS†, AND JOHN DAVISSON†

INTRODUCTION

Data protection and innovation are frequently pitted against one another, like the tech world equivalent of Superman vs. Batman. However, like their comic book counterparts, conflict between the two is often manufactured or circumstantial, rather than based on some inherent tension. Further, the two may actually gain power by banding together.[1]

For many companies, governments, and lawmakers, it seems to be accepted as a given that data protection stifles

[†] Calli Schroeder is Global Privacy Counsel at the Electronic Privacy Information Center (EPIC).

[†] Ben Winters is Counsel at the Electronic Privacy Information Center (EPIC).

[†] John Davisson is Director of Litigation and Senior Counsel at the Electronic Privacy Information Center (EPIC).

[1] The existence of *The Justice League*, ignore the two bonding over the name "Martha," because that is not necessarily canon and was very annoying. *See generally* THE JUSTICE LEAGUE (Warner Bros. Pictures 2017).

innovation.[2] Indeed, the need to protect innovation is often raised as a reason to oppose or weaken proposed privacy laws, as when Representative Marsha Blackburn stated that, when companies follow the European privacy model, "[r]evenues fall, innovation stalls and you lose out to innovators who choose to work elsewhere."[3] Innovation is presented as an ultimate and unequivocal good while data protection is relegated to, at best, an annoying item on a checklist and, at worst, the enemy of innovation which will lead to economic detriment, the collapse of small companies and start-ups, and the death of scientific research and consumer choice.[4] Even more progressive takes on the two still speak to the necessity of a "balance"—essentially, making sure that the amount of data protection and the amount of innovation are appropriate, but still framing them as weakening or interfering with one another.[5]

This way of thinking often leads to technology policy that prioritizes innovation while sidelining data protection with mere lip service, like the recent National Security Commission on Artificial Intelligence ("NSCAI") report which essentially argues that data protection must be sacrificed to allow for more

[2] *5 Things to Keep in Mind When Navigating the World of Data Privacy*, KINESSO (Feb. 16, 2021), https://kinesso.com/5-things-to-keep-in-mind-when-navigating-the-world-of-data-privacy/ [https://perma.cc/CSN6-HYHF] ("Privacy is important—but—don't let it hinder innovation"); *see also* Rosemary Belson, *German Industry: Strict Privacy Laws Hinder Innovation*, POLITICO (Sept. 26, 2017), https://www.politico.eu/article/german-industry-strict-privacy-laws-hinder-innovation/ [https://perma.cc/H5AG-2KT9]; *see also* Monica Nickelsburg, *Amazon Warns Onerous Privacy Regulations Could Hinder Innovation in Senate Hearing*, GEEKWIRE (Sept. 26, 2018), https://www.geekwire.com/2018/amazon-warns-onerous-privacy-regulations-hinder-innovation-senate-hearing/ [https://perma.cc/QB3E-3365].

[3] Jathan Sadowski, *Why Does Privacy Matter? One Scholar's Answer*, ATLANTIC (Feb. 26, 2013), https://www.theatlantic.com/technology/archive/2013/02/why-does-privacy-matter-one-scholars-answer/273521/ [https://perma.cc/EHN8-7HAY].

[4] *See* Jennifer Huddleston, *The Price of Privacy: The Impact of Strict Data Regulations on Innovation and More*, AM. ACTION F. (June 3, 2021), https://www.americanactionforum.org/insight/the-price-of-privacy-the-impact-of-strict-data-regulations-on-innovation-and-more/ [https://perma.cc/YYQ6-HDUC].

[5] *See* David Deming, *Balancing Privacy with Data Sharing for the Public Good*, N.Y. TIMES (Feb. 19, 2021), https://www.nytimes.com/2021/02/19/business/privacy-open-data-public.html [https://perma.cc/CRU9-PYKW] (Stating privacy risks "should always be minimized and balanced against the benefits of the innovations that may arise from increased data availability.").

innovation (which it seems to believe will necessarily lead to economic and political good).[6] Similar sentiments have been frequently expressed by even consumer protection leaders, including Federal Trade Commission leaders.[7] That this oppositional perspective of data protection and innovation has permeated leadership speaks to the scope of this problem and the potential impact if left unaddressed. Sacrificing data protection in the name of innovation carries over to the text and enforcement of regulations, resource allocation and funding, regulatory and corporate priorities, and heightened risks to human rights.

By misunderstanding the nature of both data protection and innovation, this way of thinking limits each concept and leads to either allowing for less creative thinking or putting human rights at risk. We contend that data protection and innovation are not in conflict with one another and can, in fact, enhance and support one another when concentrated effort is made to strengthen both. To demonstrate this, we split the paper into two portions. First, we examine the background of the problem: the current understanding, its flaws, and how reframing can benefit us. Second, we look to real-world examples of how this thinking has been put in place, the detriments of that approach, and the potential for meaningful change through rethinking the data protection and innovation relationship.

I. BACKGROUND

In order to dismantle the wide-spread dichomatic understanding of data protection versus innovation, it is imperative that we first be clear on the meaning of each term.

[6] *See generally* NAT'L SEC. COMM'N ON ARTIFICIAL INTEL., FINAL REPORT 473 (2021), https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf [https://perma.cc/GKU5-ESGS] [hereinafter NSCAI].

[7] *See* Muaren K. Ohlhausen, Comm'n F.T.C., Room to Run: Regulatory Responses to Dynamic Changes in the Organization of Work 4 (July 30, 2015), https://www.ftc.gov/system/files/documents/public_statements/691841/150730roomtorunspeech.pdf [https://perma.cc/G6AX-SLWF] ("So let me suggest that the better course here is caution. We can simply wait and see what develops in this area. If real harms actually do arise, that is the appropriate time for action. At that point, we will know a lot more than we know now and we can narrowly tailor whatever regulation might be required to address that clear, identifiable harm. For now, we should let the market do one of the things it truly excels at: sorting out the innovations that are ultimately useful and beneficial to society.").

"Data protection" in the context of this document refers to more than merely the security of data. We mean the term to encompass privacy, data minimization, and data security. "Innovation" is typically used to refer to a novel approach to an existing practice (such as law enforcement, education, or more) or an entirely new idea.

With this understanding of the two concepts, we more fully look at the current framing and its flaws. First, we examine the current understanding of the two through examples. Next, we explore why this false conflict leads to problems and what those problems are. Finally, we look at the potential for good and growth in reframing the discussion and allowing for more collaborative thinking.

A. Current Understanding

Some of the most powerful corporations and policy-making bodies have historically used innovation as a justification for failure to prioritize data protection and privacy. It's also used as a threat to stave off substantial action that would require industry to innovate in a consumer and data protective way. Essentially, this argument boils down to two assumptions: that data protection is a limitation on innovation and that innovation is a greater good than data protection. Neither assumption is true.

A 2012 Federal Trade Commission report recommended a privacy framework that was "designed to be flexible to permit and encourage innovation…by not includ[ing] rigid provisions such as specific disclosures or mandatory data retention and destruction periods."[8] In response to a draft of this report, trade associations and companies hammered home a fear that implementing significant privacy protections would hinder innovation and the introduction of new projects. The Internet Association wrote that "any legislative proposal to address 'big data' may result in a 'precautionary principle problem' that

[8] F.T.C., PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 9 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/S4RS-9NZ7].

hinders the advancement of technologies and innovative services before they develop."[9]

In 2021, the NSCAI report repeatedly pushed that "the United States must do what it takes to retain its innovation leadership and position in the world."[10] Their influential policy recommendations, which they say as of September 2021 has inspired more than 190 pieces of legislation,[11] center on guiding billions of dollars toward procurement of AI systems in order to stay active in a "competition" with other global powers without investing money in adequate safeguards or testing and holding those systems accountable.[12] Of course, the NSCAI was comprised of individuals at Microsoft, Google, Oracle, Amazon, and many others large data-consuming companies that stand to profit from continued mass data collection and use, which is illustrative of regulatory capture and mirrors the way the companies have pushed one path to profit over privacy time and time again.[13]

The changing nature of information necessitates a more full understanding of the connection between data protection and innovation.[14] The two are too intertwined to operate independently of one another, so any developing policy in one area must include considerations of how the other will be affected.[15] Unfortunately, many businesses and industries still

[9] *See* Internet Association, Comments Concerning Big Data and the Consumer Privacy Bill of Rights 2 (Aug. 5, 2014), https://www.ftc.gov/system/files/documents/public_comments/2014/08/00019-92375.pdf [https://perma.cc/Y5S9-7US6].

[10] NSCAI, *supra* note 6, at 11.

[11] National Security Commission on AI (@AiCommission), TWITTER (Sept. 22, 2021, 9:37 AM), https://twitter.com/AiCommission/status/1440701757353443346 [https://perma.cc/52DD-K59P].

[12] *See generally* NSCAI, *supra* note 6, at 157–67, 276–396.

[13] Tom Simonite, *This Group Pushed More AI in US Security—and Boosted Big Tech*, WIRED (Nov. 1, 2021), https://www.wired.com/story/group-pushed-ai-us-security-boosted-tech/ [https://perma.cc/3C8G-UCUL].

[14] *See generally* Avi Goldfarb & Catherine Tucker, *Privacy and Innovation*, 12 INNOVATION POL'Y & ECON. 65, 65–89 (2012), https://www.journals.uchicago.edu/doi/full/10.1086/663156#_i16 [https://perma.cc/8DMG-FKCR].

[15] *Id.*

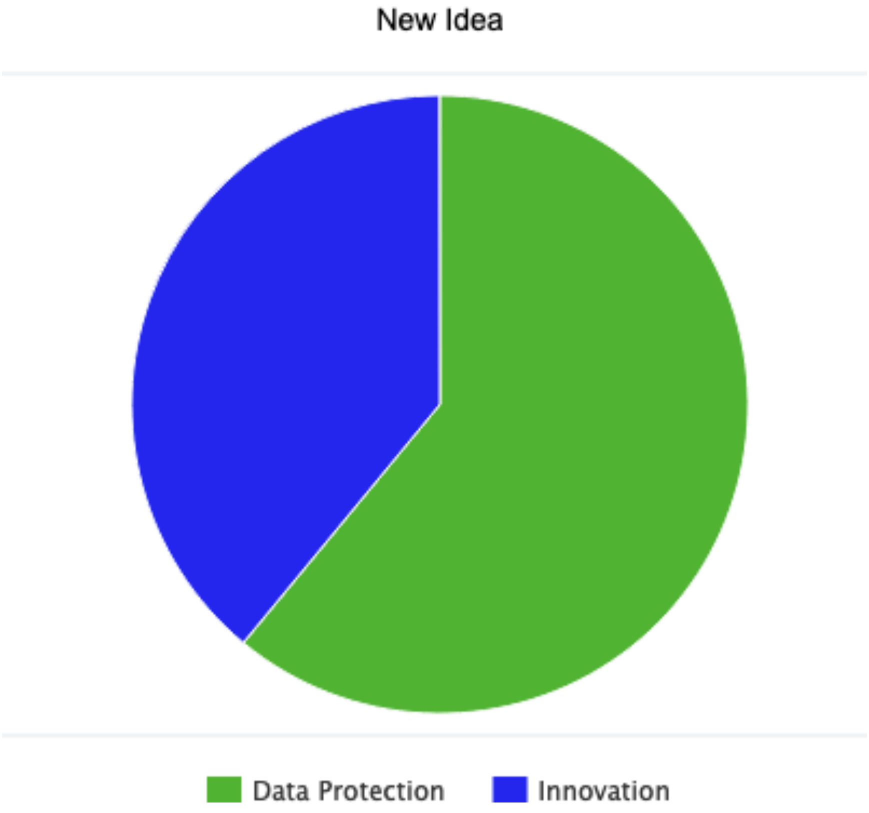
make the argument that proposed improvements to privacy policy are bad for industry, competition, and consumers.[16]

B. Problems With This Framing

Two key problems come out of the common framing of data protection and innovation existing in an adversarial state. First, this sets up a false binary choice where pursuit of one goal necessarily means some degree of sacrifice of the other. Second, the lack of effort to incorporate both in developments enshrines historically problematic structures rather than envisioning new approaches, effectively stifling true innovation.

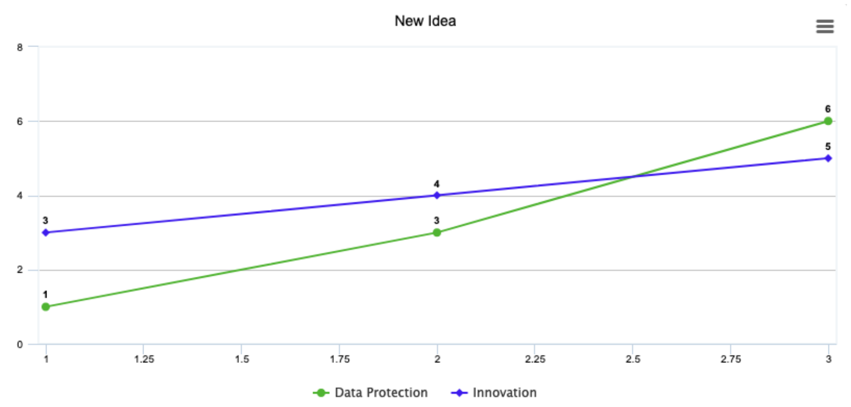
The false binary understanding of data protection and innovation posits, essentially, that any given approach can either be data protectionist or innovative. Any attempt to increase one of these values would necessarily lead to a decrease of the other. To visually represent this, consider the following pie chart.

[16] *See EPIC Freedom of Information Act Request to Federal Communications Commission re: Communications Relating to Privacy Regulations on Broadband Internet Access Service Providers,* ELEC. PRIV. INFO. CTR. (June 14, 2016), https://epic.org/wp-content/uploads/privacy/cpni/EPIC-16-06-14-FCC-FOIA-20160614-Request.pdf [https://perma.cc/RW9E-7UQ2]; *see generally* Adam Thierer & Ryan Hagemann, *Removing Roadblocks to Intelligent Vehicles and Driverless Cars*, 5 WAKE FOREST J.L. & POL'Y 339 (2015) (arguing that regulations on personal data collection and use by driverless vehicles will harm start-ups and small businesses and deprive consumers of potential innovations).



In this representation, the new idea is one finite whole and each priority—data protection and innovation—gets a portion. If the amount of data protection is increased, as in the chart, the amount of innovation is necessarily decreased and vice versa. This way of thinking is inherently limiting, functionally preventing innovators from imagining revolutionary approaches to data protection that could reinvent existing systems. In short, failing to consider data protection when crafting new products, systems, or approaches leads to more predictable and less creative solutions.

We posit that the relationship between data protection and innovation is more accurately represented by a line graph, as pictured below.



In this framing, the two concepts are not dependent on one another and both can increase or decrease independent of what the other does. This idea is more reflective of the true relationship between data protection and innovation and allows businesses to prioritize multiple areas when making developments, rather than determining that the end product is necessarily limited. It also allows the two concepts to be considered as equally valuable at the same time—there is no reason why the two cannot rise together.

The belief that one must choose either data protection or innovation often leads to time, effort, brain power, and overall resources being allocated to one goal rather than pursuing both concurrently. When determining which goal to pursue in this false framing, innovation is often treated as an unqualified good and privacy treated as a hindrance. However, innovation pursued for innovation's sake fails to pull back and consider whether developments are actually improvements or whether they are merely a novelty. It also can lead to a "create now and fix the problems later" mindset. This approach is what leads to the "move fast and break things" motto held by Facebook (now Meta) founder Mark Zuckerberg.[17] The results of this mindset have, indeed, yielded some world-changing designs. However, those often come at a substantial human cost, from contributing

[17] Hemant Taneja, *The Era of "Move Fast and Break Things" Is Over*, HARV. BUS. REV. (Jan. 22, 2019), https://hbr.org/2019/01/the-era-of-move-fast-and-break-things-is-over [https://perma.cc/GZ3L-6XWK].

to body image issues in young people to enabling stalking to live-streaming mass shooting or contributing to genocide.[18]

Shifting the framework to assume by default that innovation will work with data protection has several important benefits. First, it forces innovators to look at the systems that they operate within, challenging structure at a systemic level and reimagining historic practices rather than merely replicating existing social order. It also creates a greater focus on human rights as they interact with data protection, allowing for increased focus on alleviating harms, particularly for historically and systemically marginalized groups.

Real-world examples demonstrate that a data protection priority may encourage more innovation. Apple, for instance, was named the most innovative company in the world by a recent Fast Company survey, due in part to its creativity in developing features that assist in user privacy and security.[19]

[18] *See* Billy Perrigo, *Instagram Makes Teen Girls Hate Themselves. Is That a Bug or a Feature?*, TIME (Sept. 16, 2021), https://time.com/6098771/instagram-body-image-teen-girls/ [https://perma.cc/FT3L-87NS]; *see* James Vincent, *Instagram Internal Research: 'We Make Body Image Issues Worse for One in Three Teen Girls'*, VERGE (Sept. 15, 2021), https://www.theverge.com/2021/9/15/22675130/facebook-instagram-teens-mental-health-damage-internal-research [https://perma.cc/38N7-5WMR]; Sam Levin, *Facebook Fires Engineer Accused of Stalking, Possibly by Abusing Data Access*, GUARDIAN (May 2, 2018), https://www.theguardian.com/technology/2018/may/02/facebook-engineer-fired-alleged-stalker-tinder [https://perma.cc/8ZZP-MNPE]; Lyra Hale, *New Book Says Facebook Employees Abused Access to Track and Stalk Women*, MARY SUE (July 13, 2021), https://www.themarysue.com/facebook-employees-abused-access-target-women/ [https://perma.cc/XD4U-RRYH]; Meagan Flynn, *No One Who Watched New Zealand Shooter's Video Live Reported It to Facebook, Company Says*, WASH. POST (Mar. 19, 2019), https://www.washingtonpost.com/nation/2019/03/19/new-zealand-mosque-shooters-facebook-live-stream-was-viewed-thousands-times-before-being-removed/ [https://perma.cc/77CE-9NAM]; Jack Stubbs, *17 Minutes of Carnage: How New Zealand Gunman Broadcast His Killings On Facebook*, REUTERS (Mar. 15, 2019), https://www.reuters.com/article/us-newzealand-shootout-livestreaming/17-minutes-of-carnage-how-new-zealand-gunman-broadcast-his-killings-on-facebook-idUSKCN1QW294 [https://perma.cc/92RT-KMHN]; Paul Mozur, *A Genocide Incited on Facebook*, *With Posts From Myanmar's Military*, N.Y. TIMES (Oct. 15, 2018), https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html [https://perma.cc/SJV2-4597].

[19] *As Leis de Proteção de Dados freiam a inovação?* [Do Data Protection Laws Curb Innovation?], OLHAR DIGITAL (Nov. 27, 2018), https://olhardigital.com.br/2018/11/27/noticias/as_leis_de_protecao_de_dados_freiam_a_inovacao/_[https://perma.cc/BNH9-2YKJ]; *see Most Innovative Companies Apple*, FAST COMPANY, https://www.fastcompany.com/company/apple [https://perma.cc/DRG7-49XE](last visited Mar. 7, 2022).

The following sections will describe how prominent technology used in three key sectors with substantial power asymmetries illustrates the false innovation and data protection trade-off. In education, invasive proctoring tools adopted at an even higher-than-normal rate during the COVID pandemic were sold as innovative must-haves, but are ineffective, inaccurate, and shortsighted. In employment, automated tools used throughout the job application process increase surveillance, limit opportunities for diverse applicants, and force data collection on employees. In law enforcement, predictive policing tools and networked surveillance tools like Amazon's Ring encode and entrench racists policing, encourages profiling, and contributes to a flood of collection of highly sensitive data. These sections will explain how the current forms of these tools are *not* innovative, and how a stronger focus on data protection could help obviate where these tools can be improved.

II. EDUCATION

In March 2020, as the COVID-19 pandemic began to set in across the United States, many colleges and universities took the drastic step of suspending in-person instruction to limit the transmission of the novel coronavirus.[20] Within a matter of weeks, higher education was upended, undergoing a radical shift to predominantly remote learning.[21] This sea change forced a series of urgent questions on administrators and instructors: in an era of remote learning, how should students be evaluated in their courses? Should instructors who had administered tests and exams prior to the pandemic continue to do so remotely? And, if so, how should those assessments be carried out without the availability of in-person proctoring and supervision?

[20] *See* Sarah Mervosh & Vanessa Swales, *Colleges and Universities Cancel Classes and Move Online Amid Coronavirus Fears*, N.Y. TIMES (Mar. 10, 2020), https://www.nytimes.com/2020/03/10/us/coronavirus-closings.html [https://perma.cc/LA82-G3U9].

[21] *See The Evolution of Distance Education in 2020*, UNIV. KAN. SCH. ED. & HUM. SCI. BLOG (Sept. 17, 2020), https://educationonline.ku.edu/community/distance-education-evolution-in-2020 [https://perma.cc/KS3B-ZCQC] ("More than 1.5 billion students, or 91.3% of global enrollments, were directly affected by school closures at the height of the COVID-19 outbreak in early April.").

In response, many institutions and instructors made the hurried decision to continue administering exams with the aid of test surveillance tools, also known as remote proctoring, online proctoring, or e-proctoring.[22] Remote proctoring systems vary in their details, but as a general matter these tools capture video, audio, and other inputs from a student's computer to deter and—in theory—identify possible indicators of cheating.[23] Typically a student must give the proctoring tool access to their home computer or laptop by installing a browser extension or other piece of software before an exam.[24] Using this access, the proctoring system captures video and audio of the student and their surroundings and may record data about the student's computer usage during the exam session, including keystrokes and any websites visited.[25] The system may also temporarily lock down the student's computer, preventing them from accessing other applications during an exam.[26]

The data captured by a remote proctoring system is processed in one or several ways. Some systems rely on human proctors to monitor and review test sessions, either in real time[27] or after the fact.[28] In other cases, data captured by a remote proctoring system is processed in the first instance—either in whole or in part—by algorithms or artificial intelligence.[29] These systems purport to automatically detect indicators of student behaviors associated with cheating or otherwise designated as impermissible by the instructor or institution

[22] Sean Gallagher & Jason Palmer, *The Pandemic Pushed Universities Online. The Change was Long Overdue*, HAR. BUS. REV. (Sept. 29, 2020), https://hbr.org/2020/09/the-pandemic-pushed-universities-online-the-change-was-long-overdue [https://perma.cc/XHZ9-UASD].

[23] *In re Online Test Proctoring Companies*, ELEC. PRIV. INFO. CTR. (Dec. 9, 2020), https://epic.org/documents/in-re-online-test-proctoring-companies/ [https://perma.cc/GU27-EFKS].

[24] *Id.*

[25] *Id.*

[26] *See, e.g.*, *LockDown Browser*, RESPONDUS, https://web.respondus.com/he/lockdownbrowser/ [https://perma.cc/SC9H-472P] (last visited Mar. 7, 2022).

[27] *See, e.g.*, *Live+*, PROCTORU, https://www.proctoru.com/services/live-online-proctoring [https://perma.cc/MB7S-9PNA] (last visited Feb. 17, 2022).

[28] *See, e.g.*, *Review+*, PROCTORU, https://www.proctoru.com/services/review-plus [https://perma.cc/U9H2-TWCN](last visited Feb. 5, 2022).

[29] *See, e.g.*, *Record+*, PROCTORU, https://www.proctoru.com/services/record-plus [https://perma.cc/R2WC-G7WA](last visited Feb. 5, 2022).

administering the test.[30] Such systems may rely on facial recognition, eye movement tracking, or other forms of biometric analysis.[31] Based on its evaluation of an exam session, the proctoring system will generate flags, risk scores, or other indicators of prohibited behaviors.[32] These behaviors may include looking offscreen, so-called "atypical" eye or bodily movements, audible talking, or unusual shadows in the student's room.[33]

Risk scores and flags generated by automated proctoring tools are provided to the instructor or administrator, who can review the reports generated by the system, typically alongside the recording of the student's exam session.[34] Based on this information, an instructor or administrator may decide to follow up with a student suspected of cheating during a remote exam or potentially initiate academic disciplinary proceedings. Vendors of remote proctoring tools often note that it is up to the instructor or institution to decide whether flagged behavior warrants disciplinary follow-up,[35] but the flags and risk scores—at least in the first place—are the work of automated processing.

Although remote proctoring tools came into existence well before COVID-19, the pandemic triggered an explosion in their use.[36] But this rapid growth brought with it increased scrutiny

[30] ELEC. PRIV. INFO. CTR., *supra* note 23 ("Proctorio tracks speech, eye movements, and mouse clicks. This data is then analyzed for abnormal behavior. Proctorio claims that the software eliminates human error and bias.").

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *See, e.g.*, *Online Assessments and e-Proctoring: Guidance for Instructors*, UNIV. MINN., https://teachingsupport.umn.edu/resources/online-assessments-and-e-proctoring-guidance-instructors [https://perma.cc/R2PR-ETW4](last visited Mar. 7, 2022).

[35] Allie Luker, *How to Combine AI and Live Human Proctoring*, HONORLOCK (July 20, 2021), https://honorlock.com/blog/how-to-combine-ai-and-live-human-proctoring/ [https://perma.cc/A8MB-P88U] ("Easy Reviewing: The AI proctoring format makes it easy for instructors to review any incidents. Exam reports typically provide flags and allow the instructor to review the video if it was recorded to determine if the student broke any rules.").

[36] *See* Susan Grajek, *EDUCAUSE COVID-19 QuickPoll Results: Grading and Proctoring*, EDUCAUSE (Apr. 10, 2020), https://er.educause.edu/blogs/2020/4/educause-covid-19-quickpoll-results-grading-and-proctoring#fn2 [https://perma.cc/C5VR-NKQV] ("Over three-quarters of institutions may use online or remote proctoring for exams during the pandemic.

of, and pushback against, remote proctoring tools. Over the past two years, students, educators, and others have raised or renewed their objections to e-proctoring systems; arguing that these systems are ineffective,[37] collect excessive biometric and other personal data,[38] fail to fully disclose how that information is used and processed,[39] discriminate against students of color[40] and those with disabilities,[41] provoke emotional distress in test-takers,[42] signal distrust by instructors and administrators,[43] and lack sufficient safeguards to ensure that a student can understand or challenge a negative determination.[44] Students, educators, lawmakers, privacy and civil rights advocates, and

Half of institutions (54%) are currently using online or remote proctoring services, and another 23% are planning or considering using them.").

[37] Scott McFarland, *AI-only proctoring is risky and doesn't work. We're not doing it any more*, TIMES HIGHER EDUC. (May 29, 2021), https://www.timeshighereducation.com/blog/ai-only-proctoring-risky-and-doesnt-work-were-not-doing-it-any-more [https://perma.cc/C9AP-RZHF].

[38] *Complaint and Request for Investigation, Injunction, and Other Relief*, ELEC. PRIV. INFO. CTR. 1, 6–10 (Dec. 9, 2020), https://epic.org/wp-content/uploads/privacy/dccppa/online-test-proctoring/EPIC-complaint-in-re-online-test-proctoring-companies-12-09-20.pdf [https://perma.cc/ZT2L-TNEC].

[39] *Id.* at 10–16.

[40] Mitchell Clark, *Students of color are getting flagged to their teachers because testing software can't see them*, VERGE (Apr. 8, 2020), https://www.theverge.com/2021/4/8/22374386/proctorio-racial-bias-issues-opencv-facial-detection-schools-tests-remote-learning [https://perma.cc/75KD-J24M].

[41] Lydia X. Z. Brown, *How Automated Test Proctoring Software Discriminates Against Disabled Students*, CTR. FOR DEMOCRACY & TECH. (Nov. 16, 2020), https://cdt.org/insights/how-automated-test-proctoring-software-discriminates-against-disabled-students/ [https://perma.cc/PG56-TLPV].

[42] Daniel Woldeab & Thomas Brothen, *Video Surveillance of Online Exam Proctoring: Exam Anxiety and Student Performance*, 36 INT'L J. E-LEARNING & DISTANCE EDUC. 1, 21 (2021) ("As this study shows, being remotely monitored by webcam appears to be a source of anxiety for some students.").

[43] Nora Caplan-Bricker, *Is Online Test-Monitoring Here to Stay?*, NEW YORKER (May 27, 2021), https://www.newyorker.com/tech/annals-of-technology/is-online-test-monitoring-here-to-stay [https://perma.cc/8D49-YR3L] ("'When they can't get to know you as a good student, it furthers the weird distrust everyone is feeling,' she said. 'I felt like I was fighting to prove my academic integrity more than my knowledge.'").

[44] Jason Kelley, Bill Budington, & Sophia Cope, *Proctoring Tools and Dragnet Investigations Rob Students of Due Process*, ELEC. FRONTIER FOUND. (Apr. 15, 2021), https://www.eff.org/deeplinks/2021/04/proctoring-tools-and-dragnet-investigations-rob-students-due-process [https://perma.cc/7YXG-X4AL].

others have challenged these systems through a range of legal, policy, and grassroots organizing means.[45]

The pressure, it seems, has had an effect. A growing number of schools have refused to adopt or since abandoned remote proctoring, including Cabrillo College, City University of New York, Duke University, Princeton University, San Francisco State University, Stanford University, the University of Illinois-Champaign, the University of Massachusetts Lowell, the University of Michigan-Dearborn, and the University of Southern California.[46]

This trend is an encouraging one, yet it underscores a truth about the widespread adoption of remote proctoring that occurred at the outset of the COVID-19 pandemic: it didn't have to be this way. In far too many cases, the desire to replicate the basic features of in-person proctored exams led to a hasty institutional embrace of remote proctoring systems without regard for their efficacy or the privacy, civil rights, and emotional harms they cause. Rather than treating the pandemic-inflicted shift to online learning as an opportunity to reevaluate how students should be assessed, many institutions sought out testing solutions that most closely mimicked the conditions of the in-person testing they had long relied on. And test surveillance firms were eager to meet that demand with invasive in-home surveillance tools.

By contrast, a privacy-centric approach to evaluation counsels rejecting remote proctoring systems in favor of more creative forms of assessment that do not call for constant supervision. These may include "shorter, more numerous

[45] *See, e.g.*, *Protect Student Privacy: Ban eProctoring*, https://www.baneproctoring.com/ [https://perma.cc/8SA4-KZSN](last visited Mar. 7, 2022); *Blumenthal*, *Blumenthal Leads Call for Virtual Exam Software Companies to Improve Equity, Accessibility & Privacy for Students Amid Troubling Reports*, RICHARD BLUMENTHAL (Dec. 3, 2020), https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-leads-call-for-virtual-exam-software-companies-to-improve-equity-accessibility-and-privacy-for-students-amid-troubling-reports [https://perma.cc/E8TF-9U7J]; Drew Harwell, *Cheating-detection companies made millions during the pandemic. Now students are fighting back.*, WASH. POST (Nov. 12, 2020), https://www.washingtonpost.com/technology/2020/11/12/test-monitoring-student-revolt/ [https://perma.cc/5UZY-673L].

[46] *See, e.g.*, *Protect Student Privacy: Ban eProctoring,* https://www.baneproctoring.com/ [https://perma.cc/4JWQ-TJ3P](last visited Mar. 7, 2022).

quizzes; long papers, graded at multiple stages such as outline, first draft, and final draft; a series of shorter response papers; presentations with a peer critique component; an annotated research bibliography; student-proposed projects; and other creative approaches[.]"[47] If an instructor concludes that it is nevertheless necessary to give an exam, the risk of academic dishonesty can still be minimized without resort to remote proctoring. Instructors can administer exams in a "non-proctored environment" through the use of cheating acknowledgement statements, reduced timeframes, and non-traditional formats (such as open-book or oral exams).[48]

The University of Michigan-Dearborn provides an instructive example. When the COVID-19 pandemic set in, the University—concerned that remote proctoring "can constitute an invasion of privacy for students[] and can discriminate against students of color and disabled students"—made the laudable decision "to resist any new implementation of remote proctoring software and to invest in additional instructional design staff and programming to support instructors in implementing alternative assessments."[49] In lieu of traditional exams, the University's Hub for Teaching and Learning Resources urged instructors to "employ authentic assessments"[50]—"those that ask students to apply their knowledge on 'intellectually worthy tasks'"[51] and "those should have 'the same competencies, or combinations of knowledge, skills, and attitudes, that [students] need to apply in the criterion situation in professional life[.]'"[52] Not only are such

[47] Lindsey Barrett, *Rejecting Test Surveillance in Higher Education*, 1 MICH. ST. L. REV. (forthcoming 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3871423 [https://perma.cc/P96D-B6KS].

[48] *See, e.g.*, *Alternatives to Proctored Exams*, KY. CMTY. & TECH. COLL. SYS., https://kctcs.edu/education-training/kctcs-online/learn-by-term/proctor-exams/alternatives-to-proctored-exams.aspx [https://perma.cc/LX6B-EL8U] (last visited Mar. 7, 2022).

[49] Sarah Silverman et al., *What Happens When You Close the Door on Remote Proctoring? Moving Toward Authentic Assessments with a People-Centered Approach*, 39 TO IMPROVE THE ACADEMY 115, 115–16 (2021).

[50] *Id.* at 122.

[51] *See id.* (quoting Grant Wiggins, *The Case for Authentic Assessment*, 2 PRACTICAL ASSMT. RSCH. & EVAL. 1, 1 (1990)).

[52] *See id.* (quoting J. T. M. Gulikers et al*., A five-dimensional framework for authentic assessment*, 52 EDUC. TECH. RSCH. & DEV. 69, 75 (2004)).

assessments less susceptible to academic integrity concerns, they also "help motivate students because they connect the course material to real-world applications"[53] and "can help students avoid the test anxiety and cognitive overload that often accompany traditional, timed exams."[54]

These examples undercut the notion that privacy and innovation are in constant tension with one another. Indeed, in the context of remote assessment, prioritizing the privacy and dignity of students actually *compels* educational innovation—a marked contrast from the well-worn exam formats that have given rise to the invasive institution of remote proctoring.

III. HIRING AND EMPLOYMENT

Employment is another area rife with purported "innovations" that in fact simply recreate the status quo in a more digitized (and frequently more invasive) format. The rise in automated software and AI systems used for hiring, tracking performance metrics, determining payment, and at-home or on-device surveillance as workers shifted out of the physical office is frequently hailed as wildly innovative.[55] However, the lack of consideration for data protection in these shifts has not only

[53] *See id.* (citing Marilla D. Svinicki, *Authentic assessment: Testing in reality*, NEW DIR.S FOR TEACHING & LEARNING 23, 23–29 (2005)).

[54] *See id.* (citing Rona Carter et al., *Cognitive and emotional facets of test anxiety in African American school children*, 22 COGNITION & EMOTION 539, 539–51 (2008); citing Hamzeh Dodeen, *Assessing test-taking strategies of university students: Developing a scale and estimating its psychometric indices*, 33 ASSMT. & EVAL. IN HIGHER EDUC. 409, 409–19 (2008)).

[55] *See, e.g.*, *How innovative technology can revolutionise recruitment efforts*, IDG CONNECT (Sept. 28, 2021), https://www.idgconnect.com/article/3634474/how-innovative-technology-can-revolutionise-recruitment-efforts.html [https://perma.cc/3CUU-6LCN]; *see* Jon Gitlin, *How Automated Resume Screening Can Transform the Way Your Team Recruits,* WORKATO, https://www.workato.com/the-connector/automated-resume-screening/ [https://perma.cc/S7TW-DQ4L] (last visited Mar. 7, 2022); Kayla Kozan, *Talent Acquisition Innovation: Resume Screening Using AI*, IDEAL (Nov. 15, 2016), https://ideal.com/resume-screening-using-ai/ [https://perma.cc/3EZZ-BSJ3]; *4 Innovative Strategies for High-Volume Hiring*, EG WORKFORCE SOLUTIONS (Dec. 21, 2021), https://egnow.com/4-innovative-strategies-for-high-volume-hiring/ [https://perma.cc/T7WU-MXTV]; Benjamin Laker, *Embedding Artificial Intelligence at Work: From Efficiency Gains to Leadership Expertise*, FORBES (Nov. 14, 2021), https://www.forbes.com/sites/benjaminlaker/2021/11/14/embedding-artificial-intelligence-at-work-from-efficiency-gains-to-employee-experience/ [https://perma.cc/NTS8-XJ78].

caused demonstrable harm to individual dignity, human rights, and employment opportunities—it has also exposed a distinct lack of imagination in picturing and working towards systemic shifts in how we go about hiring and work. Many purported "innovations" in employment simply shift existing abuses and biases into a digital form.[56] To provide examples of this scenario, we look at three employment areas: resume and application review, interviews, and performance monitoring.

A. Resume and Application Review

The resume and application review process has always been time-consuming for businesses. Now, several companies tout "innovative" technology that will take care of the issue for recruiters.[57] Resume and application review systems (commonly referred to as Applicant Tracking Software or "ATS") have exploded in use in the past few years, with some surveys showing use by 98% of Fortune 500 companies.[58] Lists ranking the best systems for businesses are widely available as well.[59]

[56] *See, e.g.*, Zephyr Teachout, *When Big Brother is Your Boss: The Rise of Surveillance Wages*, NATION (Jan. 5, 2022), https://www.thenation.com/article/society/surveillance-wages-amazon-labor/ [https://perma.cc/CRV2-HP4F]; *see* Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, REUTERS (Oct. 10, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G [https://perma.cc/DU82-34VS].

[57] *See, e.g.*, Supriya Saxena, *5 Most Innovative ATS You Can Not Afford to Miss*, SOFTWARE SUGGEST (Feb. 5, 2021), https://www.softwaresuggest.com/blog/most-innovative-ats/# [https://perma.cc/E9BA-AZHM]; *Artificial Intelligence ATS: the Latest Innovation in Recruiting*, LOXO (Dec. 3, 2019), http://loxo.co/blog/artificial-intelligence-ats-the-latest-innovation-in-recruiting/ [https://perma.cc/235F-VY5W]; Colin Parker, *12 Reasons You Need a Modern Applicant Tracking System*, CRELATE (Mar. 19, 2020), https://www.crelate.com/blog/applicant-tracking-system [https://perma.cc/24QQ-BNTE].

[58] Jon Shields, *Over 98% of Fortune 500 Companies Use Applicant Tracking Systems (ATS)*, JOBSCAN (June 20, 2018), https://www.jobscan.co/blog/fortune-500-use-applicant-tracking-systems/ [https://perma.cc/3MJN-KU9X].

[59] Phil Strazzulla, *The Top 13 Best Applicant Tracking systems (ATS) – 2022*, SELECTSOFTWARE REV.S (Jan. 18, 2022), https://www.selectsoftwarereviews.com/buyer-guide/applicant-tracking-systems [https://perma.cc/GHF5-FGVA]; Tim Reitsma, *10 Best Applicant Tracking systems List [2022]*, PEOPLE MANAGING PEOPLE (Jan. 3, 2022), https://peoplemanagingpeople.com/tools/best-applicant-tracking-systems/ [https://perma.cc/8N5Z-74WK]; Hardik Vishwakarma, *The Top 15 Best Applicant*

Among many other features—such as scheduling email updates and potential interviews, setting deadlines, and putting out job posting updates—these systems review submitted resumes for keywords, generally preselected by the company using the system and related to desired skills or qualifications, filtering through applications for those keywords and determining which applications will be passed on for human review.[60] While the ATS likely does not choose who will be hired, they are frequently empowered to automatically reject or discard candidates, effectively barring certain candidates from consideration or human review.[61] In addition to the issues with the automated portion of ATS, many require candidates to create accounts in order to submit an application on these systems, which could lead to candidates creating multiple accounts across multiple systems during their job hunt.

This is a clear example of taking an existing system and merely shifting it to a digitized form while claiming that this shift makes the process innovative. In fact, this "innovation" recreates an existing system. Human resume reviewers often look for key qualifications and skills when reviewing applications to ensure the applicant is a good fit for the job. One may think that this points to a benign, though not necessarily novel or creative, shift in the application review process. However, there are serious detriments to these digitized systems.

First, automatic filtering will often remove a candidate from consideration prior to any human review.[62] This may result in

Tracking Systems in 2022, DATA DRIVEN INVESTOR (Oct. 26, 2021), https://medium.datadriveninvestor.com/the-top-15-best-applicant-tracking-systems-in-2022-96e0d425577c [https://perma.cc/QJ6N-PGGA].

[60] *See* Jon Shields, *8 Things You Need to Know About Applicant Tracking Systems*, JOBSCAN (May 27, 2021), https://www.jobscan.co/blog/8-things-you-need-to-know-about-applicant-tracking-systems/ [https://perma.cc/3Z63-6X7K]; James Hu, *How to Pick Resume Keywords That'll Get Your Job Application Past the ATS*, THE MUSE, https://www.themuse.com/advice/a-job-hunters-guide-to-getting-your-resume-past-the-ats-and-into-human-hands [https://perma.cc/X3JZ-HC5S](last visited Mar. 7, 2022); Finn Bartram, *How Do Applicant Tracking Systems Work?*, PEOPLE MANAGING PEOPLE (Mar. 2, 2021), https://peoplemanagingpeople.com/articles/how-do-applicant-tracking-systems-work/ [https://perma.cc/AD6F-XVE5].

[61] Aaron Rieke & Miranda Bogen, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, UPTURN (Dec. 10, 2018), https://www.upturn.org/work/help-wanted/ [https://perma.cc/UR7U-NPWR].

[62] *Id.*

several qualified candidates with less knowledge regarding how to "game" these systems losing out on employment opportunities. The illogic of the keyword filtration system is so well-known that there are now multiple articles available detailing how to manipulate the system to ensure that a resume is passed through for further review.[63] Second, a system cannot adjust for context as humans can. If an ATS system is set to look for "code" or "coding" as a key term but the applicant has written "programming" in their documents to describe skills, that applicant may be screened out. A human reviewer would be able to understand that programming would likely include coding.

In addition, bias will frequently be embedded in the system through which keywords or traits are given priority.[64] Algorithmic systems, which are trained on historic data, are likely to perpetuate biases that existed within prior hiring systems, such as selecting for more white-sounding names or favoring men over women.[65] Systems trained on historic hiring data reflect biased practices from the past without active intervention (for example, if a position was only open to men for a period of time, the historic data would skew a system to favor male applicants). Finally, forcing candidates to create separate accounts across multiple systems for application submission is unnecessary (resumes, cover letters, and the like could just as easily be submitted to a dedicated email address) and opens applicants up to higher risk of information leaking in the event

[63] *See, e.g.*, Regina Borsellino, *Beat the Robots: How to Get Your Resume Past the System and Into Human Hands*, THE MUSE, https://www.themuse.com/advice/beat-the-robots-how-to-get-your-resume-past-the-system-into-human-hands [https://perma.cc/6QPD-5HRV] (last visited Mar. 7, 2022); Ken Coleman, *How to Beat Applicant Tracking Systems (ATS)*, RAMSEY (Sept. 9, 2021), https://www.ramseysolutions.com/career-advice/how-to-beat-applicant-tracking-systems [https://perma.cc/KV4P-5MPA]; James Clift, *How to Beat an Applicant Tracking System (ATS) with a 100% Pass Rate*, VISUALCV (Oct. 21, 2020), https://www.visualcv.com/blog/how-to-beat-the-applicant-tracking-system/ [https://perma.cc/LKH7-J8HW]; Lee Woodrow, *How to Beat an Applicant Tracking System (ATS)*, LINKEDIN (Oct. 6, 2020), https://www.linkedin.com/pulse/how-beat-applicant-tracking-system-ats-lee/ [https://perma.cc/K4CY-NH5T].

[64] *See* Miranda Bogen, *All the Ways Hiring Algorithms Can Introduce Bias*, HARV. BUS. REV. (May 6, 2019), https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias [https://perma.cc/89KN-KC3W].

[65] Dastin, *supra* note 56; Gideon Mann & Cathy O'Neil, *Hiring Algorithms are Not Neutral*, HARV. BUS. REV. (Dec. 9, 2016), https://hbr.org/2016/12/hiring-algorithms-are-not-neutral [https://perma.cc/MZV3-DQ4N].

of a data breach—essentially, it broadens the potential risk surface for no real reason.

Concerns about these practices are significant, as are calls for regulations to better protect against algorithmic bias. New York City has already taken action with a new regulation addressing automated employment decision tools that will take effect on January 1, 2023.[66]

B. Interviews

"Innovative" technology that fails to consider privacy risks faces exponential problems related to job interviews. There has been a sharp rise in companies that offer "AI-driven assessments" of candidates that process minute and highly sensitive data like facial movements, vocal tone, and word choice during on-camera interviews to generate an "employability" score.[67] These assessments can include seemingly benign criteria, like asking for writing samples or having users take quizzes and personality tests or play games.[68] Some are much more invasive, using video interviews to analyze word choice and usage, eye movements, facial cues, and other traits to determine potential candidate job success.[69] All of these systems have serious flaws regarding bias and data protection.

[66] Simone R.D. Francis, *New York City to Restrict Use of Automated Employment Decision Tools: What Employers Should Know*, OGLETREE DEAKINS (Jan. 6, 2022), https://ogletree.com/insights/new-york-city-to-restrict-use-of-automated-employment-decision-tools-what-employers-should-know/ [https://perma.cc/M3XQ-VWCB].

[67] *See, e.g.*, *Hiring Experience Platform*, HIREVUE, https://www.hirevue.com/ [https://perma.cc/RAK3-YRHL] (last visited Mar. 7, 2021); Drew Harwell, *A Face-Scanning Algorithm Increasingly Decides Whether You Deserve the Job*, WASH. POST (Nov. 6, 2019), https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/ [https://perma.cc/ER7G-FGC8]; Matt O'Brien, *Want a Job? Employers Say, Talk to a Computer*, CHI. SUN TIMES (June 15, 2021), https://chicago.suntimes.com/2021/6/15/22535386/job-hunt-hirevue-computer-ai [https://perma.cc/N9DD-UQAQ].

[68] Hilke Schellmann, *Auditors Are Testing Hiring Algorithms for Bias, But There's No Easy Fix*, MASS. INST. TECH. REV. (Feb. 23, 2021), https://www.technologyreview.com/2021/02/11/1017955/auditors-testing-ai-hiring-algorithms-bias-big-questions-remain/ [https://perma.cc/RKK5-HXQN]; *Gamified Soft Skills Assessments*, PYMETRICS, https://www.pymetrics.ai/assessments [https://perma.cc/UNL6-H398] (last visited Feb. 23, 2022).

[69] Yixuan Xie, *AI for Candidate Screening: Eliminating or Reinforcing Bias*, MEDILL REP.S CHI. (Sept. 6, 2019),

Some flaws are ever-present. As discussed regarding resume and application review, when these systems are trained on existing data or previous criteria, they are likely to enshrine historic bias within the new hiring process.[70] For example, Pymetrics' technology includes a measure that has current employees play games to create a baseline of trait results which candidate results are then compared to.[71] However, if existing employees are all of one similar demographic (for example, all middle-class, middle-age, straight, white men), the baseline traits measured may reflect that demographic rather than any particular trait linked with doing the job well. Another problem is that collecting so much individualized data, including biometric data, creates a more broad risk surface for potential data misuse or breach.

The use of AI video and audio analysis in interviews has revealed larger problems. For example, HireVue, a prominent company offering autonomous interview analysis, claimed that its algorithmic assessment could collect up to 500,000 data points on candidates in 30 minutes, including intonation, inflection, and emotions.[72] HireVue further claimed that its algorithmic analysis could use these traits to determine cognitive ability, psychological traits, emotional intelligence, and social aptitudes of candidates.[73] However, questions regarding how these traits were determined by the algorithm were often unanswered, possibly because "the company doesn't

https://news.medill.northwestern.edu/chicago/ai-for-candidate-screening-eliminating-or-reinforcing-bias/ [https://perma.cc/N2DT-GY4Y].

[70] *See, e.g.*, Dastin, *supra* note 56.

[71] *Retorio vs. Pymetrics*, RETORIO, https://www.retorio.com/competitors/pymetrics [https://perma.cc/79UH-2KQ7] (last visited Feb. 6, 2022); Josh Constine, *Pymetrics Attacks Discrimination in Hiring with AI and Recruiting Games*, TECHCRUNCH (Sept. 20, 2017), https://techcrunch.com/2017/09/20/unbiased-hiring/ [https://perma.cc/RF25-79HC].

[72] Drew Harwell, *A Face-Scanning Algorithm Increasingly Decides Whether You Deserve the Job,* WASH. POST (Nov. 6, 2019), https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/ [https://perma.cc/2M3A-D63H]; *Complaint and Request for Investigation, Injunction, and Other Relief Submitted by The Electronic Privacy Information Center (EPIC)*, ELEC. PRIV. INFO. CTR. 1, 4 (Nov. 6, 2019), https://epic.org/wp-content/uploads/privacy/ftc/ai/epic-ai-rulemaking-petition/EPIC_FTC_HireVue_Complaint.pdf [https://perma.cc/N9EV-XBWH] [hereinafter EPIC] (see ¶ 23 of the complaint submitted to the Federal Trade Commission in the Matter of HireVue, Inc.).

[73] EPIC, *supra* note 72, at 5.

always know how the system decides."[74] This lack of transparency makes auditing algorithms exceedingly difficult and turns verification into a game of they-said, we-said.[75]

Beyond the transparency problem, assigning particular traits to facial movements and structure can be discriminatory in several ways. Eye movement tracking may be negatively affected by a candidate's medical state, such as the presence of Parkinson's, depression, or physical disabilities.[76] Individuals with Autism Spectrum Disorder may have a more difficult time making direct eye contact during an interview or may focus in ways not considered typical by the algorithm.[77] Different emotions are expressed via different facial expressions and physical movements across cultures and individuals, meaning emotion or trait recognition may be furthering cultural, racial, gender, or disability bias.[78] In response to these criticisms, and in the wake of a complaint filed with the Federal Trade Commission regarding HireVue's facial recognition practices, HireVue announced that they would halt their use of facial recognition (while continuing use of intonation and other behavior in assessments, which has many additional problems).[79]

[74] Harwell, *supra* note 72.

[75] Alex Engler, *Independent Auditors are Struggling to Hold AI Companies Accountable*, FAST CO. (Jan. 26, 2021), https://www.fastcompany.com/90597594/ai-algorithm-auditing-hirevue [https://perma.cc/8R29-HM75].

[76] Ian Taylor Logan, *For sale: Window to the Soul Eye Tracking as the Impetus for Federal Biometric Data Protection*, 123 PA. STATE L. REV. 779, 783–85 (2019).

[77] Corinne Green & Kun Guo, *Factors Contributing to Individual Differences in Facial Expression Categorisation*, COGNITION & EMOTION 1, 6 (2016).

[78] Lisa Feldman Barret et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements*, 20 ASS'N FOR PSYCH. SCI. 1, 46 (2019), https://journals.sagepub.com/doi/pdf/10.1177/1529100619832930 [https://perma.cc/9CHE-WYPX]; Abeba Birhane, *The Impossibility of Automating Ambiguity*, 27 MASS. INST. TECH. ARTIFICIAL LIFE 44, 56 (2021).

[79] Will Knight, *Job Screening Service Halts Facial Analysis of Applicants*, WIRED (Jan. 12, 2021), https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/ [https://perma.cc/S98G-5MEA]; Sheridan Wall & Hilke Schellmann, *We Tested AI Interview Tools. Here's What We Found*, MASS. INST. TECH. REV. (July 7, 2021), https://www.technologyreview.com/2021/07/07/1027916/we-tested-ai-interview-tools/ [https://perma.cc/B64Y-LFV6] (describing flaws in interview tools, including one which rated a tester at a 6 out of 9 in English competency when they completed the interview entirely speaking German, and noting that intonation is not considered a reliable indicator of personality traits).

C. Performance Monitoring

Employee monitoring has been around for some time but exploded in the shift to remote work during the COVID-19 pandemic and comes with a trove of serious privacy and human rights concerns.[80] Employee surveillance has become increasingly more invasive, both in the amount and type of information that it captures and due to many employees working out of their private spaces which may reveal much more than they intend or find acceptable.[81] Tracking systems may monitor mouse movements, websites and apps visited, typing speed, eye contact with the screen, moving in a seat, sound in a room, and more through keystroke tracking, screenshots, and audio or video recording.[82] Metrics extracted from this monitoring are

[80] *See, e.g.*, Jennifer Alsever, *Your company could be spying on you: Surveillance software use up over 50% since pandemic started*, FORTUNE (Sept. 1, 2021), https://fortune.com/2021/09/01/companies-spying-on-employees-home-surveillance-remote-work-computer/ []https://perma.cc/P4N2-W7QM; Danielle Abril & Drew Harwell, *Keystroke tracking, screenshots, and facial recognition: The boss may be watching long after the pandemic ends*, WASH. POST (Sept. 24, 2021), https://www.washingtonpost.com/technology/2021/09/24/remote-work-from-home-surveillance/ [https://perma.cc/LFT4-HHGH]; Lindsay Clark, *Workplace Surveillance Booming During Pandemic, Destroying Trust in Employers*, REGISTER (Nov. 12, 2021), https://www.theregister.com/2021/11/12/workplace_monitoring_report/ [https://perma.cc/4NCR-TTQW].

[81] *See* Jennifer Alsever, *Your Company Could Be Spying on You: Surveillance Software Use Up Over 50% Since Pandemic Started*, FORTUNE (Sept. 1, 2021), https://fortune.com/2021/09/01/companies-spying-on-employees-home-surveillance-remote-work-computer/ [https://perma.cc/GYG5-79HB]; *see* Ryan Smith, *Tracking Remote Staff*, HUM. RES. DIR. (Dec. 3, 2021), https://www.hcamag.com/au/news/general/tracking-remote-staff/318704 [https://perma.cc/M8CV-JLSC]; *see* Owen Hughes, *Remote-Working Job Surveillance is on the Rise. For Some, the Impact Could be Devastating*, ZDNET (Dec. 9, 2021), https://www.zdnet.com/article/remote-working-job-surveillance-is-on-the-rise-for-some-the-impact-could-be-devastating/ [https://perma.cc/YWL9-BBDX] ("In the pandemic, your house was everything. It was where you worshipped, it was where you worked and your school. If you drop invasive monitoring on top of all that, it's just going to be devastating to people when they don't have support and are isolated in their homes.").

[82] Sam Blum, *Employee surveillance is exploding with remote work—and could be the new norm*, HR BREW (Jan. 19, 2022), https://www.morningbrew.com/hr/stories/2022/01/19/employee-surveillance-is-exploding-with-remote-work-and-could-be-the-new-norm [https://perma.cc/VD9Q-J79X]; Jed Kim & Jesus Alvarado, *Surveillance is entering the workplace — even if your workplace is your home,* MKT. PLACE (Dec. 14, 2021), https://www.marketplace.org/shows/marketplace-tech/surveillance-is-entering-

now used for AI-powered performance reviews, employer feedback, penalties or rewards, and to determine wages or promotions.[83]

In addition to many of the concerns raised in the application and interview portions of this paper, this surveillance causes serious privacy concerns that go beyond the employee. Roommates and family members, who may be minors or vulnerable in other ways, may have conversations overheard or be watched in their homes due to the tracking technology.[84] Personal details regarding employees or others may be revealed with in-home tracking—medical information revealed through medication in the background of a video or checking test results on a tracked device, information to financial accounts through keystroke tracking and screenshots, etc.

Algorithmically-reviewed performance metrics may be tracked incorrectly, resulting in individuals being penalized for work issues entirely outside their control.[85] Constant surveillance has also eroded worker trust in employers, causing psychological harm to employees who feel dehumanized in the workplace.[86] Some have reacted by creating methods to "game"

the-workplace-even-if-your-workplace-is-your-home/ [https://perma.cc/E4VG-N7WU]; *see generally* Abril & Harwell, *supra* note 80;
Matthew Finnegan, *Rise in employee monitoring prompts calls for new rules to protect workers*, COMPUT. WORLD (Nov. 30, 2021), https://www.computerworld.com/article/3642712/rise-in-employee-monitoring-prompts-calls-for-new-rules-to-protect-workers.html [https://perma.cc/F8Q5-KV3A].

[83] *See* Zephyr Teachout, *When Big Brother is Your Boss: The Rise of Surveillance Wages*, NATION (Jan. 5, 2022), https://www.thenation.com/article/society/surveillance-wages-amazon-labor/ [https://perma.cc/S9UR-CRMY]; *see also* Aishwarya Sinha Ray, *AI in Performance Management*, PEOPLE HUM. (Nov. 23, 2021), https://www.peoplehum.com/blog/scope-of-ai-in-performance-management [https://perma.cc/4BBB-EABS]; *see also Use of Artificial Intelligence in Performance Reviews*, PROFIT CO. https://www.profit.co/blog/performance-management/use-of-artificial-intelligence-in-performance-reviews/ [https://perma.cc/MZN4-ASD3].

[84] *See generally* Abril & Harwell, *supra* note 80.

[85] Katyanna Quach, *Amazon delivery staff 'denied bonus' pay by AI cameras misjudging their driving*, REG. (Sept. 27, 2021), https://www.theregister.com/2021/09/27/in_brief_ai/ [https://perma.cc/HTF6-WGGD] (discussing how cameras in Amazon delivery vehicles penalized drivers for other cars cutting them off, turning on the radio, and glancing at side mirrors with no opportunity to discuss the matter with a human reviewer).

[86] *See* Hughes, *supra* note 81 (noting that regulators have proposed tougher laws to counteract the "pronounced negative impact" of constant employee monitoring); *see also* Jessica Vitak & Michael Zimmer, *Workers' Attitudes Toward*

these surveillance systems.[87] Concerns regarding the rampant rise of employee surveillance have led to several calls for stronger regulations to protect employees.[88]

These examples demonstrate that many purported "innovations" in the employment space fail to actually innovate, instead merely digitizing existing biased or flawed systems and, in many cases, exacerbating those flaws. By ignoring privacy, data protection, and human rights considerations in the development process and simply taking existing systems further, creators in this space were LESS innovative, failing to foresee harms or imagine what new systems could look like. Incorporating data protection considerations in the design process could possibly have allowed for much more true innovation. For example, if application systems decided to forgo black box algorithms and considered the harms of using past data to set current standards, they may have been more thoughtful in determining what lead to biased hiring practices previously and determining what actual qualities were necessary in the roles. Awareness of bias risk could have promoted increased discussion and collaboration with historically marginalized groups. If interview innovators considered barring biometric data collection from the interview process, they may have come up with systems that identified previous sources of discrimination in hiring and worked to alleviate those matters. Essentially, by grappling with the history and existing structure of systems and envisioning where those systems fail and how they can be improved through the

Increased Surveillance During and After the Covid-19 Pandemic, SOC. SCI. RSCH. COUNCIL (Sept. 16, 2021), https://items.ssrc.org/covid-19-and-the-social-sciences/covid-19-fieldnotes/workers-attitudes-toward-increased-surveillance-during-and-after-the-covid-19-pandemic/ [https://perma.cc/P2BL-DLD6].

[87] *See generally* Aaron Mak, *The Exploding Market for Devices that Help You Evade Corporate Productivity Trackers*, SLATE (Dec. 3, 2021), https://slate.com/technology/2021/12/mouse-movers-market-corporate-productivity-tracking.html [https://perma.cc/4NFP-7Q9J]; *see generally* Samantha Cole, *Workers are Using 'Mouse Movers' So They Can Use the Bathroom in Peace*, MOTHERBOARD (Dec. 8, 2021), https://www.vice.com/en/article/88gqgp/mouse-mover-jiggler-app-keep-screen-on-active [https://perma.cc/XN7Z-X7LY].

[88] Kyle Wiggers, *AI Weekly: Workplace Surveillance Algorithms Need to be Regulated Before It's Too Late*, VENTURE BEAT (Nov. 12, 2021), https://venturebea18/.t.com/2021/11/12/ai-weekly-workplace-surveillance-algorithms-need-to-be-regulated-before-its-too-late/ [https://perma.cc/589Q-9PP2]; Finnegan, *supra* note 82; Clark, *supra* note 80.

lens of data protection, companies have an opportunity to truly think outside the box for the future of the industry.

IV. LAW ENFORCEMENT

A. Predictive Policing

The adoption of technology in law enforcement is omnipresent, opaque, and significant. Two examples of rapid adoption of technology in law enforcement are predictive policing and networked private cameras with interactive law enforcement resources. As in many cases, the innovation in question was largely a maintenance of the status quo in terms of process, but with additional data collection, opaque data processing, and prediction layered in with a veneer of "data-driven," and therefore less fallible, policing.

Predictive Policing Tools are "any policing strategy or tactic that develops and uses information and advanced analysis to inform forward-thinking crime prevention"[89] (emphasis removed). Predictive policing comes in two main forms: location-based and person-based.[90] Location-based predictive policing works by identifying places of repeated property crime and trying to predict where the crimes will occur next.[91] Person-based predictive policing aims to pinpoint *who* might be committing a crime—trying to measure the risk that a given individual will commit future crimes.[92] Both are used in different jurisdictions and use past policing data as the main driver of these predictions, necessarily creating a self-fulfilling prophecy of arresting resources.[93]

After high-profile police murders and subsequent protests in the 2010s caused some within law enforcement to publicly recognize the racially discriminatory history of policing, tools

[89] CRAIG D. UCHIDA, A NATIONAL DISCUSSION ON PREDICTIVE POLICING: DEFINING OUR TERMS AND MAPPING SUCCESSFUL IMPLEMENTATION STRATEGIES, NAT'L INST. OF JUST. 1 (2010), https://www.ojp.gov/pdffiles1/nij/grants/230404.pdf [https://perma.cc/4ZGW-BSPW] (quoting the "working definition" provided by John Morgan, Ph.D.).

[90] ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 35, 62 (2017).

[91] *Id.* at 62.

[92] *Id.* at 35.

[93] *See id.* at 16.

that made it appear like there would be a meaningful shift in policing from subjective racist police actions to objective "data-driven" were particularly appealing.[94] The National Institute of Justice (NIJ) held its first Predictive Policing Symposium in 2009, and began awarding grants to police departments to adopt predictive policing systems that year under a grant program entitled "Smart Policing Initiative," now named "Strategies for Policing Innovation."[95] Since then, systematic adoption of predictive policing tools has been funded by grants from the Department of Justice totaling over $68,000,000.[96]

Despite widespread adoption of predictive policing, it has become clear through studies that it is harmful, racist, and self-perpetuating.[97] As data on predictive policing has become clear, through significant empirical studies by government auditors[98] and independent third parties,[99] several jurisdictions have

[94] *Id.* at 28–29 ("Out of the tension of black lives' frustration with police officers and blue lives' frustration with police administration, the lure of technology to add objectivity of policing and to do more with less began to grow. 'Smart policing,' 'intelligence-led policing,' and 'data-driven policing' became catchphrases for the future.").

[95] *See generally* Symposium, *Predictive Policing Symposiums,* NCJ 248891 NAT'L INST. JUST. (2010), https://nij.ojp.gov/library/publications/predictive-policing-symposium-june-2-3-2010 [https://perma.cc/8CMZ-KKFG]; *Strategies for Policing Innovation (SPI)*, BUREAU OF JUST. ASSISTANCE U.S. DEP'T OF JUST., https://bja.ojp.gov/taxonomy/term/87751#filter- [https://perma.cc/7MJU-MMQY] (last visited Mar. 7, 2022).

[96] *See generally Awards*, BUREAU OF JUST. ASSISTANCE U.S. DEP'T OF JUST., https://bja.ojp.gov/funding/awards/list?field_award_status_value=All&state=All&field_funding_type_value=All&fiscal_year=&combine_awards=smart+policing&awardee=&city=#awards-awards-list-block-96p-ly-hjdt28vdn [https://perma.cc/JNX6-RFBE] (last visited Mar. 7, 2022); *EPIC v. DOJ (Criminal Justice Algorithms),* ELEC. PRIV. INFO. CTR. https://epic.org/foia/doj/criminal-justice-algorithms/ [https://perma.cc/6J2L-BSW8].

[97] *See generally* Chris Gilliard, *Crime Prediction Keeps Society Stuck in the Past*, WIRED (Jan. 2, 2022), https://www.wired.com/story/crime-prediction-racist-history/ [https://perma.cc/W25E-RCQ4].

[98] *See* Charlie Beck, *Advisory Concerning the Chicago Police Departments Predictive Risk Models*, CITY OF CHI. OFF. INSPECTOR GEN. 1, 5 (Jan. 23, 2020), https://igchicago.org/wp-content/uploads/2020/01/OIG-Advisory-Concerning-CPDs-Predictive-Risk-Models-.pdf [https://perma.cc/4JQE-9BMP].

[99] *See, e.g.*, Annie Gilbertson, *Data-Informed Predictive Policing Was Heralded As Less Biased. Is it?*, MARKUP (Aug. 20, 2020) https://themarkup.org/ask-the-markup/2020/08/20/does-predictive-police-technology-contribute-to-bias [https://perma.cc/6L5X-HYZC] (synthesizing the findings of multiple independent studies about the discriminatory effect of predictive policing); Dhruv Mehrotra, Surya Mattu, Annie Gilbertson, & Aaron Sankin, *How we Determined Predictive Policing Software Disproportionately Targeted Low-Income, Black, and Latino*

canceled contracts with predictive policing developers or banned the use of those tools moving forward.[100]

Although most jurisdictions have not discontinued use, it shows that innovation isn't the same to everyone—and doesn't necessarily improve equity or preserve rights in its unaltered state. In this case, for jurisdictions that adopted predictive policing to improve after recognizing racialized harm, the innovation was counterproductive.

Particularly with government agencies adopting commercial systems in the most sensitive contexts, Ruha Benjamin's Race After Technology succinctly articulates the unique risks:

> Consider that machine learning systems, in particular, allow officials to outsource decisions that are or should be the purview of democratic oversight. Even when public agencies are employing such systems, private companies are the ones developing them, thereby acting like political entities but with **none of the checks and balances**.
>
> They are, in the eyes of one observer, governing without a mandate, which means that people whose lives are being shaped in ever-increasingly automated ways have very little say in how they are governed[101] (emphasis added).

These predictive policing tools, promising more "objective" policing, simply don't deliver on that promise of innovation. They are accepting, encoding, and perpetuating the status quo, and

Neighborhoods, GIZMODO (Dec. 2, 2021), https://gizmodo.com/how-we-determined-predictive-policing-software-dispropo-1848139456 [https://perma.cc/DTU4-ZZQF] ("Overall, we found that PredPol's algorithm relentlessly targeted the Census block groups in each jurisdiction that were the most heavily populated by people of color and the poor, particularly those containing public and subsidized housing. The algorithm generated far fewer predictions for block groups with more White residents.").

[100] WENDY LEE, JUMANA MUSA, & MICHAEL PINARD, *Garbage In, Gospel Out: How Data-Driven Policing Technologies Entrench Historic Racism and 'Tech-wash' Bias in the Criminal Legal System*, NAT. ASS'N CRIMINAL DEF. LAWYERS 1, 72 (Sept. 2021), https://www.nacdl.org/getattachment/eb6a04b2-4887-4a46-a708-dbdaade82125/garbage-in-gospel-out-how-data-driven-policing-technologies-entrench-historic-racism-and-tech-wash-bias-in-the-criminal-legal-system-09142021.pdf [https://perma.cc/897J-63QY].

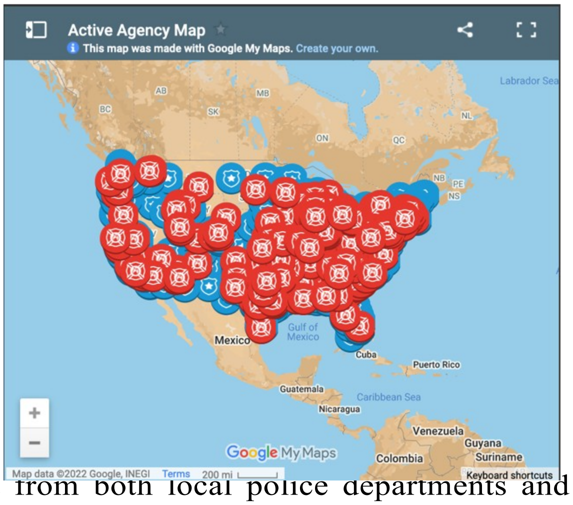
[101] RUHA BENJAMIN, RACE AFTER TECHNOLOGY: ABOLITIONIST TOOLS FOR THE NEW JIM CODE 36 (2019).

should be forced to consider what innovation means for a public purpose rather than purchasing a product labeled as innovation.

It's unclear if tools made in this context can be tinkered with to be truly innovative while protecting data security, privacy, and civil rights. More innovative techniques with the developed technology can help jurisdictions pinpoint where their police are targeting, and where they can better offer social services and support to those they are criminalizing.

B. Networked Public-Facing Cameras Connected to Law Enforcement

The popularity of networked private cameras with interactive law enforcement resources demonstrates the problem of products that implicate residents and businesses of a community. While law enforcement adoption illustrates a blind push for innovation at the cost of equal treatment. Prominent examples of networked public-facing cameras connected to law enforcement are Ring (owned by Amazon) and SimpliSafe. Both are consumer-marketed surveillance tools but are networked together and in many cases connected directly to police departments.



The marketing materials of both products offer persistent connected surveillance throughout an individual's home and devices and the surveillance is frequently connected directly to local police. This is the result of a significant PR effort from both local police departments and Ring.[102] There are now over 2,000 known police departments

[102] 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/ [https://perma.cc/2QH8-BQWS]; *Alarm*

that are connected to cameras in individual homes, yielding new levels of surveillance laundered through preying on an individual's sense of safety, rather than a public function that requires more process and approval.[103]

Although Ring and SimpliSafe tout this additional surveillance as inherently innovative, and have been validated with awards about innovation, this again allows private entities to influence and replace. Beyond the issues with police, this quick sale of surveillance as innovation has left some vulnerable in their own home, and more importantly, left every person passing by another person's doorbell vulnerable to potential security vulnerabilities allowing *anyone* (in addition to police departments) to view camera feeds.[104] Beyond these clear violations of privacy and autonomy, there are also persistent concerns about chilling effects of networked surveillance, and how the corresponding community app "Neighbors" labels people as thieves or suspicious.[105] It doesn't allow for practical consent or notice about what cameras are seeing you and who can access them, let alone what software runs on them.

Monitoring Features, SIMPLISAFE, https://simplisafe.com/features-alarm-monitoring [https://perma.cc/3FUQ-F37S] (last visited Mar. 7, 2022).

[103] Kim Lyons, *Amazon's Ring now reportedly partners with more than 2,000 US police and fire departments*, VERGE (Jan. 31, 2021), https://www.theverge.com/2021/1/31/22258856/amazon-ring-partners-police-fire-security-privacy-cameras [https://perma.cc/LSH7-48XA].

[104] Ken Colburn, *Ring video doorbell: Could this home security system be vulnerable to breaches?*, AZCENTRAL. (Nov. 11, 2019), https://www.azcentral.com/story/money/business/tech/2019/11/11/why-ring-video-doorbell-had-recent-safety-concerns/2532137001/ [https://perma.cc/4R8Y-KQ8M]; Drew Harwell, *Massive camera hack exposes the growing reach and intimacy of American surveillance*, WASH. POST (Mar. 10, 2021), https://www.washingtonpost.com/technology/2021/03/10/verkada-hack-surveillance-risk/ [https://perma.cc/W669-3NG5] ("With a single breach, those scenes — and glimpses from more than 149,000 security cameras — were suddenly revealed to hackers, who had used high-level log-in credentials to access and plunder Verkada's vast camera network. A hacker shared some of the materials with The Washington Post to spotlight the security threat of widespread surveillance technologies that subject the public to near-constant watch. The cache includes real-world images and videos as well as the company's voluminous client list, which names more than 24,000 organizations across a vast cross-section of American life, including schools, offices, gyms, banks, health clinics and county jails.").

[105] *See* Grace Beak, *Are video doorbells and neighborhood watch apps generating more fear than security?*, CBS NEWS (Feb. 24, 2020), https://www.cbsnews.com/news/neighborhood-watch-apps-ring-doorbells-racial-profiling-2-0-cbsn-originals-documentary/ [https://perma.cc/YH6R-DUBQ].

The current use of these tools does not comport with the innovation they sell. There should be strict controls on (1) the radius of vision into public spaces for the cameras; (2) the sharing of data with other people through Neighbors or other social media; (3) the sharing of data with law enforcement; and (4) the use of additional video analysis tools like facial recognition, emotion recognition, and more.

Both predictive policing systems and tools like Ring or SimpliSafe encode existing systems and give the cover of innovation while maintaining the status quo and increasing needless surveillance and data collection. Reports have shown that neither helps fight or reduce crime,[106] which is supposed to justify the persistent surveillance, criminalization of innocent behavior, and increased police presence that these tools bring. Particularly in the criminal legal cycle, innovation examining existing systems of law enforcement, including impact on marginalized communities, and rethinking these systems to prioritize data protection would be revolutionary.

CONCLUSION

The current understanding of data protection and innovation battling one another has been detrimental both to the state of data protection and to facilitating true innovation. Examples of "innovations" in education, employment, and law enforcement that prioritize the new over data protection considerations are plentiful and have been described within this paper. However, by modifying this framework and approaching data protection as a vital component of innovation, we can both provide true data protection for consumers and facilitate innovation that moves beyond merely shifting existing systems to new formats and takes on the challenge of rethinking historic systems.

[106] 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 [https://perma.cc/P3UG-PH9X].