NOTE

The Modern Lie Detector: AI-Powered Affect Screening and the Employee Polygraph Protection Act (EPPA)

COURTNEY HINKLE*

Predictive algorithms are increasingly being used to screen and sort the modern workforce. The delegation of hiring decisions to AI-powered software systems, however, will have a profound impact on the privacy of individuals. This Note builds on the foundational work of legal scholars studying the growing trend of algorithmic decisionmaking in recruiting and hiring practices. However, this Note will differ from their analysis in critical ways. Although this issue has primarily been studied through the lens of federal antidiscrimination law and for the potential for algorithmic bias, this Note will explore how federal privacy law, namely the oft-forgotten Employee Polygraph Protection Act (EPPA), offers a more robust regulatory framework.

This Note will specifically analyze the use of video-interviewing screens that rely upon affect-recognition technology, which analyze an applicant's voice tonality, word choice, and facial movements. The current vogue for AI-powered affect screening is, however, reminiscent of an early period of employee screening tests: the lie detector. Congress prohibited the use of lie detectors by employers in the 1980s. By embracing old analytical shortcuts, which purport to correlate psychophysiological responses with desired character traits, namely honesty, this growing industry is operating in violation of federal law. This Note will also critique the limits of antidiscrimination law, data protection law, and consumer protection law to address the scope of privacy harms posed by these screens.

TABLE OF CONTENTS

* Georgetown University Law Center, J.D. expected 2021; The University of the South, B.A. 2012. I am grateful to Professor Julie E. Cohen for her invaluable guidance and support in developing the paper that became this Note. I also want to acknowledge Jenny R. Yang and Professor Danielle K. Citron for their thoughtful insights. Finally, I want to thank Orion de Nevers, Anna Stacey, Maggie O'Leary, and all the *Georgetown Law Journal* editors and staff for their helpful contributions.

INTRODUCTION

Predictive algorithms are increasingly being used to screen and sort the modern workforce.[1] In the brave new world of algorithmic hiring, artificial intelligence and machine learning tools are used to determine an applicant's overall fit and likelihood of success for a particular role.[2] Some of these new tools hold the

1. Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857, 857, 860 (2017); Claire Cain Miller, *Can an Algorithm Hire Better Than a Human?*, N.Y. TIMES (June 25, 2015), https://www.nytimes.com/2015/06/26/upshot/can-an-algorithm-hire-better-than-a-human.html.

2. *See* Kim, *supra* note 1, at 860. The term "artificial intelligence" (AI) is used to define various computational techniques for automating intelligent behavior, which are often used to predict future outcomes based on analysis of past data; however, "[t]here is no single definition of AI that is

promise—and the peril—of translating the practice of using paper-and-pencil integrity tests into lines of code.[3] For example, video-interviewing screens that incorporate affect- or emotion-recognition technology—which purports to surface desirable character traits hidden in each applicant's subconscious by studying voice tonality, word choice, and facial movements—are increasingly among the most popular digital hiring tools on the market.[4] Proponents of the technology

universally accepted by practitioners." *See* COMM. ON TECH., EXEC. OFFICE OF THE PRESIDENT, PREPARING FOR THE FUTURE OF ARTIFICIAL INTELLIGENCE 6–7 (2016), https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf [https://perma.cc/YHF3-FWH6] (providing examples of various definitions offered by experts). These techniques include machine learning, deep learning, learning algorithms, and many other terms. *See id.* at 8–9. For a more in-depth explanation, see Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 674 n.10 (2016), which defines an "algorithm" as "a formally specified sequence of logical operations that provides step-by-step instructions for computers to act on data and thus automate decisions." *See also* Bernard Marr, *What Is the Difference Between Artificial Intelligence and Machine Learning?*, FORBES (Dec. 6, 2016, 2:24 AM), https://www.forbes.com/sites/bernardmarr/2016/12/06/what-is-the-difference-between-artificial-intelligence-and-machine-learning/?sh=30f8a05e2742 (defining AI as "the broader concept of machines being able to carry out tasks in a way that we would consider 'smart,'" whereas machine learning is "a current application of AI based around the idea that we should really just be able to give machines access to data and let them learn for themselves"). Notably, a deep dive into the differences between the various types of AI is not necessary for the purpose of this Note.

3. Integrity tests have been used "for decades to measure candidates' attitudes toward theft, dishonesty, absenteeism, violence, drug use, alcohol abuse and other counterproductive behaviors." Bill Roberts, *Your Cheating Heart*, SOC'Y FOR HUM. RESOURCE MGMT. (June 1, 2011), https://www.shrm.org/hr-today/news/hr-magazine/pages/0611roberts.aspx [https://perma.cc/CYA4-QDF5] (providing a history of integrity and personality testing by employers). Written, paper-and-pencil honesty tests became an increasingly popular tool for employers beginning in the late 1980s and early 1990s as a replacement for the previously preferred testing tool (the polygraph). Katrin U. Byford, Comment, *The Quest for the Honest Worker: A Proposal for Regulation of Integrity Testing*, 49 SMU L. REV. 329, 331 (1996). The tests consisted of multiple-choice questions that would ask "overt" honesty questions ("How often do you tell the truth?") or "veiled purpose" or "personality-based" questions ("True or False: I like to take chances."). *Id.* at 332–33.

4. *See* Lilah Burke, *Your Interview with AI*, INSIDE HIGHER ED (Nov. 4, 2019), https://www.insidehighered.com/news/2019/11/04/ai-assessed-job-interviewing-grows-colleges-try-prepare-students [https://perma.cc/SP68-D9AT]; *Businesses Turning to AI for Job Interviews*, CBS NEWS (Feb. 20, 2020), https://www.cbsnews.com/video/businesses-turning-to-ai-for-job-interviews/; Hilke Schellmann, *How Job Interviews Will Transform in the Next Decade*, WALL ST. J. (Jan. 7, 2020, 9:58 AM), https://www.wsj.com/articles/how-job-interviews-will-transform-in-the-next-decade-11578409136; Jessica Stillman, *Delta and Dozens of Other Companies Are Using AI and Face Scanning to Decide Whom to Hire. Critics Call It "Digital Snake Oil,"* INC. (Oct. 30, 2019), https://www.inc.com/jessica-stillman/delta-ikea-goldman-sachs-are-using-ai-face-scanning-to-decide-whom-to-hire-critics-call-it-digital-snake-oil.html.

Algorithms that use affect- and emotion-recognition technology—a subset of facial-recognition technology—are designed to "'read' our inner emotions by interpreting physiological data such as the micro-expressions on our face," and the information is used to make "sensitive determinations about who is . . . a 'good worker.'" KATE CRAWFORD, ROEL DOBBE, THEODORA DRYER, GENEVIEVE FRIED, BEN GREEN, ELIZABETH KAZIUNAS, AMBA KAK, VAROON MATHUR, ERIN MCELROY, ANDREA NILL SÁNCHEZ, DEBORAH RAJI, JOY LISI RANKIN, RASHIDA RICHARDSON, JASON SCHULTZ, SARAH MYERS WEST & MEREDITH WHITTAKER, AI NOW INST., AI NOW 2019 REPORT 12 (2019), https://ainowinstitute.org/AI_Now_2019_Report.pdf [https://perma.cc/5NP9-YGSQ].

Notably, in January 2021, HireVue—one of the most well-known vendors offering affect-recognition video screens—announced it would be suspending the use of its software to analyze applicants' facial expressions to discern character traits. Will Knight, *Job Screening Service Halts Facial Analysis of*

tout its ability to help employers more effectively and efficiently identify qualified candidates while mitigating the subjective bias of human decisionmakers.

The delegation of hiring decisions to these AI-powered software systems, however, will have a profound impact on the privacy of individuals. Moreover, the efficacy of the technology remains sharply disputed. This Note will build on the foundational work of legal scholars studying the use of algorithmic decisionmaking in employment but will differ from their analysis in critical ways. The existing body of scholarship has primarily been studied through the lens of federal antidiscrimination law to discern the potential for algorithmic bias to disproportionately exclude members of a protected category.[5] In contrast, this Note will explore how federal privacy law, namely the oft-forgotten Employee Polygraph Protection Act (EPPA),[6] offers a more robust regulatory framework to address the scope of harm caused by algorithmic hiring, specifically affect-recognition screens.

Part I will explore the rising popularity of predictive hiring and, in particular, of video-interviewing screens, analyzing both the character traits tested for by these algorithms and the limits of the current legal frameworks proposed to regulate them. Part II will consider the historical debate over the permissible uses of lie detectors by employers and will discuss Congress's motivation in the 1980s to broadly prohibit the technology under the EPPA. Part III will analyze the shift to written integrity tests following the adoption of the EPPA. In the ensuing decades, as the world moved online, outdated pen-and-pencil tests were rewritten for digital platforms. This Part will detail how developers of the new screens resorted

---

Applicants, WIRED (Jan. 12, 2021, 8:00 AM), https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants/. HireVue's Chief Executive Officer Kevin Parker defended the technology, citing a 2019 audit that showed its software does not harbor any bias. *See id.* Nevertheless, Parker pointed to "public outcry" over the use of facial analysis as the reason for halting the service. *Id.* This decision is surely viewed as a win by privacy and technology advocates who have long criticized the use of the technology. *See* CRAWFORD ET AL., *supra*, at 12, 17; Knight, *supra*. The company will continue, however, to conduct automated voice analysis, considering word choice, intonation, and behavior of applicants, to inform hiring decisions, which experts believe still poses privacy and bias concerns. *See* Knight, *supra*.

5. A sizable body of legal scholarship has emerged to address the discrimination concerns posed by algorithmic hiring. *See generally* Ifeoma Ajunwa, *An Auditing Imperative for Automated Hiring Systems*, 34 HARV. J.L. & TECH. (forthcoming 2021) [hereinafter Ajunwa, *An Auditing Imperative*]; Ifeoma Ajunwa, *The Paradox of Automation as Anti-Bias Intervention*, 41 CARDOZO L. REV. 1671 (2020) [hereinafter Ajunwa, *The Paradox of Automation*]; Barocas & Selbst, *supra* note 2; Stephanie Bornstein, *Antidiscriminatory Algorithms*, 70 ALA. L. REV. 519 (2018); Deborah Hellman, *Measuring Algorithmic Fairness*, 106 VA. L. REV. 811 (2020); Pauline T. Kim, *Auditing Algorithms for Discrimination*, 166 U. PA. L. REV. ONLINE 189 (2017); Kim, *supra* note 1; Pauline T. Kim & Sharion Scott, *Discrimination in Online Employment Recruiting*, 63 ST. LOUIS U. L.J. 93 (2018); Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson & Harlan Yu, *Accountable Algorithms*, 165 U. PA. L. REV. 633 (2017); Anya E. R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 IOWA L. REV. 1257 (2020); SARAH MYERS WEST, MEREDITH WHITTAKER & KATE CRAWFORD, AI NOW INST., DISCRIMINATING SYSTEMS: GENDER, RACE, AND POWER IN AI (2019), https://ainowinstitute.org/discriminatingsystems.pdf [https://perma.cc/Q7DP-K9MK].

6. Employee Polygraph Protection Act of 1988, Pub. L. No. 100-347, 102 Stat. 646 (codified as amended in scattered sections of 29 U.S.C.).

back to old analytical shortcuts: attempting to correlate psychophysiological responses with desired character traits.[7] Ultimately, this Note will argue that employers have forgotten their own history. By renewing their reliance on nonverbal indicators, employers and vendors using affect-recognition video-interviewing screens are triggering the same concerns underlying the EPPA, and their continued use violates the statute's express prohibitions.

I. THE CHALLENGE OF ALGORITHMIC HIRING SCREENS

For many workers, an AI-powered software system will conduct their next job interview, particularly as remote work and social distancing policies remain in place during the COVID-19 pandemic.[8] This growing deference to predictive algorithms to determine who advances to the next stage of hiring, or who is rejected, is fundamentally reshaping the recruitment and hiring landscape with profound social consequences. [9] This Part briefly traces how recruiting and hiring practices have evolved over the past two decades to keep pace with technology. Although many of these changes have been embraced by employers and job seekers alike, skeptics have raised concerns that these automated systems "introduce bias, lack accountability and transparency," threaten individual privacy and autonomy, and "aren't guaranteed to be accurate."[10] The stakes could not be higher. "Hiring decisions are among the most consequential" for any individual: determining where someone will live, how much they will earn, and what their career trajectory will be.[11] In effect, these algorithms are the modern "gatekeepers to economic opportunity."[12] This Part will argue the prevailing regulatory approaches to guard against these harms—namely antidiscrimination law, consumer protection law, and data protection law—leave much to be desired.

---

7. Psychophysiology is the "study of the interrelationship between mind and body." M.E. Dawson & A. Shell, *Psychophysiology*, *in* 18 INTERNATIONAL ENCYCLOPEDIA OF THE SOCIAL & BEHAVIORAL SCIENCES 12448, 12448 (Neil J. Smelser & Paul B. Baltes eds., 2001). Typical psychophysiological measures include heart rate, palmar sweating, and skeletal muscle activity, which are used to index long-lasting states, such as emotion. *See id.* at 12448–49.

8. *See* Scott Steinberg, *Coronavirus Hiring: How Recruiters Are Selecting and Interviewing Job Candidates During the Pandemic*, CNBC (May 24, 2020, 11:17 AM), https://www.cnbc.com/2020/05/24/how-recruiters-select-and-interview-job-candidates-amid-coronavirus.html [https://perma.cc/U87F-68RN]; *cf.* Indranil Sarkar, *Bored at Home-Coronavirus Helps Headhunters Locate Candidates, Delays Deals*, REUTERS (Mar. 10, 2020, 11:46 AM), https://www.reuters.com/article/us-health-coronavirus-recruiters/bored-at-home-coronavirus-helps-headhunters-locate-candidates-delays-deals-idUSKBN20X2AF [https://perma.cc/5W7L-9DWT] (discussing the increase in video interviews).

9. Jenny R. Yang & Bapuchandra Kotapati, *Artificial Intelligence and Its Impact on the Future of Employment Equity*, URB. INST.: NEXT50 (June 13, 2019), https://next50.urban.org/article/artificial-intelligence-and-its-impact-future-employment-equity [https://perma.cc/HWN5-LGPT].

10. *See* Rebecca Heilweil, *Artificial Intelligence Will Help Determine if You Get Your Next Job*, VOX: RECODE (Dec. 12, 2019, 8:00 AM), https://www.vox.com/recode/2019/12/12/20993665/artificial-intelligence-ai-job-screen [https://perma.cc/A57N-PCNK].

11. Manish Raghavan, Solon Barocas, Jon Kleinberg & Karen Levy, Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices 3 (Dec. 13, 2019) (unpublished manuscript), https://arxiv.org/pdf/1906.09208.pdf [https://perma.cc/R35M-YKPU].

12. Yang & Kotapati, *supra* note 9.

A. FROM JOB BOARDS TO ARTIFICIAL INTELLIGENCE (AI)

Modern job recruitment and hiring practices have changed dramatically with the growth of the Internet.[13] Starting in the 1990s, traditional media outlets, such as the classifieds section of a local newspaper, were replaced by online job boards, such as Monster.com or Craigslist.[14] The growing use of search engines and pay-per-click advertising for digital recruitment quickly followed suit.[15] By the end of the decade, employers had moved to online applications, easing the application process but also dramatically increasing the number of applicants, many of whom were unqualified or ill-suited for the role.[16] By the mid-2000s, new platform companies, such as LinkedIn and Indeed, emerged to provide employers with increasingly sophisticated digital targeting tools to grow the pool of *qualified* applicants.[17] To survive the deluge of applications, however, employers were forced to develop new methods of screening and tracking applicants.[18] Today, many of the tasks typically performed by human resource (HR) departments, such as résumé review or screening interviews, have been outsourced to automated software programs or third-party vendors.[19] In addition, many employers have embraced the benefits of big data analytics at all levels of talent management, evangelized by the promise of greater data collection and AI-powered

13. *See* MIRANDA BOGEN & AARON RIEKE, UPTURN, HELP WANTED: AN EXAMINATION OF HIRING ALGORITHMS, EQUITY, AND BIAS 5 (2018), https://www.upturn.org/reports/2018/hiring-algorithms/ [https://perma.cc/F8BK-Y52R].

14. *See id.*

15. *See id.*

16. *See id.*

17. *See id.*; Michael Overell, *The History of Innovation in Recruitment Technology and Services*, TECHCRUNCH (Oct. 29, 2016, 3:00 PM), https://techcrunch.com/2016/10/29/the-history-of-innovation-in-recruitment-technology-and-services/ [https://perma.cc/TUK2-XBVQ].

18. BOGEN & RIEKE, *supra* note 13.

19. *See The Future of Work: Protecting Workers' Civil Rights in the Digital Age: Hearing Before the Subcomm. on Civil Rights & Human Servs. of the H. Comm. on Educ. & Labor*, 116th Cong. 6 (2020) [hereinafter *The Future of Work*, 116th Cong. 6] (testimony of Peter Romer-Friedman, Principal, Gupta Wessler PLLC); *cf.* BOGEN & RIEKE, *supra* note 13, at 5–6 (providing a chronological history of the advent of automated hiring technologies in recruitment and hiring). At a macrolevel, the growth in HR vendors illustrates the departure from an internal promotion and lateral transfer hiring model within large corporations that predominated in the mid-twentieth century. *See generally* WILLIAM H. WHYTE, THE ORGANIZATION MAN (Univ. of Pa. Press 2002) (1956) (detailing the relationship between an individual and "The Organization" in the 1950s as one defined by corporate loyalty in return for job security, whereby "The Organization Man" is the archetype embracing group identity over individual identity). In contrast, modern recruiting and hiring functions have been outsourced to third parties, and open positions are increasingly being filled by external hires as the trend towards "job-hopping" continues, especially with a growing share of millennials in the workforce. *See* Roy Maurer, *Employee Referrals Remain Top Source for Hires*, SOC'Y FOR HUM. RESOURCE MGMT. (June 23, 2017), https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/employee-referrals-remains-top-source-hires.aspx [https://perma.cc/YMH7-V8FY]. In 2016, external sources produced the majority of interviews (sixty-two percent), but internal sources still produced fifty-two percent of hires, compared to forty-eight percent from external sources. *Id.*

analysis to fill persistent knowledge gaps in hiring, performance, retention, and workforce planning.[20]

Employers have readily embraced these digital tools to solve two long-standing challenges in talent acquisition. First, the notoriously subjective nature of employee hiring, which increases the risk of biased and discriminatory outcomes, and second, the protracted length in "time-to-hire," or the time it takes to complete the hiring life cycle from application to an accepted offer. To state the obvious: employers want to make good hires. A recent survey of corporate leadership revealed the number one internal priority for companies is "attracting and retaining top talent."[21] And with each hiring decision, employers aim to maximize the quality of the candidate, while avoiding "toxic" hires, such as individuals likely to engage in workplace theft or harassment.[22]

However, hiring is—and always has been—hard.[23] As one writer explained, "[h]iring is hard for the same reason that dating is hard: [b]oth sides are in the dark."[24] In other words, hiring is often "expensive [and] time-consuming . . . because the hirer doesn't know what workers are the right fit, and the worker don't [sic] know what hirers are the right fit."[25] The hope for a breakthrough solution to this problem continues to be elusive in many respects. Much ink has been spilled by business leaders, social scientists, and workplace psychologists over how to make good hiring decisions or determine who would be a "good fit." But

---

20. *See* Forbes Human Res. Council, *Big Data, Better Hiring: 10 Ways HR Can Use Analytics to Find the Perfect Employee*, FORBES (Jan. 18, 2019, 9:00 AM), https://www.forbes.com/sites/forbeshumanresourcescouncil/2019/01/18/big-data-better-hiring-10-ways-hr-can-use-analytics-to-find-the-perfect-employee/?sh=c5b1064712b8*; see also* GRACE CHENSOFF, CATHERINE COPPINGER, POOJA CHHABRIA, CANDICE CHENG, ALVIN KAN & HUILING CHEONG, LINKEDIN TALENT SOLUTIONS, THE RISE OF ANALYTICS IN HR: THE ERA OF TALENT INTELLIGENCE IS HERE 23–24 (2019), https://business.linkedin.com/content/dam/me/business/en-us/talent-solutions/talent-intelligence/workforce/pdfs/Final_v2_NAMER_Rise-of-Analytics-Report.pdf [https://perma.cc/9BYK-J9SQ] (highlighting a case study where data analytics were used to understand why a company was losing talent and to identify internal mobility as key to retention).

21. Press Release, The Conference Bd., Survey: Business Leaders Start 2020 with Lingering Concerns About Talent Shortages & Recession Risk (Jan. 2, 2020), https://perma.cc/X9PL-GBJ6. The Conference Board survey, conducted annually since 1999, captured the sentiments of nearly 750 CEOs and nearly 800 other C-Suite executives, primarily from Europe, Latin America, Asia, and the United States. *Id.*

22. *See* BOGEN & RIEKE, *supra* note 13, at 6. One toxic employee per team of twenty individuals is estimated to cost an employer $12,800 in turnover and decreased productivity. Melody Wilding, *How to Spot Toxic Employees Before You Hire Them*, QUARTZ (Jan. 5, 2018), https://qz.com/work/1172945/how-to-spot-toxic-employees-beforeyou-hire-them. However, spotting a toxic employee and weeding them out during the hiring process can be tricky. *Id.* A possible strategy to avoid toxic hires, especially if correcting for loss prevention or theft, is to screen "for conscientious candidates who conduct themselves with integrity." Kiera Abbamonte, *How to Put Together a Loss Prevention Plan for Your Store*, SHOPIFY: RETAIL BLOG (Apr. 19, 2018), https://www.shopify.com/retail/retail-loss-prevention [https://perma.cc/536H-EV7Y].

23. Derek Thompson, *The Science of Smart Hiring*, ATLANTIC (Apr. 10, 2016), https://www.theatlantic.com/business/archive/2016/04/the-science-of-smart-hiring/477561/ (discussing that hiring is hard due to bilateral asymmetric information challenges and difficulties identifying metrics that predict employee success).

24. *Id.*

25. *Id.*

there is "remarkably little consensus" on exactly what factors are the best predictors of success, especially when taking into consideration the varied qualifications and skills across job categories.[26] Moreover, people are highly complex, and successfully predicting fit or performance is determined not only by the individual person, but also by how they interact in other "human systems" (or workplaces).[27] This synergy, therefore, further complicates the reliability of any one factor being determinative of a good hiring outcome.

Another shortcoming of traditional methods abounds: hiring decisions tend to rely on what information is most readily available.[28] Unsurprisingly, the most ubiquitous screening tool is the résumé. But research has shown the information housed on a typical résumé is not necessarily the most predictive indicator of success.[29] In 1998, a comprehensive study analyzing over eighty-five years of research in personnel selection found the top résumé boosts—including years of experience, education, and interests—had little to no correlation to later job performance.[30] This is because a résumé tends to focus not on relevant job skills but, rather, on a candidate's claim to have experience doing something that "looks like" the prospective role.[31] In the absence of stronger evaluative criteria, subjective perceptions of a candidate tend to command outsized importance in the decisionmaking process.[32] The tendency to prefer similar past experiences extends to preferencing candidates of a "similar race, class, gender, and other traits" of the hiring manager.[33] Research shows that not only is the "look alike" method of hiring ineffective at predicting performance, but it also compounds and perpetuates

---

26. *See* Peter Cappelli, *Your Approach to Hiring Is All Wrong*, HARV. BUS. REV. (May–June 2019), https://hbr.org/2019/05/recruiting.

27. Thompson, *supra* note 23.

28. *See id.* ("[A] fundamental challenge in hiring [is] identifying the metrics that actually predict employee success, rather than relying on the most available pieces of information.").

29. *See* Alison Beard, *Experience Doesn't Predict a New Hire's Success*, HARV. BUS. REV. (Sept.–Oct. 2019), https://hbr.org/2019/09/experience-doesnt-predict-a-new-hires-success; Pavel Krapivin, *Why Past Experience Is a Lousy Predictor of Job Success*, FORBES (July 31, 2019, 5:19 AM), https://www.forbes.com/sites/pavelkrapivin/2019/07/31/why-past-experience-is-a-lousy-predictor-of-job-success/#541a35fe3353; Thompson, *supra* note 23.

30. *See* Frank L. Schmidt & John E. Hunter, *The Validity and Utility of Selection Methods in Personnel Psychology: Practical and Theoretical Implications of 85 Years of Research Findings*, 124 PSYCHOL. BULL. 262, 265, 272 (1998); *see also* Stacie Garland, *Design a Recruitment Process to Predict Job Performance*, VERVOE (July 8, 2020), https://vervoe.com/predict-job-performance/ [https://perma.cc/W4FE-BMSG] ("Eighty-five years of research prove that résumés—summaries of a person's work experience and education—are entirely ineffective at predicting job performance."); Omer Molad, *An Embarrassment of Riches: Too Many Job Applicants for Every Role*, VERVOE (Apr. 21, 2020), https://vervoe.com/too-many-applicants-for-every-job/ [https://perma.cc/A2WJ-3CZ7] (observing that the traditional résumé screening process is "ineffective in predicting a candidate's performance").

31. Cassidy Leventhal, Opinion, *Resumes Are a Terrible Way to Hire People*, BLOOMBERGQUINT (Feb. 24, 2020, 9:12 PM), https://www.bloombergquint.com/gadfly/resumes-are-a-terrible-way-to-hire-people.

32. *See* Drake Baer, *If You Want to Get Hired, Act Like Your Potential Boss*, BUS. INSIDER (May 29, 2014, 2:16 PM), https://www.businessinsider.com/managers-hire-people-who-remind-them-of-themselves-2014-5.

33. Leventhal, *supra* note 31; *see also* Sachin Waikar, *A Tilted Playing Field*, KELLOGG INSIGHT (May 1, 2015), https://insight.kellogg.northwestern.edu/article/a-tilted-playing-field [https://perma.cc/

existing inequities in the workplace.[34] At the same time, the high volume of online applicants has made screening for top talent an increasingly expensive and time-intensive process.[35] According to the Society for Human Resource Management, an employer in the United States spends on average $4,425 per new hire ("cost-per-hire").[36] The average "[t]ime-to-fill" an open position is estimated to be between five and six weeks.[37] The confluence of these factors has placed acute pressure on employers to identify shortcuts to optimize their hiring practices.

For many employers, AI and big data analytics are believed to be the long-awaited solution.[38] An employer is able to collect and synthesize highly granular personal data not only on prospective job applicants, but also on their current workforce.[39] Armed with a seemingly deeper understanding about workers' behavior—both on and off the job[40]— employers have ostensibly identified a

CZ45-M4L5] (discussing research by Lauren Rivera that shows interviewers with minimal training "look for a sense of connection" and base decisions on "subjective perceptions of applicant quality").

34. *See* Baer, *supra* note 32; Al Smith & Josh Wright, *How to Hack Hiring to Reduce Bias and Drive Success*, HR DAILY ADVISOR (July 31, 2019), https://hrdailyadvisor.blr.com/2019/07/31/how-to-hack-hiring-to-reduce-bias-and-drive-success/ [https://perma.cc/PR6M-WJWU]; Ruchika Tulshyan, *How to Reduce Personal Bias When Hiring*, HARV. BUS. REV. (June 28, 2019), https://hbr.org/2019/06/how-to-reduce-personal-bias-when-hiring.

35. *See* BOGEN & RIEKE, *supra* note 13, at 6; Brian O'Connell, *Five Recruiting Trends for the New Decade*, SOC'Y FOR HUM. RESOURCE MGMT. (Nov. 16, 2019), https://www.shrm.org/hr-today/news/all-things-work/pages/five-recruiting-trends.aspx [https://perma.cc/J886-LUN3].

36. SOC'Y FOR HUMAN RES. MGMT., 2017 TALENT ACQUISITION BENCHMARKING REPORT 4 (2017), https://www.shrm.org/hr-today/trends-and-forecasting/research-and-surveys/Documents/2017-Talent-Acquisition-Benchmarking.pdf [https://perma.cc/J58C-ZQ4R].

37. *See id.* at 13.

38. *See* Drew Harwell, *A Face-Scanning Algorithm Increasingly Decides Whether You Deserve the Job*, WASH. POST (Nov. 6, 2019, 12:21 PM), https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/. The appeal of these technologies is particularly desirable for large companies looking to fill a "high-volume [of] entry-level openings." *Id.*

39. *See* Don Peck, *They're Watching You at Work*, ATLANTIC (Dec. 2013), https://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/ (describing the application of predictive analytics to people's careers as an attempt to understand the "deepest of human mysteries: how we grow, whether we flourish, what we become").

40. *See* Sarah Krouse, *The New Ways Your Boss Is Spying on You*, WALL ST. J. (July 19, 2019, 5:30 AM), https://www.wsj.com/articles/the-new-ways-your-boss-is-spying-on-you-11563528604; Recruiting Daily Advisor Editorial Staff, *What Happens on Social Media, Stays on Social Media . . . and Employers Are Noticing*, HR DAILY ADVISOR (Aug. 13, 2018), https://hrdailyadvisor.blr.com/2018/08/13/happens-social-media-stays-social-media-employers-noticing/ [https://perma.cc/8YZQ-V66R]. Whereas there used to be a bigger information asymmetry problem, employers now have access to more information than ever before about each applicant. For example, an applicant's entire online history may be analyzed to extract information about their social lives, education level, and past employment experiences. *See* Saige Driver, *Keep It Clean: Social Media Screenings Gain in Popularity*, BUS. NEWS DAILY (Mar. 23, 2020), https://www.businessnewsdaily.com/2377-social-media-hiring.html [https://perma.cc/5YPP-Y3RB]; Recruiting Daily Advisor Editorial Staff, *supra*. Of course, many scholars have raised concerns about bias, false identifications, victims of cyberbullying, or the inability of these AI tools to recognize social context, such as humor and sarcasm, in an online forum. *See* Shirin Ghaffary, *The Algorithms That Detect Hate Speech Online Are Biased Against Black People*, Vox: RECODE (Aug. 15, 2019, 11:00 AM), https://www.vox.com/recode/2019/8/15/20806384/social-media-hate-speech-bias-black-african-american-facebook-twitter [https://perma.cc/BHN4-H5XW]; Carrie Goldberg, Opinion, *How Google Has Destroyed the Lives of Revenge Porn*

solution to the knowledge asymmetry problem. Employers can improve their practices by using AI to more efficiently and inexpensively isolate good candidates and exclude bad candidates.[41] An algorithm can be trained to extract valuable insights from enormous data sets, noting correlations and "'interpretable patterns' otherwise too subtle" for human detection.[42] For example, an algorithm can screen for both specific qualifications, such as ability to do the job, and general characteristics. In theory, all good workers share common character traits, namely honesty and integrity, regardless of industry or position.[43] These character traits are often threshold criteria for any hiring decision. At the same time, efforts to improve workplace diversity and inclusion (D&I) initiatives have prompted employers to embrace these tools as an effective means of eliminating bias and reducing reliance on subjective decisionmaking.[44] Proponents of the predictive data science approach claim the algorithms make fairer decisions because they are based on neutral and objective criteria that can be evaluated independently from a candidate's identity, age, name, gender, or education, which are frequently factors ripe for unconscious bias.[45]

This is why so many employers are developing an AI team. Traditional human resources departments are being rebranded as strategic talent acquisition

Victims, N.Y. POST (Aug. 17, 2019, 1:10 PM), https://nypost.com/2019/08/17/how-google-has-destroyed-the-lives-of-revenge-porn-victims/ [https://perma.cc/U9TJ-FARH]; Hillary K. Grigonis, *Social (Net)Work: What Can A.I. Catch – and Where Does It Fail Miserably?*, DIGITAL TRENDS (Feb. 3, 2018), https://www.digitaltrends.com/social-media/social-media-moderation-and-ai/ [https://perma.cc/43FK-F2CB]; Rebecca Heilweil, *Beware of These Futuristic Background Checks*, Vox: RECODE (May 11, 2020, 7:00 AM), https://www.vox.com/recode/2020/5/11/21166291/artificial-intelligence-ai-background-check-checkr-fama [https://perma.cc/67KG-LE26]. Moreover, this process of analyzing web histories does not necessarily correlate with job performance any more than inferring past behaviors based on a résumé. *See* John Sullivan, *The Top 10 Reasons Why Social Media Background Checks Are a Dumb Idea*, ERE (Aug. 20, 2018), https://www.ere.net/the-top-10-reasons-why-social-media-background-checks-are-a-dumb-idea/ [https://perma.cc/HU9Z-2M6R].

41. *See* BOGEN & RIEKE, *supra* note 13, at 3; CHENSOFF ET AL., *supra* note 20, at 5–6; Forbes Human Res. Council, *supra* note 20.

42. McKenzie Raub, Comment, *Bots, Bias and Big Data: Artificial Intelligence, Algorithmic Bias and Disparate Impact Liability in Hiring Practices*, 71 ARK. L. REV. 529, 533 (2018); *see also* Alexander Furnas, *Everything You Wanted to Know About Data Mining but Were Afraid to Ask*, ATLANTIC (Apr. 3, 2012), https://www.theatlantic.com/technology/archive/2012/04/everything-you-wanted-to-know-about-datamining-but-were-afraid-toask/255388/ (providing an overview of data mining and explaining how discovering information from large data sets take two forms—description and prediction—that allow us to infer conclusions based on pattern detection).

43. *See* Billy Arcement, *Why Honesty and Ethics Are the Two Most Powerful Leadership Traits*, BUS. JS. (Sept. 17, 2015, 9:10 AM), https://www.bizjournals.com/bizjournals/how-to/growth-strategies/2015/09/honesty-and-ethics-most-powerful-traits.html; Tom Searcy, *How to Hire Like Warren Buffett*, CBS NEWS: MONEYWATCH (Jan. 20, 2012, 1:57 PM), https://www.cbsnews.com/news/how-to-hire-like-warren-buffett/ [https://perma.cc/T5H6-L5LN]; Ken Sundheim, *15 Traits of the Ideal Employee*, FORBES (Apr. 2, 2013, 1:03 AM), https://www.forbes.com/sites/kensundheim/2013/04/02/15-traits-of-the-ideal-employee/?sh=4ec2ab16161f (identifying honesty as a key trait, reasoning "[a]n employee can have all the talent in the world, but without integrity and authenticity, nothing great will be accomplished").

44. *See* BOGEN & RIEKE, *supra* note 13, at 3, 5–6.

45. *See* Heilweil, *supra* note 10; Roy Maurer, *AI-Based Hiring Concerns Academics, Regulators*, SOC'Y FOR HUM. RESOURCE MGMT. (Feb. 14, 2020), https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/ai-based-hiring-concerns-academics-regulators.aspx [https://perma.cc/J33R-PEFQ].

departments.[46] Many companies created new "Chief People Officer[]" positions, filled by MBA graduates with a penchant for pop neuroscience,[47] and futuristic-sounding assessments that promise to revolutionize candidate screening and hiring procedures.[48] Branching beyond the traditional interview process, which can frequently become unstructured and consequently has long been derided as ineffective,[49] HR vendors are selling all kinds of new ways for employers to "rewire the brain circuitry"[50] of their workforce, and are offering a quicker way to sort candidates and determine potential based on completed cognitive and emotional assessments or neuroscience-based games.[51]

Industry experts anticipate significant growth and increased adoption rates for these predictive tools. A recent LinkedIn survey of nearly 9,000 hiring managers and recruiters who used some form of AI found sixty-seven percent embraced the technology because of time-to-hire efficiency gains, while forty-three percent credited AI as an effective means of combating bias in hiring decisionmaking.[52] That same survey found almost half of respondents identified data analytics as "[v]ery" or "extremely" important, and nearly one-fifth stated they had "[m]ostly" or "completely adopted" its use in their hiring practices.[53] Another survey revealed more than fifty-five percent of HR managers in the United States said AI would be "a regular part of their work within the next five years."[54] In recent years, the demand for algorithmic hiring screens has ballooned into an estimated

46. DAN LYONS, LAB RATS: HOW SILICON VALLEY MADE WORK MISERABLE FOR THE REST OF US 3 (2018).

47. *Id.* "Pop neuroscience" is a reference to our society's growing obsession and commercialization of neuroscience and consumer psychology that point to "the neural foundations of human behavior to explain everything." Sally Satel & Scott O. Lilienfeld, *Pop Neuroscience Is Bunk!*, SALON (June 8, 2013, 7:30 PM), https://www.salon.com/2013/06/08/pop_neuroscience_is_bunk/ [https://perma.cc/53FC-9WUP].

48. Cappelli, *supra* note 26; *see, e.g.*, Heilweil, *supra* note 10 (describing a company that promises it can predict applicants' "cognitive and personality traits" through assessments such as one in which applicants are asked to "hit[] the spacebar whenever a red circle, but not a green circle, flashes on the screen").

49. *See* Cappelli, *supra* note 26; Garland, *supra* note 28; Gene Marks, *Are Traditional Interviews a Thing of the Past?*, WASH. POST (Jan. 12, 2018, 10:00 AM), https://www.washingtonpost.com/news/on-small-business/wp/2018/01/12/are-traditional-interviews-a-thing-of-the-past/; Schmidt & Hunter, *supra* note 30, at 273.

50. LYONS, *supra* note 46, at 3, 154.

51. *See* Austin Carr, *Moneyball for Business: How AI Is Changing Talent Management*, FAST COMPANY (Aug. 16, 2018), https://www.fastcompany.com/90205539/moneyball-for-business-how-ai-is-changing-talent-management.

52. BENJAMIN SPAR & ILYA PLETENYUK, LINKEDIN TALENT SOLUTIONS, GLOBAL RECRUITING TRENDS 2018: THE 4 IDEAS CHANGING HOW YOU HIRE 2, 45 (Kate Reilly & Maria Ignatova eds., 2018), https://business.linkedin.com/content/dam/me/business/en-us/talent-solutions/resources/pdfs/linkedin-global-recruiting-trends-2018-en-us2.pdf [https://perma.cc/QR8Z-ZJFZ].

53. *See id.* at 4.

54. Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, REUTERS (Oct. 10, 2018, 6:04 PM), 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/TD97-RLPP].

$500 million industry[55] with over seventy different recruiting technologies available on the market today.[56] These various screens are being deployed at all stages of the hiring funnel: sourcing, screening, interviewing, and selection.[57] The types of available tools include: automated résumé review,[58] computerized matching and recommender systems,[59] interactive "chatbots,"[60] and predictive assessments and tests using web games.[61]

The latest trend in automated hiring is the use of AI-powered video-interviewing screens.[62] Many of the most prominent vendors are relying upon affect- or emotion-recognition technology, which detects an individual's emotions through the use of computer-vision algorithms and analyzes facial microexpressions, tone of voice, and other nonverbal communications to determine fit for a particular job.[63] In 2018, the emotion-detection or affect-recognition technology market was estimated to be worth $12 billion, and, according to some, could increase to as much as $90 billion by 2024.[64]

The leading player in the world of video-interviewing screens is HireVue.[65] Founded in 2004, the company quickly became well-known for its collection of preemployment assessments, including one-way prerecorded video-interviewing technology. [66] However, the company soon realized, their suite of screening tools had a timing "bottleneck": HR managers still had to manually review all of the

55. CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 108 (2016).

56. Jon Bischke, *Welcome to the Age of Recruiting Automation*, FORBES (July 12, 2018, 7:00 AM), https://www.forbes.com/sites/forbestechcouncil/2018/07/12/welcome-to-the-age-of-recruiting-automation/?sh=892878c1865e.

57. BOGEN & RIEKE, *supra* note 13, at 13–14.

58. *See Product*, IDEAL, https://ideal.com/product/ [https://perma.cc/F4ML-JY5N] (last visited Mar. 18, 2021).

59. *See About*, ZIPRECRUITER, https://www.ziprecruiter.com/about [https://perma.cc/D2Y6-GETU] (last visited Dec. 20, 2020).

60. *Meet Mya*, MYA, https://www.mya.com/meetmya/ [https://perma.cc/R6QD-AJTH] (last visited Mar. 18, 2021).

61. *Assessments*, PYMETRICS, https://www.pymetrics.ai/assessments [https://perma.cc/4XX3-W3C2] (last visited Mar. 18, 2021).

62. *See* BOGEN & RIEKE, *supra* note 13, at 36.

63. *See* CRAWFORD ET AL., *supra* note 4, at 50. Affect-recognition technology is also being used in other contexts, such as the healthcare industry to detect patient pain, the education system to measure student attentiveness, and the criminal justice system to conduct risks assessments, including identifying terrorists or detecting aggression. *Id.* However, not all video-interviewing technology companies use this technology. Some start-up companies, such as Spark Hire or WePow, allow for one-way video interviews, but unlike HireVue or Yobs Technologies, the platforms have not integrated AI or machine learning (ML) techniques to evaluate job candidates; instead, recordings of the interviews are preserved for a human reviewer. *See id.*; *Features*, SPARK HIRE (2020), https://www.sparkhire.com/tour [https://perma.cc/P6XW-XZ39] (last visited Mar. 18, 2021); *Product Tour*, WEPOW (2020), https://perma.cc/3XDX-VUMB (last visited Mar. 18, 2021); *infra* note 86.

64. Paul Sawers, *Realeyes Raises $12.4 Million to Help Brands Detect Emotion Using AI on Facial Expressions*, VENTURE BEAT (June 6, 2019, 12:30 AM), https://venturebeat.com/2019/06/06/realeyes-raises-12-4-million-to-help-brands-detect-emotion-using-ai-on-facial-expressions/ [https://perma.cc/JAX6-GX9C].

65. *See* Harwell, *supra* note 38.

66. *See* LYONS, *supra* note 46, at 157.

prerecorded videos.[67] In 2016, HireVue launched its AI and IO psychology service, an algorithm that would conduct the first round of candidate screening, as an addition to its video-interviewing software to address this issue.[68] The integrated assessments were designed to make powerful hiring predictions for their employer–clients.[69] HireVue claims their assessments, on average, can reduce the traditional time-to-hire from forty-two days to seven days, or a rate that is eighty percent faster.[70] Notably, HireVue emphasizes its focus on the user experience, framing these tools as a technological update to long-standing screening and testing assessments created fifty years ago.[71] Currently, the company has 700 customers worldwide, including some of the most globally recognizable brands: Nike, Goldman Sachs, Hilton, Unilever, and more.[72] The company's proprietary affect-recognition technology has already been used to conduct more than 12 million interviews worldwide.[73] The company has reportedly raised more than $90 million in venture capital,[74] and in late 2019, it announced the private-equity giant, Carlyle Group, as a new majority investor with an undisclosed capital investment.[75]

HireVue's system allows an applicant to self-record a response to a series of interview questions using a personal computer or cellphone camera.[76] For each applicant, tens of thousands of data points are evaluated by an algorithm, including the candidate's voice intonation, speech inflection, eye contact, perceived "enthusiasm" for the role, and up until recently, facial expressions.[77] These data

67. *Id.* Lyons noted that the recruiters could still fast-forward through videos, and thus, some efficiency gains were still being realized. *Id.* However, this was not enough. *Id.* In an effort to scale, HireVue's CEO Kevin Parker noted that "[w]e started asking, how can we use technology to take the place of what humans are doing?" *Id.*

68. *See* Erica Hill, *Introducing HireVue's IO Psychology and Assessment Experts*, HIREVUE (Aug. 5, 2016), https://perma.cc/SS26-QCWG. The company assembled a team of industrial organization (IO) psychologists and data scientists to encode "facial action units" into software. LYONS, *supra* note 46, at 157.

69. *See* Hill, *supra* note 68.

70. Joel Cheesman, *HireVue Goes Beyond Video Interviews to Tackle Artificial Intelligence*, RECRUITING TOOLS (Nov. 2, 2016), https://recruitingtools.com/hireview-digital-assessment/ [https://perma.cc/MLE2-WD2Q] (quoting Amanda Hahn, Director of Product Marketing, HireVue).

71. *See id.*

72. *See* LYONS, *supra* note 46, at 156–57; *Customers*, HIREVUE, https://perma.cc/2PCV-CH86 (last visited Dec. 20, 2020); David Rothnie, *HireVue Interview Questions at Goldman Sachs and JPMorgan*, EFINANCIALCAREERS (Aug. 25, 2020), https://news.efinancialcareers.com/us-en/292549/hirevue-interview-questions-goldman-sachs-jpmorgan [https://perma.cc/KDU4-477T]. However, not all of the clients use the AI-powered assessments. *See* LYONS, *supra* note 46, at 157.

73. Harwell, *supra* note 38.

74. Terena Bell, *This Bot Judges How Much You Smile During Your Job Interview*, FAST COMPANY (Jan. 15, 2019), https://www.fastcompany.com/90284772/this-bot-judges-how-much-you-smile-during-your-job-interview.

75. Harwell, *supra* note 38.

76. *See Frequently Asked Questions*, HIREVUE, https://www.hirevue.com/candidates/faq [https://perma.cc/87ZL-J3Q8] (last visited Mar. 18, 2021).

77. *See* Complaint & Request for Investigation, Injunction, & Other Relief Submitted by the Electronic Privacy Information Center (EPIC) at 11, *In re* HireVue, Inc. (F.T.C. Nov. 6, 2019) [hereinafter EPIC Complaint], https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf [https://perma.cc/R93P-JJX2]; NATHAN MONDRAGON, CLEMENS AICHHOLZER & KIKI LEUTNER,

points are then analyzed to determine the fit and suitability of the candidate and HireVue assigns each applicant a numerical "'employability' score."[78] The precise criteria are often developed in consultation with the employer to establish "future top performer" qualities and behaviors.[79] But in determining a candidate's employability score, the algorithm will typically evaluate cognitive ability, emotional intelligence, and personality traits,[80] including core competencies such as "willingness to learn," "conscientiousness & responsibility," and "personal stability."[81] Prior to its decision to halt facial analysis of candidates, the company's Chief Technology Officer, Loren Larsen, revealed as much as thirty percent of a candidate's score is based on facial expressions.[82] The scores are provided to the employer, who ultimately decides whether to follow up with a candidate. Even as the algorithms build "a database of deep, rich psychographic information on millions of people,"[83] HireVue does not provide candidates an opportunity to opt out of the video screens or to meaningfully challenge the assessments.[84]

HireVue is certainly not the only company offering these types of screens. For example, Yobs Technologies (Yobs) analyzes a number of nonverbal indicators of communication style—including tone, pitch, and emotions—as well as the applicant's word choice and sentence construction.[85] The company advertises that its

---

HIREVUE, THE NEXT GENERATION OF ASSESSMENTS 3–4 (2018); Harwell, *supra* note 38; *How to Prepare for Your HireVue Assessment*, HIREVUE (Apr. 16, 2019), https://www.hirevue.com/blog/how-to-prepare-for-your-hirevue-assessment [https://perma.cc/5WXL-PCPJ]; Knight, *supra* note 4 (noting in January 2021, HireVue announced it was halting facial expression analysis).

78. *See* MONDRAGON ET AL., *supra* note 77, at 3–4, 7; Harwell, *supra* note 38.

79. Harwell, *supra* note 38. HireVue claims that all algorithms are tested for bias impact prior to use and that they will take steps to mitigate any bias impact in compliance with the Uniform Guidelines on Employee Selection Procedures, jointly adopted by the Equal Employment Opportunity Commission (EEOC), the Department of Labor, the Department of Justice, and the U.S. Civil Service Commission. *See Bias, AI Ethics and the HireVue Approach*, HIREVUE, https://www.hirevue.com/why-hirevue/ai-ethics [https://perma.cc/2DB6-AGX7] (last visited Mar. 18, 2021). In addition, the company reports its data scientists comply with the "legal, professional, and validation standards established within the field of psychology." *Id.*

80. *See* MONDRAGON ET AL., *supra* note 77, at 3; *see also How to Prepare for Your HireVue Assessment*, *supra* note 77 (discussing evaluations of "game-based assessments").

81. Harwell, *supra* note 38.

82. Terena Bell, *supra* note 74. Of course, HireVue has since announced it will halt facial analysis of candidates, and so it remains to be seen which other factors will be weighted more heavily in the final evaluation score. *See* Knight, *supra* note 4.

83. LYONS, *supra* note 46, at 159. Although such data protection concerns are beyond the scope of this Note, it is worth noting that the data collected—data that is enormously sensitive because it creates a "psychographic blueprint" attached to all personal information typically provided to a prospective employer—is not anonymous. *See id.* Although HireVue claims to be careful in safeguarding and to not sharing the data beyond the contracting employer, the potential for it to be misused certainly exists. *See id.*

84. EPIC Complaint, *supra* note 77, at 12.

85. *The Science Behind Yobs*, YOBS TECHNOLOGIES, https://www.yobstech.com/how-it-works [https://perma.cc/E3UA-2JRY] (last visited Mar. 18, 2021). Yobs has created an "application programing interface (API) for measuring behavioral insights from voice, video and text communication" that uses "prosody," linguistic analysis, and community vision to infer personality characteristics that can be used to predict the likelihood of success and fit for the role. *See id.* Prosody is the process of analysis of "tone, pitch, emotions and other non-verbal elements of communication" to ascertain a person's communication style. *Id.* The API is trained to evaluate the "Big 5," which are the

platform is capable of "unlock[ing] the behavior, soft skills and personality data trapped" in voice and video interviews.[86] Accordingly, the company eschews relying on résumé or cover letters as indictors of success: "[b]usiness has moved to voice and video" and Yobs' API "provides the missing insights on behavior, soft skills, personality and more."[87] Another company, Talview, has developed a proprietary software, Talview Behavioral Insights (TBI), that is capable of gauging emotions and analyzing tone and other indicators of communication style.[88] Notably, the company claims the TBI engine can "analy [ze] the *subtext* of a candidate's video" to uncover fake insights.[89] In other words, the technology screens for the sincerity and honesty of candidates' responses. Another competitor, VCV.AI (VCV), has similarly developed a screen which uses facial and voice recognition software to analyze a candidate's video or phone interview[90] and can detect "nervousness, mood, and behavior patterns to help recruiters assess whether a person is a good cultural fit for the company."[91] And this list of vendors is certainly not comprehensive, because numerous other start-ups are looking to cash in on this burgeoning sector.

"most important dimensions of personality and soft skills" according to the Five Factor Model; the Model is "used by 85% of the Fortune 500 in hiring and training assessments" and endorsed by industry experts. *Id.* The five personality traits are: openness, conscientiousness, extraversion, agreeableness, and neuroticism. *Id.* Conscientiousness purports to measure "a person's attitude towards doing the right thing, such as doing a full detailed job, even when the boss isn't watching." *Id.*

86. *Yobs Technologies*, CRUNCHBASE, https://perma.cc/ALH7-GACF (last visited Mar. 18, 2021); *see Solutions*, YOBS TECHS., https://perma.cc/9HGX-6BNF (last visited Mar. 18, 2021) ("Unlock the value in your voice & video data.").

87. *See* YOBS TECHS., https://perma.cc/4JTK-R3FB (last visited Mar. 18, 2021).

88. *See Video Interview Software*, TALVIEW, https://www.talview.com/video-interview-software [https://perma.cc/Q9PV-W7JD] (last visited Mar. 18, 2021). Talview is an AI-powered video interviewing platform company, which offers cognitive remote proctoring technology to analyze a candidate's "soft skills, motivation, proficiency, and expertise in a single step." *Id.* The company claims to make time-to-hire sixty percent faster. *Id.* Talview's technology is currently used in more than 100 countries and by many Fortune 500 companies, including Amazon, Sephora, and others. *See Our Customers*, TALVIEW, https://www.talview.com/customers [https://perma.cc/68BK-585Z] (last visited Mar. 18, 2021).

89. *Talview Behavioral Insights*, TALVIEW (emphasis added), https://www.talview.com/behavioral-insights [https://perma.cc/QVJ5-A9DC] (last visited Mar. 18, 2021). The company has recognized that a big concern with standard multiple-choice based psychometric tests is candidates gaming the test by choosing the known "socially accepted answers," which may reduce the accuracy of the behavioral analysis. *See id.*

90. VCV, https://vcvpages.com/vcvai [https://perma.cc/V52R-AF73] (last visited Mar. 18, 2021). VCV is an "AI-powered platform that facilitates the hiring process making it ethical, smart, and fast." *Id.* VCV offers a combination of automated résumé review, phone interviewing technology, and video interviewing technology. *See id.* VCV boasts its predictive screening technology can reduce the time to select three candidates for a final in-person interview from twenty-one hours to just forty-five minutes. *Id.*

91. Mike Butcher, *The Robot-Recruiter Is Coming—VCV's AI Will Read Your Face in a Job Interview*, TECHCRUNCH (Apr. 23, 2019, 8:00 AM), https://techcrunch.com/2019/04/23/the-robot-recruiter-is-coming-vcvs-ai-will-read-your-face-in-a-job-interview/ [https://perma.cc/YJ6R-QP8M].

B. CURRENT REGULATORY APPROACHES

The use of algorithmic hiring screens has raised significant concerns about privacy, transparency, and bias. Some legal scholars have already questioned whether existing public or private regulatory enforcement mechanisms will be able to adequately redress harms.[92] The majority of existing scholarship has focused on three approaches: (1) antidiscrimination law, (2) consumer protection law, and (3) data protection law. As this Section will argue, however, each of these frameworks have inherent shortcomings that make them insufficient to address the scope of the harms caused by affect-recognition screens.

1. Antidiscrimination Law

The most well-known criticism of algorithmic hiring is the heightened risk of unlawful discrimination based on protected characteristics[93] or proxies for protected characteristics.[94] Legal scholars dispute the claim that algorithmic hiring is inherently less subjective and, therefore, less biased when compared with human

92. *See, e.g.*, Barocas & Selbst, *supra* note 2, at 698 (concluding discriminatory data mining is by definition unintentional, and not adequately addressed by the law); Jason R. Bent, *Is Algorithmic Affirmative Action Legal?*, 108 GEO. L.J. 803, 805–06, 809, 811–15, 841–42, 852–53 (2020) (discussing if algorithmic affirmative action is legal and analyzing the problem of unintentional algorithmic discrimination; the opportunity for algorithms to remedy past discrimination and strengthen workplace diversity; and the tensions between anticlassification and antisubordination theories of Title VII and equal protection); Kim, *supra* note 1, at 865–68 (arguing the harms caused by "biased algorithms are not easily captured by traditional antidiscrimination law," and although classification bias under a disparate impact theory may be amenable, due to the "diffuse nature of the harms and the significant resources that would be required to challenge biased algorithms, it may be difficult to incentivize individual plaintiffs to enforce a prohibition on classification bias"); Andrew Tutt, *An FDA for Algorithms*, 69 ADMIN. L. REV. 83, 104–11 (2017) (proposing a new regulatory agency to approve algorithms ex ante in order to address the shortcomings of antidiscrimination law).

93. *See* Ifeoma Ajunwa, Opinion, *Beware of Automated Hiring*, N.Y. TIMES (Oct. 8, 2019), https://www.nytimes.com/2019/10/08/opinion/ai-hiring-discrimination.html; Dave Gershgorn, *Companies Are on the Hook if Their Hiring Algorithms Are Biased*, QUARTZ (Oct. 22, 2018), https://qz.com/1427621/companies-are-on-the-hook-if-their-hiring-algorithms-are-biased/; Lauren Kirchner, *When Discrimination Is Baked into Algorithms*, ATLANTIC (Sept. 6, 2015), https://www.theatlantic.com/business/archive/2015/09/discrimination-algorithms-disparate-impact/403969/.

94. *See* Kirchner, *supra* note 93; Prince & Schwarcz, *supra* note 5, at 1264. A potential proxy variable for membership in a protected category is ZIP code, which is determinative of race because of a long history of discrimination in housing and "redlining." *See The Future of Work*, 116th Cong. 6, *supra* note 19, at 8; Prince & Schwarcz, *supra* note 5, at 1265–66 (arguing proxy discrimination occurs when an algorithm "uses a variable whose predictive power derives from its correlation with membership in the suspect class"). These concerns are not unique to the employment context. Regulators and academics have raised concerns about data-driven discrimination in insurance, criminal justice, education, unemployment benefits, and more. *See, e.g.*, Ryan Calo & Danielle Keats Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 EMORY L.J. 797, 800, 802 (2021) (arguing, through the frame of administrative law, that the delegation of human decisionmaking to machines may undermine important values, such as "transparency, accountability, and due process"); Aziz Z. Huq, *Racial Equity in Algorithmic Criminal Justice*, 68 DUKE L.J. 1043, 1045 (2019); Ray Lehmann, *Why 'Big Data' Will Force Insurance Companies to Think Hard About Race*, INS. J. (Mar. 27, 2018), https://www.insurancejournal.com/blogs/rightstreet/2018/03/27/484530.htm [https://perma.cc/BZ82-KPBF]; Andre M. Perry & Nicol Turner Lee, *AI Is Coming to Schools, and if We're Not Careful, So Will Its Biases*, BROOKINGS (Sept. 26, 2019), https://www.brookings.edu/blog/the-avenue/2019/09/26/ai-is-coming-to-schools-and-if-were-not-careful-so-will-its-biases/ [https://perma.cc/F2EB-T3GZ].

interviewers.[95] "[D]ata are," after all, "not neutral."[96] An algorithm is only as good as the underlying data set, which may be "inaccurate, biased, or unrepresentative."[97] Although algorithms and data mining could "breathe new life into traditional forms of intentional discrimination" through a process called "masking," the more common occurrence—and therefore, more pressing concern—is unintentional discrimination.[98] For example, the variables selected by the employer's model may be unintentionally discriminatory, particularly if they are designed to simply automate and replicate past hiring decisions. [99] Or, in the absence of the directly predictive variable, the algorithm may seek out proxies that are still highly correlated with protected characteristics.[100] In this way, critics contend, the bias of AI systems mirror the bias of human decisionmakers—or society in general—and may perpetuate existing institutional and systemic biases of past hiring decisions, only "rapidly scaled."[101]

In 2018, Amazon made headlines after scrapping an automated hiring tool created to help rank top talent after it kept discriminating against women.[102] The company's engineering team trained the predictive tool to "trawl through" and identify common terms in the résumés of top performers over a ten-year period.[103] Because most of the résumés were of male employees, however, the

95. *See, e.g.*, BOGEN & RIEKE, *supra* note 13, at 7–9, 47; Ajunwa, *The Paradox of Automation*, *supra* note 5, at 1685–86; Miller, *supra* note 1. The misconception stems from a belief that automated systems purport to be "fair" because they "rate all individuals in the same way, thus averting discrimination." Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 4 (2014).

96. Kim, *supra* note 1, at 860.

97. *Id.* at 860–61; *see also* Barocas & Selbst, *supra* note 2, at 674 ("Discrimination may be an artifact of the data mining process itself, rather than a result of programmers assigning certain factors inappropriate weight.").

98. Barocas & Selbst, *supra* note 2, at 692–93.

99. Jenny R. Yang, *Three Ways AI Can Discriminate in Hiring and Three Ways Forward*, URB. INST.: URB. WIRE (Feb. 12, 2020), https://www.urban.org/urban-wire/three-ways-ai-can-discriminate-hiring-and-three-ways-forward [https://perma.cc/T5V4-GHSJ] ("Often the bias in AI systems is the human behavior it emulates. When employers seek to simply automate and replicate their past hiring decisions, rather than hire based on a rigorous analysis of job-related criteria, this can perpetuate historic bias.").

100. Barocas & Selbst, *supra* note 2, at 691–92. Barocas and Selbst argue "[d]ecision makers do not necessarily intend this disparate impact because they hold prejudicial beliefs; rather, their reasonable priorities as profit seekers unintentionally recapitulate the inequality that happens to exist in society." *Id.* at 691. "The problem stems from what researchers call 'redundant encodings,' cases in which membership in a protected class happens to be encoded in other data." *Id.* This phenomenon explains why a discriminatory impact can occur when the algorithm is only intending to optimize the accuracy of its determination and is not intentionally discriminating based on membership in a protected category. *Id.* at 692.

101. *See* Yang, *supra* note 99; *see also* BOGEN & RIEKE, *supra* note 13, at 8 (discussing how AI systems can "[p]erpetuate [b]iases").

102. Isobel Asher Hamilton, *Amazon Built an AI Tool to Hire People but Had to Shut It Down Because It Was Discriminating Against Women*, BUS. INSIDER (Oct. 10, 2018, 5:47 AM), https://www.businessinsider.com/amazon-built-ai-to-hire-people-discriminated-against-women-2018-10; Dastin, *supra* note 54.

103. Hamilton, *supra* note 102.

algorithm learned to prefer male candidates.[104] It then penalized "résumés containing the words 'women's' and filtered out" graduates of all-women colleges.[105] The engineers tried to fix the problem by de-emphasizing certain terms.[106] Ultimately, the tool was abandoned after Amazon concluded it could not guarantee the algorithm would not continue to be biased.[107] Similarly, an audit of a different company's résumé-screening tool revealed the strongest predictors of job success turned out to be: (1) being named Jared, and (2) playing high school lacrosse.[108] The risks of discrimination are certainly not limited to automated résumé review. The use of facial-recognition technology has raised similar concerns, especially after numerous incidents where the systems failed to recognize BIPOC (Black, Indigenous, People of Color) or discriminated against individuals with disabilities.[109]

The ability of federal antidiscrimination laws, mainly Title VII of the Civil Rights Act of 1964[110] (Title VII), to address the unique risks posed by algorithmic discrimination in hiring, however, remains uncertain. Although the courts have yet to weigh in on this issue,[111] legal scholars have argued such claims could be brought under a disparate treatment or disparate impact theory.[112] However, either approach is likely to face significant legal and factual hurdles. In proving a claim of disparate treatment, or intentional discrimination, a plaintiff must overcome the ostensible neutrality of algorithmic decisionmaking[113] and the "black

104. *Id.*

105. *Id.*

106. *See* Dastin, *supra* note 54.

107. *See id.*

108. Gershgorn, *supra* note 93.

109. *See* Alex Engler, *For Some Employment Algorithms, Disability Discrimination by Default*, BROOKINGS: TECHTANK BLOG (Oct. 31, 2019), https://www.brookings.edu/blog/techtank/2019/10/31/for-some-employment-algorithms-disability-discrimination-by-default/ [https://perma.cc/25D5-KWM5]; PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 1–2 (2019) (finding empirical evidence for how the majority of face recognitions algorithms assessed race, sex, and age demographics differently).

110. 42 U.S.C. § 2000e (2018).

111. At the time of this Note's publication, no case has been filed under either state or federal antidiscrimination law.

112. *See* Bornstein, *supra* note 5, at 540–43. Professor Bornstein describes competing approaches in the current scholarship, the "improve the algorithms" theory versus the "improve the law" approach, while offering a third: freedom from individual stereotypes. *Id.* at 520, 539–40.

113. *See* Barocas & Selbst, *supra* note 2, at 698 (arguing that "[e]xcept for masking, discriminatory data mining is by stipulation unintentional"); Bornstein, *supra* note 5, at 534–35 ("[B]y its very nature . . . algorithmic discrimination is 'unintentional.'"). Of course, "a prejudiced employer might hide its discriminatory intent behind a biased," Kim, *supra* note 1, at 865, but "seemingly neutral data model to justify its intent to discriminate," Bornstein, *supra* note 5, at 537–38. This practice is called "masking," and it is a familiar problem in antidiscrimination law, even if it is being accomplished algorithmically. *See* Barocas & Selbst, *supra* note 2, at 692, 696. However, without adequate insight into the underlying data or decisionmaking process, proving discriminatory intent in algorithmic discrimination is particularly difficult. *Cf.* Courtney Hinkle, Note, *Employment Discrimination in the Digital Age*, 21 GEO. J. GENDER & L. ONLINE (2019). *But see* Kim, *supra* note 1, at 865 ("Such a scenario poses no particular conceptual challenge, although proof may be difficult as a practical matter.").

box" nature of the algorithm itself, which creates significant knowledge gaps hindering the establishment of the requisite intent to discriminate.[114]

Under a disparate impact framework, employer liability is premised on a facially neutral policy or practice that nonetheless causes "a disparate impact with respect to a protected class."[115] This framework is potentially a better fit for addressing algorithmic discrimination because there is no requirement of employer intent.[116] However, absent updates to the law, scholars have identified potential pitfalls in this approach that may limit its appeal. First, "it is unclear how much disparate impact is" required to establish a prima facie case.[117] Second, an employer's affirmative defense under Title VII—that the policy or practice is "job related" and "consistent with business necessity"—may prove to be an extremely powerful release from liability.[118] Algorithms are designed to find statistical correlations related to success on the job. And, as Professor Kim argues, asking whether the algorithm, or variables used in it, is job related is "tautological" because "the algorithm can always serve as its own validation," even if it produces a discriminatory impact.[119] In other words, the algorithm would be self-validating.[120]

Finally, an antidiscrimination law approach may inevitably turn into an endless debate over what is the threshold level of statistical correlation between a legitimate proxy variable and a legally protected characteristic in a deeply and

---

114. *See* Hinkle, *supra* note 113 (noting that a "'black-box' algorithm can shield an employer from knowing which factors were the basis for a selection decision"); Dave Gershgorn, *AI Is Now So Complex Its Creators Can't Trust Why It Makes Decisions*, QUARTZ (Dec. 7, 2017), https://qz.com/1146753/ai-is-now-so-complex-its-creators-cant-trust-why-it-makes-decisions/; Yang, *supra* note 99 ("Compounding these problems [of biased data, biased variables, and biased decisions], many systems operate as a 'black box,' meaning vendors of algorithmic systems do not disclose how inputs lead to decisions."). *See generally* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015).

115. Barocas & Selbst, *supra* note 2, at 701.

116. *See id.*

117. *Id.* The EEOC and the Uniform Guidelines on Employee Selection Procedures (Uniform Guidelines) have established a standard for determining whether a test or selection procedure is nondiscriminatory. *See id.* at 701–02. The so-called "four-fifths rule" creates a presumption of disparate impact: "[a] selection rate for any race, sex, or ethnic group which is less than four-fifths . . . of the rate for the group with the highest rate will generally be regarded . . . as evidence of adverse impact." *Id.* (quoting Uniform Guidelines on Employment Selection Procedures, 29 C.F.R. § 1607.4(D) (2015)). However, this rule was developed in an era of small data, and recently, scholars have called for an update to the Uniform Guidelines, to clarify validation standards for algorithmic screens in an era of big data. *See* Yang, *supra* note 99. Moreover, as Professor Kim notes, plaintiffs may find it difficult to identify the "relevant labor market" given that the algorithm presumes a closed universe of data. *See* Kim, *supra* note 1, at 917, 919.

118. Bornstein, *supra* note 5, at 554 (quoting 42 U.S.C. 2000e-2(k)(1)(A)(i) (2012)). Employers can prove job-relatedness and business necessity by performing a "'validation study' that demonstrates that the practice is a valid measure for job performance." *Id.* at 555.

119. *Id.* at 538 (citing Kim, *supra* note 1, at 866, 908) (discussing Professor Kim's foundational work).

120. *Id.* at 555–56.

inherently biased society.[121] For example, scholars, analogizing to historic redlining, have long recognized that ZIP codes serve as a stand in, or proxy, for race.[122] However, where so much historical discrimination is carried forward into present-day discrimination, and so much about ourselves—from our education, our employment history, or even our tastes in music—is determined by our race, gender, or national origin, it may prove impossible for any algorithm to hermetically seal off consideration of these factors. This challenge is exacerbated by the law's lack of a formal definition of proxies.[123]

While the theoretical scholarly debate continues, the wait to see how courts may rule on a Title VII challenge to an AI-powered hiring model could soon be over. In October 2019, the Equal Employment Opportunity Commission (EEOC) reportedly opened an investigation into two discrimination claims where the employer relied on an algorithm to make hiring, promotion, and other employment decisions.[124] A case is likely to reach federal court this year whether that means the EEOC brings suit or the private litigant files charges. Regardless of the results of any upcoming judicial determination, establishing protections for workers solely under the current antidiscrimination law framework would be insufficient. Regulating the use of these screens under Title VII would certainly provide some protections, and the algorithms, as well as underlying data sets, can—and should—be scrutinized for bias.[125]

But under existing legal doctrine, eliminating discriminatory outcomes and guaranteeing equal opportunity—which is essential for human dignity—are not necessarily synonymous goals and, more importantly, a narrow approach wherein oversight is conducted solely under antidiscrimination law would fail to protect individuals from the privacy harms caused by these screens. Current narrow interpretations of antidiscrimination statutes can operate as a race to the bottom for equal treatment. Since the early 1950s, the Supreme Court has interpreted the

---

121. *See* Ignacio N. Cofone, *Algorithmic Discrimination Is an Information Problem*, 70 HASTINGS L.J. 1389, 1404–06, 1412–15 (2019) (arguing "[t]he corollary problem is that, if one wanted to block all proxies for protected categories, one would never cease to find more information points that, to some degree, are predictive of each other and would need to be blocked. In that endeavor, one might have to block information *ad infinitum*." (footnote omitted)).

122. *See supra* note 94 and accompanying text.

123. *See generally* Prince & Schwarcz, *supra* note 5 (discussing the definitional sticking points between which variables in the algorithm are so closely related to an impermissible protected characteristic that a proxy problem emerges).

124. Chris Opfer, Ben Penn & Jaclyn Diaz, *Punching In: Workplace Bias Police Look at Hiring Algorithms*, BLOOMBERG L. (Oct. 28, 2019, 6:00 AM), https://news.bloomberglaw.com/daily-labor-report/punching-in-workplace-bias-police-look-at-hiring-algorithms.

125. The civil rights community has been relentless in raising the risks of discrimination and bias in algorithmic hiring. Earlier this year, "civil rights leaders [had] released an important set of Civil Rights Principles to guide tech developers, employers, and policymakers in the development, use, and auditing of hiring assessment technologies." Jenny R. Yang, *New Civil Rights Principles Mark First Step to Make AI Hiring More Equitable*, URB. INST.: URB. WIRE (July 23, 2020), https://www.urban.org/urban-wire/new-civil-rights-principles-mark-first-step-make-ai-hiring-more-equitable [https://perma.cc/S7L3-G7Q3]. These proposals should be embraced and operationalized by policymakers and regulators at the local, state, and federal level.

Equal Protection Clause[126] and other federal civil rights acts to guarantee a right of nondiscrimination.[127] The principle that "we 'do not discriminate on the basis of race' is now not only an unmovable part of our law, it has become very much a part of the American story, and even of the American dream."[128] But, the power of this commitment leaves much to be desired. As Professor Robin West writes, "[t]he antidiscrimination principle counsels nondiscrimination, but it carries no mandate, and even articulates no vision, regarding the civil rights of which we cannot, or should not, be discriminatorily deprived."[129] In other words, "while the principle posits the moral wrongness of discriminatory line-drawing, that condemnation rests solely on a set of claims about the fairness or unfairness of discriminatory decision-making, rather than on any conception of the value of that from which people cannot be discriminatorily excluded."[130] So long as everyone is treated equally, or at least equal in the formal sense, there may be no right or claim for redress guaranteed by our civil rights laws.

The limits of antidiscrimination law create a mismatch for guaranteeing the right to privacy—a critical civil right in an increasingly surveilled society—and protection from the associated harms caused by these screens.[131] Under Title VII, the threshold question is often whether these screens can be deployed across a

126. U.S. CONST. amend. XIV, § 1.

127. *See* ROBIN L. WEST, CIVIL RIGHTS: RETHINKING THEIR NATURAL FOUNDATION 30–31 & nn.5 & 6 (2019). The "antidiscrimination principle" stands for the proposition that "[d]ecision-making . . . must be *nondiscriminatory*, for it to be legal." *Id.* at 30 (citing Paul Brest, *The Supreme Court 1975 Term, Foreword: In Defense of the Antidiscrimination Principle*, 90 HARV. L. REV. 1, 5 (1976)). In other words, "decisions by either lawmakers or powerful private actors, such as employers or property conveyors and their agents, cannot be made on the *basis of categories* defined by race, and by virtue of legislative extension, by sex, ethnicity, national origin, or religious affiliation either." *Id.* (emphasis added); *see also* Helen Norton, *The Supreme Court's Post-Racial Turn Towards a Zero-Sum Understanding of Equality*, 52 WM. & MARY L. REV. 197, 210 (2010) ("[A]nticlassification rationales have increasingly commanded a majority of the contemporary Court"); Reva B. Siegel, *Equality Talk: Antisubordination and Anticlassification Values in Constitutional Struggles over* Brown, 117 HARV. L. REV. 1470, 1476–77 (2004) (discussing how the "anticlassification principle" emerged in the 1960s and 1970s to interpret equal protection doctrine and limit the effect of *Brown v. Board of Education*, 347 U.S. 483 (1954)); Reva B. Siegel, *From Colorblindness to Antibalkanization: An Emerging Ground of Decision in Race Equality* Cases, 120 YALE L.J. 1278, 1286–87 (2011) (explaining the scholarly "[d]ebate between the anticlassification and antisubordination understandings of equal protection grew out of social struggle over *Brown*," and finding "[o]n the conventional account, the anticlassification understanding of equal protection ultimately prevailed," although not sufficiently powerful to completely erase antisubordination theories from the law).

128. WEST, *supra* note 127, at 38.

129. *Id.* at 46.

130. *Id.* at 51–52. West grounds this critique in the "sizeable, and formidable, body of skeptical legal scholarship," which includes:

> [C]ritiques of antidiscrimination law first articulated by the critical legal studies movement in the 1980s, greatly expanded and elaborated critical arguments from critical race theory and critical feminist legal theory a decade later, and the more contemporary and in some ways deeper arguments put forward in the past fifteen years by postmodern and queer theorists.

Id. at 10 (citations omitted).

131. For a discussion of the resulting privacy harms from video-interviewing screens, see *infra* Part III.

diverse applicant pool without a discriminatory effect; in other words, the primary focus is on the *validity* of the technology.[132] But whether the technology is valid—or does not disproportionately exclude certain candidates above a formally identified statistical threshold—fails to reckon with the broader privacy harms. By analyzing this issue solely under this narrow framework, the legitimacy of the technology is presumed. We skip over an initial inquiry into whether the technology or practice should be unleashed on anyone at all. Or, whether, as with affect screening, the likelihood of substantial privacy violations calls for a more robust mechanism of oversight and accountability. A regulatory scheme that provides redress only for formal measures of discrimination, but not privacy violations, would not protect individuals from the full extent of harms caused by these screens. The hollowness of antidiscrimination law fails to recognize a right to be free from certain types of privacy intrusions.

2. Consumer Protection Law

In addition to antidiscrimination law, the use of algorithmic hiring screens has been challenged as an unfair and deceptive trade practice under Section 5 of the Federal Trade Commission (FTC) Act (Section 5).[133] Section 5 prohibits "unfair or deceptive acts or practices in or affecting commerce,"[134] and empowers the FTC to enforce the Act's prohibitions.[135] An act or practice is "unfair" or "deceptive" if there is a "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment,"[136] or which "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[137] Although the FTC is empowered to bring a claim in federal court, the final disposition in most

132. *See* Raghavan et al., *supra* note 11, at 4 (detailing that "[a]ccording to the Uniform Guidelines, the gold standard for pre-employment assessments is *validity*: the outcome of a test should say something meaningful about a candidate's potential as an employee," and an assessment may be legally discriminatory "if the selection rate for one protected group is less than 4/5 of that of the group with the highest selection rate," commonly known as the "4/5 rule" (citation omitted)); Maurer, *supra* note 45; Manish Raghavan & Solon Barocas, *Challenges for Mitigating Bias in Algorithmic Hiring*, BROOKINGS (Dec. 6, 2019), https://www.brookings.edu/research/challenges-for-mitigating-bias-in-algorithmic-hiring/ [https://perma.cc/F3PH-HWUS] (noting a common approach used by vendors to avoid legal liability under the Uniform Guidelines is to deploy "de-biasing" methods that test a model for disparate impact and remove variables to sufficiently mitigate any discrimination caused by the selection procedure). Some scholars have emphasized the need to update the Uniform Guidelines in the era of big data and algorithms. *See* Yang, *supra* note 99.

133. *See* EPIC Complaint, *supra* note 77, at 1.

134. 15 U.S.C. § 45(a)(1) (2018).

135. *Id.* § 45d(b)(2)(A). *See generally A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMMISSION (Oct. 2019), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority [https://perma.cc/8QKY-8UBF].

136. *In re* Cliffdale Assocs., Inc., 103 F.T.C. 110, 1984 WL 565319, at *45 (Mar. 23, 1984) (quoting letter from James C. Miller III, FTC Chairman, to Honorable John D. Dingell, Chairman of House Committee on Energy and Commerce).

137. 15 U.S.C. § 45(n).

Section 5 cases is "settlement, default judgement, or abandonment of the action by the FTC in the investigatory stage."[138] The FTC will typically require an investigative target to enter into a consent decree, or settlement agreement, which charts out the conduct the FTC believes is a violation of Section 5 and provides a roadmap to address the unlawful behavior.[139] Almost every settlement requires some type of record keeping or compliance report that must be made available to the FTC for up to twenty years.[140] However, the FTC lacks enforcement authority to extract monetary penalties, unless the terms of the consent order are violated.[141]

In November 2019, the Electronic Privacy Information Center (EPIC), a public interest organization committed to protecting privacy and civil liberties, filed a complaint with the FTC urging the agency to open an investigation into HireVue's video-interviewing assessments.[142] First, the EPIC argued that HireVue engaged in deceptive trade practices by using facial-recognition technology to evaluate candidates, despite representing otherwise to candidates.[143] Second, the EPIC argued HireVue unfairly used "facial recognition technology, biometric data, and secret algorithms" in order to assess job candidates' "'cognitive ability,' 'psychological traits,' 'emotional intelligence,' and 'social aptitudes'" in violation of the Organization for Economic Cooperation and Development (OECD) Principles on Artificial Intelligence and Section 5 of the FTC Act.[144] The EPIC argued that the collection of sensitive biometric data and use of secret algorithms "causes or is likely to cause substantial injury to a large class of people" that cannot reasonably be avoided because there are no opportunities for applicants to opt out or meaningfully challenge the assessments.[145] Even when the unfair trade practices are balanced against the "countervailing benefits to consumers or to competition," the EPIC alleged there is no legitimate business need for collecting this sensitive data.[146] The EPIC asserted this level of intrusion "causes substantial privacy harms to job candidates."[147]

---

138. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 606 (2014).

139. *See id.* at 613–19 (detailing the commonly included components of FTC settlements).

140. *See id.* at 614, 618.

141. WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 226 (2016).

142. EPIC Complaint, *supra* note 77, at 1.

143. *Id.* at 9.

144. *See id.* at 2–3, 10–12. The OECD AI Principles were first "established in 1961 to promote economic cooperation and development." *Id.* at 2. In 2019, the thirty-six member nations of the OECD, including the United States, worked with many non-OECD countries to release these principles on the use of AI. *Id.* at 2. The principles endorsed a commitment to the "rule of law, human rights and democratic values," and called for systems that are "robust, secure and safe throughout their entire lifecycle." *Id.* at 3. In particular, the OECD AI Principle on Transparency and Explainability called for meaningful information and disclosure to "make stakeholders aware of their interactions with AI systems, including in the workplace." *Id.*

145. *See id.* at 11–12.

146. *See id.* at 12.

147. *Id.* at 11.

Even though the FTC has yet to publicly announce a response to the EPIC's complaint,[148] there are limits to relying upon the FTC to regulate these hiring screens. First, the consent decree model has been criticized as "lack[ing] teeth" because of its flexible enforcement terms that allow companies to satisfy the order without fully remedying the harm.[149] As evidence of this fact, industry-leading technology companies, including Facebook, Google, Snapchat, Twitter, and Uber, are all under a consent decree.[150] But it is a well-known secret that the FTC has not actually forced these companies to fundamentally change their intrusive business practices.[151] Second, even if the FTC can secure monetary remedies for violations of a consent decree, the fines are often a drop in the bucket compared to the profits derived from the violations. For example, in 2019, the FTC announced a $5 billion fine against Facebook for violating its original 2011 settlement.[152] Despite being the largest fine ever imposed on any company, two FTC

148. *Cf.* Knight, *supra* note 4. It should also be noted HireVue recently agreed to halt its use of facial analysis earlier this year, which would address many of the concerns raised by the EPIC. *See id.* However, John Davisson, Senior Counsel at the EPIC, stated he remained concerned the automated analysis of speech could still pose problems, and the decision to end the facial analysis component did not ameliorate potential issues around data collection and bias and opacity. *See id.*

149. Michelle De Mooy, *How to Strengthen the FTC Privacy & Security Consent Decrees*, CTR. FOR DEMOCRACY & TECH. (Apr. 12, 2018), https://cdt.org/insights/how-to-strengthen-the-ftc-privacy-security-consent-decrees/ [https://perma.cc/JH2R-N4MD]; *see* Kate Conger, *FTC Privacy Audits of Companies Like Facebook and Google Are 'Woefully Inadequate*,' GIZMODO (Apr. 19, 2018, 5:01 PM), https://gizmodo.com/ftc-privacy-audits-of-companies-like-facebook-and-googl-1825387315 [https://perma.cc/8MJA-MCNH].

150. *See* De Mooy, *supra* note 149.

151. *See id.*; Makena Kelly, *If Congress Wants the FTC to Be Tougher on Tech, It Needs to Pass a Privacy Law*, VERGE (Sept. 6, 2019, 11:13 AM), https://www.theverge.com/2019/9/6/20852807/google-youtube-ftc-congress-privacy-law-bill-facebook-equifax [https://perma.cc/2EH4-B55V]. For example, the FTC's historic emphasis on requiring additional consumer disclosures as a solution to "deceptive or obstructionist default settings" does little to alter the overall design of a product—it only increases the "burden[] on consumers to understand how data can be collected [and] used." De Mooy, *supra* note 149. Moreover, the fact there are numerous repeat offenders—such as Facebook, Uber, and Google—suggests that the deterrent effect of an FTC consent decree is not sufficiently robust. *See* Press Release, Fed. Trade Comm'n, Uber Agrees to Expanded Settlement with FTC Related to Privacy, Security Claims (Apr. 12, 2018), https://www.ftc.gov/news-events/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security [https://perma.cc/M5KB-MJ7B] (discussing how Uber, while negotiating a consent decree settlement with the FTC, failed to disclose another consumer data breach, requiring the FTC to expand its oversight—but notably, no fine); *Review of FTC Settlement with Google*, CONSUMER WATCHDOG, https://www.consumerwatchdog.org/newsrelease/ftc-225-million-settlement-google-deficient-three-reasons-including-failure-include-perm [https://perma.cc/3CFA-MXK6] (last visited Mar. 19, 2021); Kara Swisher, Opinion, *Put Another Zero on Facebook's Fine. Then We Can Talk.*, N.Y. TIMES (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/opinion/facebook-fine.html. *But see* Chris Jay Hoofnagle, Woodrow Hartzog & Daniel J. Solove, *The FTC Can Rise to the Privacy Challenge, but Not Without Help from Congress*, BROOKINGS (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ [https://perma.cc/BTB5-8CDR] (arguing "the FTC has done well given its limits" and its "performance has to be evaluated in the context of its hostile environment," while conceding the agency "needs more resources, more tools, a greater shield from political pressure, and a clear Congressional mandate" to rise to the privacy challenge).

152. Cecilia Kang, *F.T.C. Approves Facebook Fine of About $5 Billion*, N.Y. TIMES (July 12, 2019), https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html.

Commissioners rightfully questioned whether the fine would have a meaningful deterrent effect, noting Facebook's gross annual revenues grew from $5 billion to over $55 billion between 2012 and 2018 and, in 2019, the company's first-quarter earnings were $15 billion.[153] Similarly, Google was fined $22.5 million "for violating the terms of its consent order," which "amounted to less than half a single day's revenue."[154] These limitations lead to a permissive regulatory environment, where companies feel emboldened to violate consumer rights and to treat the penalties as "simply the cost of doing business."[155]

3. Data Protection Law

Another way of regulating algorithmic hiring screens is applying a data protection framework. Although not entirely identical, most data protection regimes share similar consistent features.[156] For example, they presume an individual's right to control his or her personal information, which is "sometimes classified as a human right."[157] This approach is derived from the "fair information practices" (FIPs), first developed in the 1970s, which provide affirmative rights to access personal data or to request modification or deletion.[158] This type of privacy framework defines the European Union's (EU) General Data Protection Regulation (GDPR).[159] But unlike the EU, the United States never fully signed on to the data protection model.[160] Instead, the United States embraced a "patchwork approach" that is "more permissive, indeterminate, and based upon people's vulnerabilities in their commercial relationship with companies."[161]

Given the federal government's notoriously light-touch approach regarding the regulation of data privacy and AI,[162] state and local governments have started to

153. *In re* Facebook, Inc., F.T.C. No. 1823109, at 8 (July 24, 2019) (Kelly, Comm'r, dissenting), https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf [https://perma.cc/5RD2-X2WB]; *see In re* Facebook, Inc., F.T.C. No. 1823109, at 8 (July 24, 2019) (Chopra, Comm'r, dissenting), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf [https://perma.cc/C3S7-4EF9].

154. De Mooy, *supra* note 149.

155. *Id.*

156. MCGEVERAN, *supra* note 141, at 257.

157. *See id.*

158. *Id.*

159. *See id.* at 258.

160. *See id.*

161. Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1690 (2020).

162. There is currently no comprehensive federal privacy law. *Cf. id.* at 1690. And there is no overarching federal strategy to regulate AI. Martijn Rasser, *The United States Needs a Strategy for Artificial Intelligence*, FOREIGN POL'Y (Dec. 24, 2019, 7:27 AM), https://foreignpolicy.com/2019/12/24/national-artificial-intelligence-strategy-united-states-fall-behind-china/. However, growing public concern over the perceived dangers of unfettered use of AI by the private sector has prompted some lawmakers to propose legislation. For example, Representative Daniel Lipinski (D-IL-3) introduced the Growing Artificial Intelligence Through Research Act (GrAITR Act), which would invest more than $1.6 billion over five years in artificial intelligence research and development efforts. *See* H.R. 2202, 116th Cong. (2019). Senators Rob Portman (R-OH), Martin Heinrich (D-NM), and Brian Schatz (D-HI)

fill the leadership vacuum,[163] particularly California, which has emerged as a leader in adopting robust online privacy legislation.[164] In 2018, California swiftly adopted a robust, GDPR-style data protection regime—the California Consumer Privacy Act (CCPA).[165] The CCPA officially took effect on January 1, 2020, and it imposed a wide range of requirements for the collection and processing of personal data.[166] This law, which was designed to protect consumer's data, could potentially constrain the collection and use of candidate or employee data.[167] Unfortunately, lawmakers punted on the specifics and provided an extension for most employer compliance requirements until December 31, 2020.[168] And in late September 2020, Governor Gavin Newsom signed an amendment into law extending the exemptions until January 2022.[169] But even as the rules were

proposed a companion bill, the Artificial Intelligence Initiative Act (AI-IA). *See* S. 1558, 116th Cong. (2019). In addition, the Trump Administration in 2019 announced an Executive Order, Maintaining American Leadership in Artificial Intelligence, which identified five focus areas: increasing research and development; establishing AI standards; building an AI workforce; promoting public trust; and fostering international collaboration and protection. *See* Exec. Order No. 13,859, 84 Fed. Reg. 3967 (Feb. 14, 2019). In February 2020, the White House released the American Artificial Intelligence Initiative: Year One Annual Report. OFFICE OF SCI. & TECH. POLICY, EXEC. OFFICE OF THE PRESIDENT, AMERICAN ARTIFICIAL INTELLIGENCE INITIATIVE: YEAR ONE ANNUAL REPORT (2020), https://perma.cc/8UM2-4A4R. The new Biden–Harris administration is likely to face pressure from privacy and cybersecurity advocacy groups to prioritize a federal data privacy legislation, especially now that Democrats will control both the House and Senate in the 117th Congress. *See* Kristen L. Bryan, Lydia de la Torre, Glenn A. Brown & Aaron C. Garavaglia, *Election 2020: Looking Forward to What a Biden Presidency May Mean for Data Privacy and Data Privacy Litigation*, NAT'L L. REV. (Nov. 12, 2020), https://www.natlawreview.com/article/election-2020-looking-forward-to-what-biden-presidency-may-mean-data-privacy-and [https://perma.cc/W8BA-LB8A]; Cameron F. Kerry & Caitlin Chin, *How the 2020 Elections Will Shape the Federal Privacy Debate*, BROOKINGS (Oct. 26, 2020), https://www.brookings.edu/blog/techtank/2020/10/26/how-the-2020-elections-will-shape-the-federal-privacy-debate/ [https://perma.cc/VP6F-WV76]; Josephine Wolff, *It's Long Past Time for a Federal Data Protection Law*, SLATE (Nov. 30, 2020, 1:06 PM), https://slate.com/technology/2020/11/biden-administration-cybersecurity-data-protection-law.html.

163. *See* Jonathan G. Cedarbaum, D. Reed. Freeman, Jr. & Lydia Lichlyter, *Privacy Legislation Continues to Move Forward in Many States*, WILMERHALE (Apr. 30, 2019), https://www.wilmerhale.com/en/insights/client-alerts/20190430-privacy-legislation-continues-to-move-forward-in-many-states [https://perma.cc/V5PK-38MZ]; Sarah Rippy, *US State Comprehensive Privacy Law Comparison*, INT'L ASS'N PRIVACY PROFESSIONALS, https://iapp.org/resources/article/state-comparison-table/ [https://perma.cc/4AJC-8KYR] (last visited Mar. 19, 2021).

164. *See* Jessica Guynn, *California Passes Nation's Toughest Online Privacy Law*, USA TODAY (July 6, 2018, 4:26 PM), https://www.usatoday.com/story/tech/2018/06/28/california-lawmakers-pass-tough-new-online-privacy-rules-could-model-other-states/743397002/.

165. *See* CAL. CIV. CODE §§ 1798.100–.199.95 (West, Westlaw through 2021 Reg. Sess.).

166. Sara Morrison, *California's New Privacy Law, Explained*, VOX: RECODE (Dec. 30, 2019, 6:50 PM), https://www.vox.com/recode/2019/12/30/21030754/ccpa-2020-california-privacy-law-rights-explained [https://perma.cc/9ZHV-8DL9].

167. *See id.*

168. *See* Joseph J. Lazzarotti, Jason C. Gavejian & Maya Atrakchi, *California Extends CCPA Employee Personal Information Exemption*, SOC'Y FOR HUM. RESOURCE MGMT. (Oct. 22, 2020), https://www.shrm.org/ResourcesAndTools/legal-and-compliance/state-and-local-updates/Pages/California-Extends-CCPA-Employee-Personal-Information-Exemption.aspx [https://perma.cc/7U34-WG58]; Morrison, *supra* note 166.

169. Dagatha L. Delgado, Doron S. Goldstein, Megan Hardiman, Jeremy Merkel & Trisha Sircar, *CCPA Employee and B2B Exemption Extended Until* 2022, NAT'L L. REV. (Oct. 1, 2020), https://www.

actively being written, the CCPA framework began with a flawed assumption: the power (and burden) to enforce privacy violations should reside with the individual.[170] Despite its ambitious agenda, the CCPA embraced a "notice and choice" model, which requires individuals to first know what data is being gathered (notice) and to take action to withhold consent or object to that collection (choice).[171]

The focus on criticisms of the CCPA, however, may already be outdated, as the current state of data privacy law in California remains in flux, shifting rapidly. In response to criticisms that the CCPA was not sufficiently robust and consequently vulnerable to industry efforts to weaken it,[172] consumer advocates organized around a new ballot initiative to strengthen privacy protections.[173] In November 2020, less than a year after the CCPA became effective, California voters passed Proposition 24, the California Privacy Rights Act of 2020 (CPRA).[174] The CPRA will become law as written, and its substantive provisions will go into effect on January 1, 2023.[175] The new law amends the CCPA in critical ways, including: creating new "protections for sensitive personal information"; expanding "opt out rights to include new types of information sharing"; and requiring "additional mechanisms for individuals to access, correct, or delete data," particularly "information used by automated decision-making systems."[176]

---

natlawreview.com/article/ccpa-employee-and-b2b-exemption-extended-until-2022 [https://perma.cc/SX6H-6HUN].

170. *See* Hartzog & Richards, *supra* note 161, at 1712, 1734 ("Although the [CCPA] purportedly aimed to move away from the dominant U.S. 'notice and choice' model, the rights granted to Californians still center around industry transparency and individual notions of consent, control, and choice." Moreover, "[t]hese concepts [of control, informed consent, transparency, notice, and choice] are attractive because they seem empowering. But in basing policy principles for data protection on notice and choice, privacy frameworks are asking too much from a concept that works best when preserved, optimized, and deployed in remarkably limited doses."); Morrison, *supra* note 166.

171. *See* Hartzog & Richards, *supra* note 161, at 1704; Morrison, *supra* note 166 (discussing how the CPPA allows consumers the choice to tell companies to delete their personal information or to not sell it to third parties).

172. *See* Editorial, *Endorsement: Yes on Prop. 24. It's Not Perfect, but It Would Improve Online Privacy*, L.A. TIMES (Sept. 15, 2020, 3:00 AM), https://www.latimes.com/opinion/story/2020-09-15/yes-on-proposition-24.

173. *See* Tony Romm, *Privacy Activist in California Launches New Ballot Initiative for 2020 Election*, WASH. POST (Sept. 24, 2019, 8:00 PM), https://www.washingtonpost.com/technology/2019/09/25/privacy-activist-california-launches-new-ballot-initiative-election/. In particular, the ballot measure was intended to close a loophole in the CCPA that still permitted target advertisements, because social media companies did not "consider the ads to be a 'sale' of user data." *See* Laura Hautala, *Proposition 24 Passes in California, Pushing Privacy Rights to the Forefront Again*, CNET (Nov. 4, 2020, 10:02 AM), https://www.cnet.com/news/prop-24-passes-in-california-pushing-privacy-rights-to-the-forefront-again/ [https://perma.cc/ZX6P-GQR2].

174. Brian H. Lam, *California Privacy Rights Act Passes–Dramatically Altering the CCPA*, NAT'L L. REV. (Nov. 6, 2020), https://www.natlawreview.com/article/california-privacy-rights-act-passes-dramatically-altering-ccpa [https://perma.cc/U3PA-CFXS].

175. *See id.*

176. Stacey Gray, Katelyn Ringrose, Polly Sanderson & Veronica Alix, *California's Prop 24, the "California Privacy Rights Act," Passed. What's Next?*, FUTURE PRIVACY F. (Dec. 17, 2020), https://fpf.org/blog/californias-prop-24-the-california-privacy-rights-act-passed-whats-next/ [https://perma.cc/C3FM-2DKF]*; see California's Proposition 24*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/state-

For example, the CPRA improves upon the CCPA by imposing data minimization and retention requirements on businesses that collect data.[177] Additionally, the CPRA created a new California Privacy Protection Agency (PPA), consolidating rulemaking and enforcement authority under a single agency and allocating $10 million annually in funding.[178]

We must wait for a more comprehensive assessment of the benefits and weaknesses of the CPRA to be revealed, as precise details regarding how the law will be implemented will not come into focus until the time the law takes effect in 2023.[179] Additionally, the California legislature could build upon the CPRA's new foundation by passing additional amendments that strengthen (but not weaken) consumer privacy.[180] The creation of an independent enforcement agency with rulemaking authority will undoubtedly increase enforcement efforts and provide more detailed regulations interpreting the law. However, privacy advocates were split in their support for the ballot measure, and these divisions could continue as these new privacy rules are being written.[181] And a persistent criticism of the CCPA—of which the CPRA did not fully reckon[182]—is the continued embrace of a "notice and choice" framework.[183]

---

policy/ca-prop24/ [https://perma.cc/E4W9-PQ7Z] (last visited Mar. 19, 2021). A more in-depth review of the CPRA is beyond the scope of this Note.

177. Cameron F. Kerry & Caitlin Chin, *By Passing Proposition 24, California Voters Up the Ante on Federal Privacy Law*, BROOKINGS (Nov. 17, 2020), https://www.brookings.edu/blog/techtank/2020/11/17/by-passing-proposition-24-california-voters-up-the-ante-on-federal-privacy-law/ [https://perma.cc/JCW6-SL5H]; *see California's Proposition 24*, *supra* note 176.

178. *California's Proposition 24*, *supra* note 176; Gray et al., *supra* note 176.

179. *See* Gray et al., *supra* note 176.

180. *California's Proposition 24*, *supra* note 176.

181. *See* Gilad Edelman, *The Fight over the Fight over California's Privacy Future*, WIRED (Sept. 21, 2020, 9:00 AM), https://www.wired.com/story/california-prop-24-fight-over-privacy-future/; Geoffrey A. Fowler & Tonya Riley, *The Technology 202: Privacy Advocates Battle Each Other over Whether California's Proposition 24 Better Protects Consumers*, WASH. POST (Aug. 4, 2020, 8:35 AM), https://www.washingtonpost.com/politics/2020/08/04/technology-202-privacy-advocates-battle-each-other-over-whether-california-proposition-24-better-protects-consumers/.

182. Although the CPRA was enacted in response to perceived weaknesses of the CCPA, the regulatory framework remains the same—that is, the CPRA provides individual-rights holders to assert more rights, but the burden remains on individuals to assert those rights. *See* Bret Cohen, Tim Tobin & Aaron Lariviere, *Understanding the New California Privacy Rights Act: How Businesses Can Comply with the CPRA*, HOGAN LOVELLS (Nov. 25, 2020), https://www.engage.hoganlovells.com/knowledgeservices/news/understanding-the-new-california-privacy-rights-act-how-businesses-can-comply-with-the-cpra [https://perma.cc/YJ9R-GL4D] ("While the CPRA maintains the core framework of the predecessor California Consumer Privacy Act (CCPA), . . . compliance will necessitate a careful review of existing practices and thoughtful changes to . . . privacy notices, [and] individual rights response procedures."); *CPRA Rivals GDPR's Privacy Protections While Emphasizing Consumer Choice*, AKIN GUMP (Nov. 11, 2020), https://www.akingump.com/en/news-insights/cpra-rivals-gdprs-privacy-protections-while-emphasizing-consumer-choice.html [https://perma.cc/2MDP-NMWB]; Damon W. Silver, *CPRA Series: Impacts on Notice at Collection and Privacy Policy*, JACKSON LEWIS (Nov. 19, 2020), https://www.workplaceprivacyreport.com/2020/11/articles/california-consumer-privacy-act/cpra-series-impacts-on-notice-at-collection-and-privacy-policy/ [https://perma.cc/6PXA-47RR].

183. *See California's Proposition 24*, *supra* note 176; Kerry & Chin, *supra* note 177.

Privacy scholars have widely criticized the notice and choice approach for its failure to adequately protect individual privacy rights.[184] As Woodrow Hartzog and Neil Richards argue, the concept of "privacy self-management" is attractive because it seems empowering.[185] But such regimes only work if there is perfect transparency and true consent—neither of which are present.[186] In practice, these regimes are intended to overwhelm human users by imposing on them the significant burden of uncovering the well hidden, nefarious uses of their personal data and intentionally designing "the path of least resistance" to facilitate a blanket release of one's privacy rights.[187] The notion that individuals have sufficient autonomy to meaningfully challenge some of the most powerful corporations in the world further illustrates the absurdity of consent in this context.[188] Additionally, the individualized focus of a notice and choice model often fails to consider the broader social and civil rights implications of protecting privacy as a societal good.[189] According to Hartzog and Richards, a data protection regime presumes the collection and processing of data is "inevitable—and inevitably good," so long as there are *some* procedural safeguards.[190] For example, in the context of video-interviewing screens, a data protection approach would do little to guard against the privacy harms imposed by the technology. Even if there was complete transparency, the power disparity between employees and employers is stark, dispelling the fictitious notions of true consent. As these screens become more ubiquitous, an applicant's only choice could be between a job or no job at all.

In 2019, Illinois passed the Artificial Intelligence Video Interview Act, which specifically governs the use of AI in hiring screens.[191] The law requires an employer using AI to fill a position in Illinois to: (1) give notice to the applicant that AI is being used to evaluate fitness for the position; (2) provide the applicant with an explanation for how the AI "works and what general types of characteristics" are being evaluated; (3) obtain consent from the applicant; (4) keep recordings confidential by limiting disclosure to only "persons whose expertise or technology is necessary in order to evaluate an applicant's fitness for a position";

184. *See* Hartzog & Richards, *supra* note 161, at 1694–95, 1704, 1734–35.

185. *Id*. at 1734.

186. *See id*. Under a notice and choice model, companies are incentivized to obfuscate the risks in their data practices by designing their tools using insights from behavioral economics to create a facade of meaningful choice. *See id*. 1734–35. For example, boxes people can check, buttons to press, or switches to activate or deactivate. *Id*. at 1735.

187. *Id*. at 1735–36.

188. *Cf*. *id*. at 1734–36.

189. *See id*. at 1725.

190. *See id*. at 1724. Under this approach, a data protection regime "fail[s] to question the implications of the processing itself." *Id*.; *see* Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEORETICAL INQUIRIES L. 1, 11 (2019) ("Data harvesting and processing are one of the principal business models of informational capitalism, so there is little motivation either to devise more effective methods of privacy regulation or to implement existing methods more rigorously. Instead, the cultural and political discourses that have emerged around data-centered 'innovation' work to position such activities as virtuous and productive, and therefore ideally exempted from state control.").

191. Heilweil, *supra* note 10.

and (5) destroy both the video and all copies within thirty days upon the applicant's request.[192] The law does not define "artificial intelligence," detail the level of "explanation" required, or clarify whether the law applies to employers filling any positions in Illinois or only to interviews completed in the state.[193] But even if the legislature could solve for this lack of clarity, the same problems with a notice and choice model remain. Employers could merely disclose the bare minimum, with a generic "click to agree" option as a condition for interviewing. So long as the notice was sufficient, the use of the technology would continue unabated because the individual applicant would still have no power to meaningfully challenge these practices other than to forgo the interview entirely.

II. THE RISE (AND FALL) OF THE LIE DETECTOR TEST

To better understand the current vogue for AI screens, one must consider a previous chapter of employee screening technology: the lie detector test. This Part will chart out the origins of lie detector technology and its modern application with a focus on the employment sector, where it was celebrated as an effective method of screening out dishonest and higher risk employees. The idea that lie detectors, however, are capable of accurately detecting deception, or distinguishing truths from falsehoods, has been sharply criticized by the scientific community.[194] But even if the technology could be validated, many policymakers and privacy scholars still questioned whether it is ever justified to permit this level of intrusion into a person's private thoughts.[195] In response to growing opposition towards their unregulated use, Congress passed a federal law banning the use of lie detectors: The Employee Polygraph Protection Act (EPPA).[196] Although arguably "one of the least-known federal workplace statutes," the EPPA's "broad prohibitions have virtually eliminated" the use of lie detector tests in the workplace.[197] Moreover, as this Part argues, flexible statutory drafting ensured the EPPA's protections could withstand the test of time and adapt to future advancements in lie-detection technology.[198]

192. 820 ILL. COMP. STAT. 42/1, 5, 10, 15 (2020).

193. *See id*.; Daniel Waltz, Molly DiRago & Ronald I. Raether, Jr., *Illinois Employers Must Comply with Artificial Intelligence Video Interview Act*, SOC'Y FOR HUM. RESOURCE MGMT. (Sept. 5, 2019), https://www.shrm.org/resourcesandtools/legal-and-compliance/state-and-local-updates/pages/illinois-artificial-intelligence-video-interview-act.aspx [https://perma.cc/N5BP-G2WX].

194. *See* OFFICE OF TECH. ASSESSMENT, U.S. CONGRESS, SCIENTIFIC VALIDITY OF POLYGRAPH TESTING: A RESEARCH REVIEW AND EVALUATION 29, 34 (1983), https://ota.fas.org/reports/8320.pdf [https://perma.cc/9ADY-QQGX].

195. *See id*. at 34–35.

196. Employee Polygraph Protection Act of 1988, Pub. L. No. 100-347, 102 Stat. 646 (codified as amended in scattered sections of 29 U.S.C.).

197. Amy Onder & Michael Brittan, *Recent Case Law Under the Employee Polygraph Protection Act: A Practical Review*, PRIVACY & DATA SECURITY L.J. 483, 483 (2009).

198. *See id*. at 484–85.

A. THE QUEST FOR THE PERFECT LIE DETECTOR

People have been trying to detect falsehoods for as long as they have been telling lies.[199] Whether we are successful at it, however, is a separate question. Despite many individuals believing that they are good at detecting lies, research shows humans are actually really bad at it.[200] On average, an individual can accurately separate truth from a lie fifty-four percent of the time—only slightly "better than tossing a coin" or mere guesswork.[201] Nevertheless, we tend to believe other people are bad at concealing lies[202] and embrace the myth that their dishonesty can reliably be observed.[203] The theory is that when a person lies, it causes certain psychological or physiological changes which involuntarily betray their statement as a truth or falsehood.[204] A common explanation is that for most people, lying is a stressful, taxing endeavor and the energy to suppress the truth leaves "evidence in our bodies and actions."[205] Despite the lack of scientific evidence that such physiological markers exist,[206] our personal deficiencies in recognizing signs of deception have sparked enormous interest in developing new methods to correct for our untrustworthy instincts.[207]

A variety of methods have been offered in pursuit of unearthing these hidden lies. The predominant techniques rely on extrapolating correlations between the subject's physical response and an act of deception.[208] A "lie detector" is, thus, a

199. COMM. TO REVIEW THE SCI. EVIDENCE OF THE POLYGRAPH, NAT'L RESEARCH COUNCIL, The POLYGRAPH AND LIE DETECTION 1 (2003).

200. *See* Richard Wiseman, *The Truth About Lying and Laughing*, GUARDIAN (Apr. 20, 2007, 7:33 PM), https://www.theguardian.com/science/2007/apr/21/weekendmagazine.

201. Amit Katwala, *The Race to Create a Perfect Lie Detector—and the Dangers of Succeeding*, GUARDIAN (Sept. 5, 2019, 1:00 PM), https://www.theguardian.com/technology/2019/sep/05/the-race-to-create-a-perfect-lie-detector-and-the-dangers-of-succeeding.

202. *Cf.* KEN ALDER, THE LIE DETECTORS: THE HISTORY OF AN AMERICAN OBSESSION, at xii-xiii (2007) ("[T]he vast majority of us are very bad at detecting deception, despite our confidence in our own powers."); ALDERT VRIJ, DETECTING LIES AND DECEIT: PITFALLS AND OPPORTUNITIES 2 (2d ed. 2008) (explaining "[p]eople tend to *over*estimate their own *ability to detect lies*"); Maggie Koerth, *Why Humans Are Bad at Spotting Lies*, FIVETHIRTYEIGHT (Sept. 28, 2018, 3:00 PM), https://fivethirtyeight.com/features/why-humans-are-bad-at-spotting-lies/ [https://perma.cc/8PHZ-CY9D] (noting people "falsely believe [they] are good at interpreting trustworthiness from behavior," despite the lack of evidence).

203. *See The Truth About Lie Detectors (aka Polygraph Tests)*, AM. PSYCHOL. ASS'N (Aug. 5, 2004), https://www.apa.org/research/action/polygraph [https://perma.cc/LW95-DLZB].

204. *See id.* As Sigmund Freud once claimed: "No mortal can keep a secret . . . . Betrayal oozes out of him at every pore." Katwala, *supra* note 201.

205. Katwala, *supra* note 201.

206. *See* Joseph Stromberg, *Lie Detectors: Why They Don't Work, and Why Police Use Them Anyway*, VOX (Dec. 15, 2014, 2:00 PM), https://www.vox.com/2014/8/14/5999119/polygraphs-lie-detectors-do-they-work [https://perma.cc/SGJ4-8LNA]; *cf.* Katwala, *supra* note 201 (discussing how psychological responses could be from "fear of getting caught in a lie, or anxiety about being wrongly accused").

207. *See* ALDER, *supra* note 202 (detailing the methods of detecting deception dating back centuries, and how, due to our persistent inability to successfully sort truth tellers from liars, "in the early years of the twentieth century, a coterie of American psychologists set out to decipher the operations of the human mind by peering beneath the skin").

208. *See* Ken Alder, *To Tell the Truth: The Polygraph Exam and the Marketing of American Expertise*, 24 HIST. REFLECTIONS 487, 488 (1998) ("The premise of these [lie detector] tests is that while

misnomer: such methods only infer generalized deception in response to a series of questions or actions.[209] Some of the earliest methods date back three thousand years, where "the accused were forced to chew and spit out rice; the grains were thought to stick in the dry, nervous mouths of the guilty."[210] Other methods included trial by ordeal or torture.[211] According to "[t]he historical writings of various European countries," the rationale for the "*trial by ordeal* - or the *Judgements of God* . . . was based on the belief that God would not let a righteous man suffer and injustice prevail."[212]

In the modern era, lie detection has become almost synonymous with the polygraph test, which was first developed in the 1920s.[213] According to John Larson, the inventor of the polygraph, "[w]hen our conscious self deviates from the truth, and denies it, the subconscious self and the body demand to be adapted to reality, to be truthful." [214] In other words, "[w]e come to the paradoxical formulation that human beings lie with their consciousness, but are truthful with their unconscious, and when they do not confess with their mouths, then they confess with their body."[215] The polygraph device was designed in order to capture these physiological responses and infer a conclusion about the subject's truthfulness or deceptions.[216] "Although there are numerous variations in testing procedures, the polygraph" testing instruments are fairly uniform.[217] The polygraph will measure the "heart rate, blood pressure, sweating, and breathing" of an individual in response to a series of questions.[218] A physiological recorder is often used to

---

the mind may lie (those malicious—if immortal—souls of men and women), the body is honest (our subtle—but analyzable—corporeal particularity)."); Paul V. Trovillo, *A History of Lie Detection*, 29 AM. J. POL. SCI. 848, 852–57 (1939); Katwala, s*upra* note 201.

209. *The Truth About Lie Detectors*, *supra* note 203.

210. Katwala, s*upra* note 201; *see* Trovillo, *supra* note 208, at 853.

211. Trovillo, *supra* note 208, at 850–54. Methods included: "The Ordeal of the Balance," which arose in India and required the accused to stand on a scale, and if after listening to the judge deliver an exhortation, the accused weight less than before, he was acquitted; "The Boiling Water Ordeal," which was used in Africa, and identified a thief by requiring individuals to stick their arms first into cold water, then quickly into boiling pot, if the individual developed blisters or peeling, he was guilty. *Id.* at 851–52.

212. Martina Vicianova, *Historical Techniques of Lie Detection*, 11 EUR.'S J. PSYCHOL. 522, 523 (2015). For example, "[i]n one such test presumed liars were asked to lick a burning hot poker, straight from the fire. If God wanted to commend their honesty, their tongues would not be burned." Alder, *supra* note 208.

213. Katwala, s*upra* note 201.

214. Margaret Gibson, *The Truth Machine: Polygraphs, Popular Culture and the Confessing Body*, 11 SOC. SEMIOTICS 61, 61 (2001) (emphasis omitted) (quoting John Larson).

215. *Id.*

216. *See* Katwala, *supra* note 201.

217. OFFICE OF TECH. ASSESSMENT, *supra* note 194, at 11.

218. Stromberg, *supra* note 206; *see* Katwala, *supra* note 201. A popular method of administering the test uses the Control Question Technique (CQT). Stromberg, *supra* note 206. For example, in a criminal investigation, "the questioner will mix control questions"—usually vaguely threatening questions unrelated to the inquiry, such as "[h]ave you ever stolen from a friend?"—"with specific questions relevant to the case," such as "[d]id you commit the robbery on June 17?" *Id.* The theory presumes the control questions will establish a baseline anxiety, "because the questions are vague and hard to answer entirely truthfully," which will be lower in response to the specific questions if they are not lying. *Id.*

administer the test.[219] Examiners will typically use "pneumographs wrapped around a subject's chest" to measure rate and depth of respiration, a blood pressure cuff to measure cardiovascular activity, and "electrodes attached to a subject's fingertips" to measure galvanic skin responses or sweat.[220] Examiners then analyze patterns created by the rise and fall of needles, which make lines on paper in response to the subject's physical reactions, to determine if a person being deceptive or truthful.[221]

The recent advancements in data technology have introduced new methods of diagnosing truthfulness or deceptiveness, often called "next-generation lie detector[s]."[222] These new tools analyze not only the words we say, but also the way we say them.[223] Our word choice may indicate an intent to deceive.[224] Experts in digital communications conducted a study of online dating profiles and found individuals who used words in them; such increased use of negations (for example, "no," "not," "never") and decreased use of self-references (for example, "I," "me," or "myself") were more likely to have outright lies or deceptive exaggerations about themselves in their profile.[225] The sound of our voice, or nonverbal content of our speech, may also reveal our dishonesty.[226] For example, voice-stress analysis (VSA) and Layered Voice Analysis (LVA) technology aims to measure deception by analyzing changes in tone of voice, which look at "microtremors" indicting stress, or physical effort, of attempting to deceive.[227]

Another method is the Guilty Knowledge Test (GKT) which involves "developing a multiple-choice test with items concerning knowledge that only a guilty subject could have." *The Truth About Lie Detectors*, *supra* note 203. For example, to test a thief, the questions might contain varying values for a stolen item, such as "[w]as $500, $1,000, or $5,000 stolen?" *Id.* If only a guilty mind would know the correct answer, there would be a correlating physiological reaction. *Id.*

219. *The Truth About Lie Detectors*, *supra* note 203.

220. *Id.*

221. Christina Sterbenz, *The One Thing You Need to Know to Pass a Polygraph Test*, BUS. INSIDER (June 3, 2015, 10:55 AM), https://www.businessinsider.com/how-to-pass-a-polygraph-test-2015-5.

222. *See Eye Detect*, CONVERUS, https://converus.com/eyedetect/ [https://perma.cc/NBT7-SEFF] (last visited Mar. 20, 2021); Katwala, *supra* note 201.

223. *See* Katwala, *supra* note 201.

224. *See id.*

225. Catalina L. Toma & Jeffrey T. Hancock, *What Lies Beneath: The Linguistic Traces of Deception in Online Dating Profiles*, 62 J. COMM. 78, 80–81 (2012).

226. *See* Katwala, *supra* note 201.

227. *See* Kelly R. Damphousse, *Voice Stress Analysis: Only 15 Percent of Lies About Drug Use Detected in Field Test*, NAT'L INST. JUST. (Mar. 16, 2008), https://nij.ojp.gov/topics/articles/voice-stress-analysis-only-15-percent-lies-about-drug-use-detected-field-test [https://perma.cc/HHJ4-3LPT]; Katwala, *supra* note 201. In addition to the criminal context, voice-analysis technology is increasingly used in call centers to monitor customer reactions; in the latest generation of voice-controlled virtual assistants, such as Siri and Alexa; and in wearable technologies. *See* Isobel Asher Hamilton, *AI Experts Doubt Amazon's New Halo Wearable Can Accurately Judge the Emotion in Your Voice, and Worry About the Privacy Risks*, BUS. INSIDER (Aug. 29, 2020, 5:30 AM), https://www.businessinsider.com/experts-skeptical-amazon-halo-judges-emotional-state-from-voice-2020-8; Tom Simonite, *This Call May Be Monitored for Tone and Emotion*, WIRED (Mar. 19, 2018, 7:00 AM), https://www.wired.com/story/this-call-may-be-monitored-for-tone-and-emotion/. For example, Amazon is currently marketing its new wearable device, Halo, as capable of analyzing voice tone in order to detect emotions, such as whether you sound "happy, sad, excited or tired." *See* Austin Carr, *Amazon's New Wearable Will Know If I'm Angry. Is that Weird?*, BLOOMBERG (Aug. 31, 2020, 6:45 AM), https://www.bloomberg.com/news/newsletters/2020-08-31/amazon-s-halo-wearable-can-read-emotions-is-that-too-weird. Voice-

Another technique relies on facial movements and body language, such as micro expressions or twitching, which might reveal an individual's brief expression of glee or guilt over delivering a deceptive response.[228] For example, Converus' EyeDetect technology uses an infrared camera to record an individual's eye behaviors, measuring pupil dilation, eye movements, blinks, and reaction times; an algorithm then analyzes the results to detect any deception.[229]

Although the quest to perfect a lie detector throughout human history is not a uniquely American phenomenon,[230] the widespread use and reverent cultural attachment to lie detection technology in the United States is notably distinct.[231] In the early

analysis technology is also being used to fight fraud by detecting exaggerations and using a combination of markers, such as pauses, which may indicate deception or providing of false information. *See* Charu Mishra & Aarti Mehta Sharma, *A Review Paper on Voice Analytics*, 5 INT'L J. SCI. TECH. & MGMT. 247, 253 (2016) (detailing one application of voice analytics in the financial sector, which is identifying intentional deception and highlighting research on verbal and nonverbal cues, such as tone of voice: "[o]ne such vocal marker of deception (vocal marker is a type of non-verbal cue) is Cognitive dissonance which is a state of psychological arousal and discomfort occurring when an individual takes actions that contrast with a belief, such as cheating while believing one to be honest"); John McCormick, *What AI Can Tell from Listening to You*, WALL ST. J. (Apr. 1, 2019, 9:43 PM), https://www.wsj.com/articles/what-ai-can-tell-from-listening-to-you-11554169408; Mark Memmott, *Is That CEO Being Honest? Tone of Voice May Tell a Lot*, WBUR (Feb. 2, 2012), https://www.wbur.org/npr/146288038/is-that-ceo-being-honest-tone-of-voice-may-tell-a-lot [https://perma.cc/Y4Cm-RHQM].

228. *See* Katwala, *supra* note 201.

229. *See Eye Detect*, *supra* note 222; Mark Harris, *An Eye-Scanning Lie Detector Is Forging a Dystopian Future*, WIRED (Dec. 4, 2018, 7:00 AM), https://www.wired.com/story/eye-scanning-lie-detector-polygraph-forging-a-dystopian-future/. The technology is being used widely in the privacy and public sector:

> EyeDetect[] has been used by FedEx in Panama and Uber in Mexico to screen out drivers with criminal histories, and by the credit ratings agency Experian, which tests its staff in Colombia to make sure they aren't manipulating the company's database to secure loans for family members. In the UK, Northumbria police are carrying out a pilot scheme that uses EyeDetect to measure the rehabilitation of sex offenders. Other EyeDetect customers include the government of Afghanistan, McDonald's and dozens of local police departments in the US.

Katwala, *supra* note 201.

230. *See* Alder, *supra* note 208, at 491 n.12; Trovillo, *supra* note 208, at 850–54.

231. *See* ALDER, *supra* note 202, at xiv ("[N]o country other than the United States has made use of the [lie detector] technique to any significant degree."). Historians have noted that in the early twentieth century, the United States set itself on a different trajectory from the rest of the world in its embrace of the latest lie detector technology (the polygraph). *See id.* at xiii–xiv; *cf.* Alder, *supra* note 208, at 491. The countries that regularly use polygraph tests tend to have far fewer examiners, and, as one historian noted, close security relationships with the United States. *Id.* at 491 n.12. By the 1960s, when use of the polygraph was already widespread in the United States, other countries—such as Japan, China, Israel, and Korea—were just starting their own programs. *See* Dona Grubin & Lars Madsen, *Lie Detection and the Polygraph: A Historical Review*, 16 J. FORENSIC PSYCHIATRY & PSYCHOL. 357, 362 (2005). Unlike the United States, use of the polygraph never took root in the United Kingdom. *Id.* at 365. In the 1980s, the British Psychological Society (BPS) published a report concluding the "polygraph procedures were insufficiently standardised [sic] to be acceptable as a scientific test, and stressed the limited amount of empirical evidence of its accuracy and reliability." *Id.* Historians are not entirely certain how big of an impact the BPS report ultimately had, but the British criminal justice system or intelligence services never embraced the technology. *Id.* But this too may be changing; interest in the technology is growing the United Kingdom, particularly within the past decade. *See* Katwala, *supra* note 201. For example, since 2014, lie detectors have been used on sex offenders in the United Kingdom. *Id.* But recently, there is growing concern in the United Kingdom and throughout Europe over the use of lie detection

twentieth century, many Americans became fixated with curtailing "criminal disorder and political corruption" and seeking a pathway toward a more "honest society."[232] In pursuit of these goals, the lie detector promised to "pierce the human opacity," which allowed disfavored behavior to flourish.[233] In 1921, John Larson invented the first design of the polygraph test.[234] By the middle of the century, lie detectors were in widespread use increasing dramatically by the 1980s.[235] From federal and local government agencies to law enforcement to banks and factories, polygraphs were being used to screen employees and investigate crimes.[236] Employers wielded the technology as a means to identify thieves and peer into the "deepest recesses of the [human] psyche."[237] By 1985, an estimated 2 million job applicants and employees were forced to take a polygraph test, a threefold increase over the previous decade.[238] A hostile social climate toward drug use and growing concern of employee theft, among other concerns, prompted many employers to conduct routine testing and to screen job applicants and employees to measure honesty or propensity for falsehoods.[239] A survey of U.S. corporations revealed employers used lie detectors primarily to assess employee honesty and

technologies at airports. *See* Ryan Gallagher & Ludovica Jona, *We Tested Europe's New Lie Detector for Travelers—and Immediately Triggered a False Positive*, INTERCEPT (July 26, 2019, 5:00 AM), https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/ [https://perma.cc/98D7-DSX4]; Rob Picheta, *Passengers to Face AI Lie Detector Tests at EU Airports*, CNN (Nov. 2, 2018), https://www.cnn.com/travel/article/ai-lie-detector-eu-airports-scli-intl/index.html [https://perma.cc/8H7W-X9GR]. A deeper exploration of the cultural and political differences, and varied conceptions of human rights and privacy, that could explain why there was selective adoption of lie detection technologies around the world is worth further consideration; however, such an analysis is beyond the scope of this Note.

232. *See* ALDER, *supra* note 202, at xi.

233. *Id.* At this time, disfavored, "secret" behavior in society included adultery, murder, conspiracy, and espionage, which all reflected a capacity to deceive and betray one's fellow citizens. *See id.*

234. William Grimes, *The Tangled Web of the Truth Machine*, N.Y. TIMES (Mar. 2, 2007), https://www.nytimes.com/2007/03/02/books/02book.html.

235. *See* GAIL MCCALLION, ECON. DIV., CONG. RESEARCH SERV., POLYGRAPH TESTING: EMPLOYEE AND EMPLOYER RIGHTS 1–2 (1987). A 1978 study conducted by researchers at Wichita State University confirmed that, within the past decade, "one-fourth of all major corporations" were regularly using lie detectors. *See* John A. Belt & Peter B. Holden, *Polygraph Usage Among Major U.S. Corporations*, PERSONNEL J., Feb. 1978, at 80, 82.

236. *See* Mark Harris, *The Lie Generator: Inside the Black Mirror World of Polygraph Job Screenings*, WIRED (Oct. 1, 2018, 7:00 AM), https://www.wired.com/story/inside-polygraph-job-screening-black-mirror/. Throughout the first half of the twentieth century, the administering of lie detector tests was conducted with little oversight. *Id.* Polygraphs were often used to intimidate and stifle dissent, particularly during the Cold War when the "tests were used to target left-wingers and homosexuals in government agencies." *Id.* During the 1940s and 1950s, this weaponized mass use of the tests was intended to measure disloyalty in an explicitly ideological and political context. *See* Alder, *supra* note 208, at 515–16; Dwight MacDonald, *The Lie-Detector Era*, REPORTER, June 8, 1954, at 10, 16–18.

237. Grimes, *supra* note 234.

238. MCCALLION, *supra* note 235, at 1.

239. *See id.* at 2. In 1988, employee theft in the United States was *conservatively* estimated to cost businesses between $15 billion to $25 billion annually, with researchers noting that the potential losses to be closer to $56 billion per year. William T. Dickens, Lawrence F. Katz, Kevin Lang & Lawrence H. Summers, *Employee Crime and the Monitoring Puzzle*, 7 J. LAB. ECON. 331, 332 & n.1 (1989); *see* Terry Morehead Dworkin, *Protecting Private Employees from Enhanced Monitoring: Legislative Approaches*, 28 AM. BUS. L.J. 59, 61 & n.10 (1990).

loyalty, to verify employment applications, and to investigate theft or other irregularities.[240] For example, Coors brewery developed a preemployment screening program in the 1970s using polygraphs tests to help "ensure 'that the applicant does not want the job for some subversive reason such as sabotaging our operation.'"[241]

B. LIE DETECTORS: MYTHS AND CRITICISMS

As a society, we instinctively gravitate toward the use of lie detectors "because we long for a form of justice that is swift, certain, and non-coercive . . . [and] because we expect that science *can* and *will* pierce the veil of earthly appearances."[242] But growing opposition to the unfettered uses of lie detectors has sparked vigorous debate over the merits and consequences of such technological shortcuts. The criticisms of lie detectors fall into two camps: (1) concerns over the scientific validity of the testing methodology, and (2) concerns over individual privacy and the threat to human dignity.

1. Lack of Scientific Validity

Despite the popularity of lie-detection technology, its accuracy has long been viewed with skepticism by the scientific community.[243] Although there is general agreement that the tests can accurately measure physiological changes in response to questioning, the scientific community disagrees on whether the results can be correlated with the truth or deception.[244] In fact, the American Psychological Association (APA), the leading scientific and professional organization of psychologists in the United States,[245] issued a rebuke of lie detectors declaring that there is no evidence that the technology can accurately determine deception.[246] First, the APA identified an underlying theoretical problem with lie detectors: "There is no evidence that any pattern of physiological reactions is unique to deception."[247] According to Dr. Leonard Saxe, a well-known psychologist and lie detector expert at Brandeis University, "[t]here's no unique physiological sign of deception. And there's no evidence whatsoever that the things

240. *See* Belt & Holden, *supra* note 235, at 82.

241. Grubin & Madsen, *supra* note 231, at 362. The Coors program actually represented a good "example of how the polygraph could be, and [were], misused." *Id.* Despite the specific concerns expressed by the company, prospective employees were asked questions that suggested other interests: "What are your sexual preferences?" or "How often do you change your underwear?" and "Have you ever done anything with your wife that could be considered immoral?" *Id.* at 363.

242. Eleanor Cummins, *Polygraph Tests Don't Work as Lie Detectors and They Never Have*, POPULAR SCI. (Sept. 20, 2018), https://www.popsci.com/polygraph-test-science/ (emphasis added) (quoting Ken Alder).

243. *See* Harris, *supra* note 236.

244. *See* MCCALLION, *supra* note 235, at 3.

245. *About APA*, AM. PSYCHOL. ASS'N, https://www.apa.org/about/ [https://perma.cc/49EF-KFV6] (last visited Mar. 20, 2021).

246. *See The Truth About Lie Detectors*, *supra* note 203.

247. *Id.*; *see* Leonard Saxe, *Science and the CQT Polygraph: A Theoretical Critique*, 26 INTEGRATIVE PHYSIOLOGICAL & BEHAV. SCI. 223, 227–28 (1991).

the polygraph measures—heart rate, blood pressure, sweating, and breathing—are linked to whether you're telling the truth or not."[248] Moreover, if a lie detector test is presumptively intended to measure anxiety, a paradox emerges that may skew the results.[249] An honest person may actually be nervous in their response, whereas a dishonest person may be calm.[250] As such, the more comfortable or practiced a person is at lying, the less anxious they are likely to be.[251] This has led many experts to conclude a polygraph, or similar lie detection technology, is probably beatable by people with training.[252]

Second, the APA found that research on lie detectors does not separate out the "placebo-like effects," or the individual's subjective belief in the accuracy of the test, from an analysis of the correlation between deception and their physiological response.[253] Even if the test may *appear* to detect deception, the phenomena could be better explained by the fact the individual—who believes the technology works and therefore, thinks they are about to be caught—confesses or becomes anxious under questioning.[254] As Dr. Saxe explained, "[i]f the examiner does the theater well, and tricks the subject into believing that his or her lies can be detected, they might confess."[255] Therefore, it is plausible the measurable physiological response being detected is feelings of distress or fear and not deception.

The view that lie detectors are inaccurate and lack sufficient reliability is supported by multiple studies commissioned by the federal government. In 1965, the U.S. House Committee on Government Operations conducted an empirical review of the polygraph.[256] The final report issued a damning verdict: "There is no lie detector. . . . People have been deceived by a myth that a metal box in the hands of an investigator can detect truth or falsehood."[257] This view has been replicated by subsequent scientific publications.[258] In 1987, the House Report on the EPPA noted: "For more than 20 years Congress has been interested in the validity of these tests and every study done since 1963 for the United States Congress has found that there is no scientific basis for polygraphs as lie detectors."[259] Even forty years after its initial report, the federal government remains just as skeptical of the technology. In 2003, a comprehensive report published by the National Research Council concluded: "Almost a century of research in

248. Stromberg, *supra* note 206.
249. *See id*.
250. *Id*.
251. *Id*.
252. COMM. TO REVIEW THE SCI. EVIDENCE OF THE POLYGRAPH, *supra* note 199, at 215–16.
253. *The Truth About Lie Detectors*, *supra* note 203.
254. *Id*.
255. German Lopez, *Why Police Use Lie Detectors—Even Though the Tests Are Bogus*, VOX (Oct. 18, 2015, 11:00 AM), https://www.vox.com/2015/10/18/9560391/polygraphs-wrong-police [https://perma.cc/VV4F-LZ49].
256. H.R. REP. NO. 100-208, at 7 (1987).
257. *Id*.
258. Cummins, *supra* note 242.
259. H.R. REP. NO. 100-208, at 6.

scientific psychology and physiology provides little basis for the expectation that a polygraph test could have extremely high accuracy."[260] Notably, the report ruled out the potential for advances in the technology to ameliorate these concerns, concluding "this inherent ambiguity of the physiological measures used in the polygraph suggests that further investments in improving polygraph technique and interpretation will bring only modest improvements in accuracy."[261] In other words, the entire theory underpinning the use of all lie detectors—that there exists some common physiological indicator of deception—is not supported by science.

Moreover, the availability of research validating the accuracy of lie detectors is slim when venturing beyond specific-incident questions.[262] The lack of research on the varied contexts in which lie detectors are used is highly problematic. The accuracy of lie detectors is highly context specific, and, depending on the circumstances, a different theory and relevant body of research is applicable.[263] Further, acceptable research findings that focus on event-specific investigations should not be extrapolated to general screening purposes, such as preemployment screening in the absence of a known incident or allegation, where almost no research has been conducted.[264] In fact, the relevance of specific-incident research to preemployment screening polygraphs is "highly questionable because such [general] screening involves inferences about future behavior on the basis of polygraph evidence about past behaviors that are probably quite different in kind."[265]

The lack of scientific validity, however, did not deter the use of lie detectors. In the employment context, polygraphs and other lie detector tests were valued far more as a "business product" than as an effective or accurate scientific technique.[266] Employers exploited the "scientific aura" of the tests as cover for the continued use of the technology "to shape their workforce."[267] The applied psychologists developing these tests also had an economic incentive to promote their "'science' to industry."[268] This phenomenon of selling science followed a playbook: listing researchers' degrees from prestigious academic institutions; manipulating the presentation of results; taking advantage of the public with claims of

260. COMM. TO REVIEW THE SCI. EVIDENCE OF THE POLYGRAPH, *supra* note 199, at 212 (emphasis omitted).

261. *Id*. at 2.

262. *See The Truth About Lie Detectors*, *supra* note 203.

263. *See id*.

264. *See* COMM. TO REVIEW THE SCI. EVIDENCE OF THE POLYGRAPH, *supra* note 199, at 215–16; *The Truth About Lie Detectors*, *supra* note 203.

265. COMM. TO REVIEW THE SCI. EVIDENCE OF THE POLYGRAPH, *supra* note 199, at 216 (emphasis omitted).

266. *Cf.* Craig Haney, *Employment Tests and Employment Discrimination: A Dissenting Psychological Opinion*, 5 INDUS. REL. L.J. 1, 6 (1982); George Allan Hanson, *To Catch a Thief: The Legal and Policy Implications of Honesty Testing in the Workplace*, 9 LAW & INEQ. 497, 503 (1991) (quoting Haney, *supra*).

267. *See* Harris, *supra* note 236.

268. Hanson, *supra* note 266, at 502.

"reliability" to imply accuracy; and other shady sales techniques.[269] It seemed the lack of credible science was almost irrelevant. The use of lie detectors remained popular because employers knew people *believed* the lie detector to be effective.[270] Accordingly, "the real power of [the polygraph] was in convincing people that it works."[271] By the end of his life, Larson expressed despair over his invention, writing: "Beyond my expectation, through uncontrollable factors, this scientific investigation became for practical purposes a Frankenstein's monster."[272]

2. Privacy Violations and Human Dignity

In addition to its lack of scientific validity, lie detectors pose a broader threat to the privacy and dignity of individuals.[273] These issues were prominently raised during public debate over the adoption of the EPPA. In support of the legislation, Representative Cornelius E. Gallagher (D-NJ) summarized his objections to the use of lie detectors as follows:

> In my opinion, lie detector tests constitute an insidious search of the human mind and are a breach of the most fundamental of human rights. They provide a vehicle of excursion into the most private recesses of the human mind. Even if the polygraph testing was trustworthy, there is still no possible justification for such "mental wiretapping." . . . Its use upon Federal employees and job applicants is *especially repugnant* and should be stopped now—today.[274]

The heightened concern over the use of lie detectors in a general screening context can be explained by the inherent motivations for using a lie detector in these situations and the sweeping conclusions made about an individual based on the results. In some circumstances, a polygraph administrator would presumably be interested in the *content* of the subject's answers, particularly with regard to specific incidents in an internal company investigation or criminal investigation.[275] However, where a test is used to prescreen individuals for jobs and security clearances, the administrator is more interested in the inferences that can be made about the subject's *character* as a predictor of future performance based on responses about past acts.[276] In many ways, broadly probing questions, untethered to a specific incident and used to make sweeping generalizations about an individual's propensity to be an honest or dishonest person, are far more problematic from a privacy and human dignity perspective than discrete determinations concerning past offenses or acts of dishonesty.[277] For example, critics have argued the

---

269. *See id.* at 503 n.25 (citing Paul R. Sackett, Laura R. Burris & Christine Callahan, *Integrity Testing for Personnel Selection: An Update*, 42 PERSONNEL PSYCHOL. 491, 523 (1989)).

270. Katwala, *supra* note 201.

271. *Id.* (quoting Dr. Andy Balmer).

272. *Id.* (quoting John Larson).

273. *See* Dworkin, *supra* note 239, at 64–65; Donald H. J. Hermann III, *Privacy, the Prospective Employee, and Employment Testing: The Need to Restrict Polygraph and Personality Testing*, 47 WASH. L. REV. 73, 75 (1971).

274. H.R. REP. NO. 89-198, at 43 (1965) (emphasis added).

275. *See* COMM. TO REVIEW THE SCI. EVIDENCE OF THE POLYGRAPH, *supra* note 199, at 23–24.

276. *See id.* at 23.

277. *See* Hermann III, *supra* note 273, at 85–87.

preemployment screen denies an individual the opportunity for reformation from prior past acts, which may not be a reliable indicator of future conduct.[278]

Representative Gallagher's concerns were similarly reflected in a growing body of literature by psychologists, philosophers, and privacy scholars at the time, who argued that all lie detectors posed significant privacy concerns. A common law right to privacy was first recognized by legal giants, Samuel D. Warren and Louis Brandeis, in their famous *Harvard Law Review* essay *The Right to Privacy*.[279] Seventy years later, just as the debate over lie detector tests started to gain traction in Congress, William Prosser published his seminal law review article, *Privacy*, which defined four distinct privacy torts,[280] and by and large, established a sense of legitimacy to privacy law that was previously lacking.[281] However, in the debate over preemployment screens, the "right to privacy" conceptualized by policymakers was not limited to these narrow categories, rather it was considered the broader "*inviolate*" *right of privacy* as theorized by Warren and Brandeis.[282] According to Warren and Brandeis, a privacy tort would safeguard every individual's inherent right to determine "to what extent [their] thoughts, sentiments, and emotions shall be communicated to others."[283] In other words, the law should empower individuals to determine "whether that which is [theirs] shall be given to the public."[284] A lie detector poses a direct threat to that right. After all, the fundamental purpose of a lie detector is to discover the inner thought processes of others to invade the "secret, private and invisible thought processes" in pursuit of the "truth."[285]

Deception, however, is a perfectly normal part of our everyday life.[286] Any burden on this function necessarily compromises an important part of an individual's personal autonomy—the capacity to withhold information from discovery by the outside world.[287] Distorting the truth and keeping secrets is a skill developed over a lifetime. The majority of people first learn to and have the capacity to

278. *Id.* at 85.

279. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198, 206 (1890).

280. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960) (dividing tort privacy into four distinct torts: (1) intrusion upon seclusion; (2) public disclosure of private fact; (3) false light publicity; and (4) appropriation of name or likeness for commercial gain).

281. *See* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1888 (2010).

282. *See, e.g.*, Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1807 (2010); *see also* Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 963–64, 973–77 (1964) (proposing "a general theory of individual privacy," distinguished from Prosser's "four distinct torts," in order to clarify confusion concerning the interest that the "right to privacy" protects, which is of "utmost significance because in our own day scientific and technological advances have raised the spectre [sic] of new and frightening invasions of privacy" (referencing surveillance devices, such as wiretaps, and specifically, lie detector tests)).

283. *See* Warren & Brandeis, *supra* note 279, at 198.

284. *Id.* at 199.

285. *See* Gibson, *supra* note 214, at 67.

286. VRIJ, *supra* note 202, at 11.

287. *See* Hermann III, *supra* note 273, at 128.

deceive as toddlers, often between the ages of four and five,[288] or even as early as age two.[289] Although this development often comes as a shock to a doting parent, the capacity to deceive marks an important milestone in our cognitive development,[290] a "decisive further step into separateness and autonomy."[291]As renowned poet Joseph Brodsky observed, "the real history of consciousness starts with one's first lie."[292] Thus, to deceive is fundamentally human.[293]

But the reasons people may lie, or choose to withhold information, does not necessarily indicate that they are of an immoral character, or fundamentally dishonest. By adulthood, many, if not all of us are prolific stretchers of the truth. Research reveals the average person will hear upwards of two hundred lies a day.[294] As one survey found, however, a person may tell only two "important" lies a day—if at all.[295] Many of these lies are harmless, so-called "white lies," or inconsequential niceties that may define a typical social interaction.[296] A common misconception is that people lie only to gain material advantage or avoid

288. Marjorie Rhodes, *When Children Begin to Lie, There's Actually a Positive Takeaway*, NPR (Oct. 2, 2017, 10:11 AM), https://www.npr.org/sections/13.7/2017/10/02/552860553/when-children-begin-to-lie-theres-actually-a-positive-takeaway [https://perma.cc/VY6P-UE8C].

289. Alex Stone, Opinion, *Is Your Child Lying to You? That's Good*, N.Y. TIMES (Jan. 5, 2018), https://www.nytimes.com/2018/01/05/opinion/sunday/children-lying-intelligence.html?action=click&module=RelatedLinks&pgtype=Article.

290. Rhodes, *supra* note 288.

291. J.A. BARNES, A PACK OF LIES: TOWARDS A SOCIOLOGY OF LYING 8 (John Dunn, Jack Goody & Geoffrey Hawthorn eds., 1994) (quoting American psychiatrist, Joseph Smith) (discussing the importance of children lying). Similarly, another group of psychiatrists argued: "Lying becomes an important, perhaps essential mechanism by which the child can test the limits of his or her own ego boundaries in order to define and establish autonomy." *Id.*

292. *Id.* (quoting poet Joseph Brodsky).

293. ALDER, *supra* note 202, at xii. This behavior may seem in tension with the widely shared view that honesty and integrity are positive social virtues, or indicative of strong leadership traits. *See, e.g.*, Emma Edelman Levine, Navigating the Tension Between Benevolence and Honesty: Essays on the Consequences of Prosocial Lies 1 (Jan. 1, 2016) (unpublished Ph.D. dissertation, University of Pennsylvania), https://repository.upenn.edu/cgi/viewcontent.cgi?article=3628&context=edissertations [https://perma.cc/EHJ7-ZB2K]; *see also* Roger C. Mayer, James H. Davis & F. David Schoorman, *An Integrative Model of Organizational Trust*, 20 ACAD. MGMT. REV. 709, 719 (1995) (recognizing that integrity is an essential characteristic of trustworthy persons); Linda K. Treviño, Gary R. Weaver & Scott J. Reynolds, *Behavioral Ethics in Organizations: A Review*, 32 J. MGMT. 951, 952 (2006) (defining honesty as a "minimal moral standard"). However, social science experts have identified conflicts between honesty and other moral values, such as kindness, benevolence, and compassion. Levine, *supra*, at 1–2. Thus, there is a trade-off that individuals make in balancing complete honesty with benevolence, and usually, these decisions are far from black-and-white binary choices. *See id.*

294. Katwala, *supra* note 201.

295. Wiseman, *supra* note 200.

296. *See* VRIJ, *supra* note 202, at 12. "White lies" may involve common responses—such as, "I think you performed really well," or "of course you will soon find a new boyfriend"—or they may include:

> A man says that he is pleased with his birthday presents, although in fact they are not what he really wanted; the host receives compliments about his cooking, although the food was not really good; and a schoolgirl watching TV tells her dad that she has finished her homework, although she has not actually yet started it.

Id. at 11–12, 20.

punishment, but people lie for a variety of reasons.[297] A person may lie to maintain a particular image that reflects how *they* wish to be seen by others.[298] A person may lie to avoid embarrassment or disclosing any personal failures or mistakes.[299] Or a person may lie to avoid hurting the feelings of others or to make someone feel better about themselves.[300] All of these purposes are certainly legitimate. Our capacity to lie is a prerequisite for navigating the complexity of daily social interactions and controlling how we choose to present ourselves to the world.[301] By attempting to extort one's "uncontrolled" responses, the lie detector invades this realm of personal autonomy, and thus, poses a critical threat to an individual's privacy, integrity, and dignity.[302]

C. A FEDERAL RESPONSE: THE EMPLOYEE POLYGRAPH PROTECTION ACT (EPPA)

Beginning in the mid-1960s, Congress began to earnestly debate the increasingly widespread use of lie detector tests, subsequently causing almost fifty bills to be introduced "[f]rom the 93rd Congress through the 100th."[303] In 1988, after decades of attempts to coordinate a federal response, Congress finally succeeded in passing the Employee Polygraph Protection Act (EPPA), clarifying its intent "[t]o prevent the denial of employment opportunities by prohibiting the use of lie detectors by employers."[304] Prior to the EPPA, "[a]pproximately half of the states had passed legislation severely limiting the use of lie detectors."[305] The restrictions ranged from partial or complete bans to procedural safeguards, such as licensing requirements for administrators or limiting the types of questions.[306] However, the lack of uniform rules provided an opportunity for employers and examiners to circumvent protections by conducting the test in a neighboring state with more lenient laws.[307] With the creation of the EPPA, Congress intervened to establish a federal standard.

Specifically, the EEPA prohibits the use of lie detectors by private employers, not only at the time of hire, but also during the course of employment.[308]

297. *See id.* at 18.

298. *See id.* at 18–19.

299. *Id.* Often, the context—or to *whom* we tell lies—is most telling in terms of the regularity, type, and perceived social acceptability of the lie. *See id.* at 25–26. Studies have revealed that job applicants regularly mislead employers, for example, by exaggerating their qualities or skills when applying, such as proclaiming more experience or a higher past salary. *Id.* In addition, a national survey found that more than eighty percent of people have lied to secure a job. Wiseman, *supra* note 200.

300. *See* VRIJ, *supra* note 202, at 19.

301. *See id.* at 18–19; Rhodes, *supra* note 288.

302. *See* Hermann III, *supra* note 273, at 153–54.

303. S. REP. NO. 100-284, at 44 (1988).

304. *See* Employee Polygraph Protection Act of 1988, Pub. L. No. 100-347, 102 Stat. 646 (codified as amended in scattered sections of 29 U.S.C).

305. Dworkin, *supra* note 239, at 64 (footnote omitted); *see* IRA MICHAEL SHEPARD & ROBERT L. DUSTON, WORKPLACE PRIVACY: EMPLOYEE TESTING, SURVEILLANCE, WRONGFUL DISCHARGE, AND OTHER AREAS OF VULNERABILITY 32–33 (1987).

306. *See* SHEPARD & DUSTON, *supra* note 305, at 32–33; Dworkin, *supra* note 239, at 64.

307. S. REP. NO. 100-284, at 43.

308. 29 U.S.C. § 2002 (2018).

Specifically, the law provides: "[I]t shall be unlawful for any employer . . . directly or indirectly, to require, request, suggest, or cause any employee or *prospective* employee to take or submit to any lie detector test."[309] The EPPA also bars employers from "us[ing], accept[ing], refer[ing] to, or inquir[ing]" about the "results of any lie detector test of any employee or prospective employee."[310] An employer may not "discharge, discipline, discriminate against in any manner, or deny employment or promotion to, or threaten to take any such action against—any employee or prospective employee who refuses, declines, or fails to take or submit to any lie detector test," or against "any employee or prospective employee on the basis of the results of any lie detector test."[311]

Based on this language, the EPPA not only prohibits the administration of lie detector tests, but also protects individuals from related retaliation by an employer. The EPPA defines a "lie detector" as:

> [A] polygraph, deceptograph, voice stress analyzer, psychological stress evaluator, or any other similar device (whether mechanical or electrical) that is used, or the results of which are used, for the purpose of rendering a diagnostic opinion regarding the honesty or dishonesty of an individual.[312]

The Department of Labor is charged with enforcement of the EPPA and may seek injunctive relief to restrain violations of the statute.[313] An employer who violates any provision of the EPPA may be assessed a civil penalty of $10,000 per violation.[314] The EPPA also provides for a private right of action by an aggrieved employee or prospective employee to recover legal or equitable relief, including reasonable costs and attorneys' fees.[315]

Even though Congress debated lie detectors' lack of scientific validity, the statute's structure and legislative history illustrates that lawmakers were primarily concerned with the broader threat posed by lie detectors to individual privacy and overall human dignity.[316] First, Congress declined to impose a complete prohibition on the use of lie detectors, a policy position that would have been most logical if lawmakers had no faith in the validity of the technology.[317] Instead, the statute exempts government employers entirely[318] and further extends this carve out to

309. *Id.* at § 2002(1) (emphasis added).
310. *Id.* at § 2002(2).
311. *Id.* at § 2002(3)(A)–(B) (enumeration omitted).
312. *Id.* at § 2001(3).
313. *Id.* at § 2005(b).
314. *Id.* at § 2005(a)(1) ("[A]ny employer who violates any provision of this chapter may be assessed a civil penalty of not more than $10,000."); Onder & Brittan, *supra* note 197, at 485.
315. *Id.* at § 2005(c)(1), (3). The statute of limitations for filing a claim is three years after the date of the alleged violation. *Id.* at § 2005(c)(2). Although beyond the scope of this Note, Congress could strengthen private enforcement of the EPPA by allowing private litigants to recover statutory damages, as is available in a public enforcement action, in addition to other legal and equitable relief, as well as reasonable costs, including attorney's fees. *See id.* at § 2005(c)(1), (3).
316. *See* Dworkin, *supra* note 239, at 64–65.
317. *See* 29 U.S.C. § 2006(a)–(f).
318. *Id.* at § 2006(a).

private sector experts, consultants, or contractors engaging in national defense or counterintelligence operations.[319] Second, the EPPA still allows private employers limited use of lie detectors, although the type of technology is limited to a polygraph test, and employers must satisfy heightened quasi-procedural due process requirements.[320] Paradoxically, although Congress expressed deep concerns about the efficacy of the technology, the EPPA permits the use of lie detectors in circumstances in which the accuracy of the results is of paramount importance: national defense, security, and legitimate ongoing investigations.

The EPPA is, therefore, intended to address the other privacy concerns raised by the use of lie detectors. A review of the legislative history shows the framework of the EPPA reflects a compromise between the legitimate business interests of employers and the *privacy interests* of employees.[321] One of the original cosponsors of the bill, Senator Orrin Hatch, described the EPPA's exemptions and limitations as "an equitable compromise of several important, but competing interests."[322] Similarly, Representative James Jeffords explained in debate on the House floor that, "[s]ome of my colleagues would like to ban the use of polygraphs entirely," whereas others "would like their use entirely unfettered."[323] However, the ultimate compromise "outlaw[s] the vast majority of tests, while prudently restricting those remaining."[324]

III. AFFECT RECOGNITION AND THE EPPA: WHAT'S OLD IS NEW AGAIN

After the EPPA was signed into law, the contours of the employer–employee relationship changed dramatically. The EPPA, however, did not "signal the end" of employers' interest in evaluating the honesty and integrity of current or prospective

319. *Id.* at § 2006(b)(1)–(2) (defining the "[n]ational defense and security exemption").

320. *Id.* at § 2006(d). Under the "[l]imited exemption for ongoing investigations," private sector employers are permitted to use *polygraph tests* for "ongoing investigations" if there is reasonable suspicion that the employee is culpable for any economic loss endured by the employer. *Id.* at § 2006(d)(1), (3). This limited exception is critical because polygraphs are only one type of lie detector. *See id.* at § 2001(3). To satisfy the exemption, the employer must provide an employee with a statement, which

> (A) sets forth with particularity the specific incident or activity being investigated and the basis for testing particular employees, (B) is signed by a person (other than a polygraph examiner) authorized to legally bind the employer, (C) is retained by the employer for at least 3 years, and (D) contains at a minimum—(i) an identification of the specific economic loss or injury to the business of the employer, (ii) a statement indicating that the employee had access to the property that is the subject of the investigation, and (iii) a statement describing the basis of the employer's reasonable suspicion that the employee was involved in the incident or activity under investigation.

Id. at § 2006(d)(4)(A)–(D)(iii).

321. *See* Joseph M. Pellicciotti, *The Employee Polygraph Act of 1988: A Focus on the Act's Exemptions and Limitations*, 51 LOY. L. REV. 911, 914 (2005) (discussing floor statements made by Senator Orin Hatch and Representative James Jeffords).

322. 134 Cong. Rec. 2,711 (1988) (statement of Sen. Hatch).

323. *Id.* at 13,064 (statement of Rep. James Jeffords).

324. *Id.*

employees.[325] As this Part explains, employers simply found new ways to screen prospective applicants, namely *written* integrity tests, that did not implicate the prohibitions of the EPPA. But in an attempt to modernize these tests and update screening procedures using technological advancements in AI, this Part argues that employers have forgotten their history. First, the advent of AI-powered video-interviewing screens has seen a return of familiar analytical shortcuts—relying on unproven correlations between nonverbal and physiological responses to determine the fit of a candidate. Second, these screens accelerate the privacy harms of lie-detection technology that were debated by Congress in the adoption of the EPPA. Third, the use of affect-recognition video-interviewing screens are expressly prohibited by the EPPA.

A. FROM WRITTEN "INTEGRITY TESTS" TO AI-POWERED AFFECT SCREENING

Notably absent from the EPPA's broad prohibitions are restrictions on "paper and pencil" integrity or "honesty" tests.[326] A passage that would have incorporated such tests was deleted from the final text of the EPPA, an intentional concession during conference negotiations.[327] As a result, employers shifted their screening operations from polygraph tests to the conceptually similar written integrity tests, with the added benefit of substantially reduced cost and legal liability.[328] The development and administration of written tests quickly became a "multimillion dollar industry."[329] Both polygraph and written integrity tests perform essentially the same function,[330] but by using different methods to detect deception: polygraphs presume a physiological "lie response," whereas integrity tests presume "dishonesty is a stable trait that can be" elucidated by clever questioning.[331] Many employers used integrity testing as an alternative to polygraph tests, and the written test was thought of as an interchangeable substitute.[332] For example, they both attempt to measure increasingly unprecise constructs. Many integrity tests evolved from overt testing for "theft" to broader measurements of "counterproductive behavior," of which theft is certainly one example.[333]

---

325. Hanson, *supra* note 266, at 498.

326. H.R. REP. NO. 100-659, at 11 (1988) (Conf. Rep.).

327. H.R. REP. NO. 100-208, at 11 (1987) ("In deciding to strike the language from the definition, the Committee concludes that this issue should be handled separately from the lie detector.").

328. *See* Hanson, *supra* note 266, at 498–99, 518; Leonard Saxe, *Detection of Deception: Polygraph and Integrity Tests*, 3 CURRENT DIRECTIONS PSYCHOL. SCI. 69, 70 (1994). Around the time of the EPPA's passing, integrity tests costs roughly eight dollars per test, whereas polygraph tests usually cost an estimated forty to fifty dollars per polygraph. David Elsner, *Hiring Tests Make Policy of Honesty*, CHI. TRIB., Aug. 19, 1986, at B1.

329. Kurt H. Decker, Commentary, *Honesty Tests—A New Form of Polygraph?*, 4 HOFSTRA LAB. L. J. 141, 144 (1986).

330. Hanson, *supra* note 266, at 498–99.

331. Saxe, *supra* note 328, at 71.

332. *See* Byford, *supra* note 3, at 331, 335.

333. OFFICE OF TECH. ASSESSMENT, U.S. CONGRESS, THE USE OF INTEGRITY TESTS FOR PRE-EMPLOYMENT SCREENING 33 (1990). Honesty tests are classified into two types: (1) "overt" or straightforward questions of dishonesty or past dishonest acts ("How often do you tell the truth?"), and (2) "veiled-purpose" questions that elicit dishonest propensities through seemingly unrelated topics that

Some commenters have questioned whether the EPPA, or similar state law equivalents would, in fact, prohibit written integrity tests.[334] After all, the written tests raise similar ethical and privacy concerns as more traditional lie detectors, and the types of questions written test the level of employees or prospective employees, which still constitute an unseemly "intrusion into personal thoughts, attitudes, and beliefs" of an individual.[335] In this regard, a prohibition on honesty tests is "within the 'spirit' and 'intent'" of legislation regulating the using of polygraphs.[336] These paper-and-pencil tests could arguably be understood as merely a polygraph test in disguise.

These arguments, however, are unconvincing. The House Conference Report explicitly said such tests were *not* intended to be included within the definition of "lie detector."[337] In addition, written integrity tests are distinguishable from lie detector tests in notable ways, such as written tests constitute avoidable privacy invasions, which would explain their exclusion from the statute. In adopting the EPPA, Congress indicated its concern with *unavoidable* privacy invasions.[338] Because lie detectors aim to measure involuntary or noncommunicative acts, individuals can never meaningfully consent to giving a response—the body is expected to betray the intended communication.[339] In contrast, an individual could theoretically skip a question or refrain from answering in a written exam. Therefore, the privacy intrusion in the context of written testing is far more limited.

Given the distinguishing characteristics of written integrity testing, modern AI-powered affect testing is closer to traditional lie detector testing. The key is whether the type of test considers involuntary communications. In the employment context, as online hiring has become standard practice across almost every

---

correlate with honesty ("On the average, [h]ow often during the week do you go to parties?"). *Id.* at 31–32, 35.

334. *See e.g.*, Decker, *supra* note 329, at 149 ("[A] paper and pencil honesty test could be viewed as a 'mechanical lie detector test' under Pennsylvania's anti-polygraph statute."). The EPPA—adopted after the Pennsylvania statute—includes similar language regarding "mechanical" lie detection technology. *See* Employee Polygraph Protection Act of 1988, 29 U.S.C. § 2001(3) (2018); *see also* Hanson, *supra* note 266, at 498–500, 499 n.8, 518 (explaining written honesty tests were perceived by publishers to have less risk of legal liability than the polygraph, even though very few lawsuits have tested this claim, while concluding it would be reasonable for Congress to adopt new legislation given how early EPPA drafts explicitly prohibited the tests).

335. Decker, *supra* note 329, at 146–47.

336. *Id.* at 149 (discussing how honesty tests should be regulated by Pennsylvania's anti-polygraph statute).

337. H.R. Rep. No. 100-659, at 11 (1988) (Conf. Rep.) ("The conferees also do not intend to include written or oral tests (commonly referred to as 'honesty' or 'paper and pencil' tests) within the definition of lie detector."); *see also* H.R. REP. NO. 100-208, at 11 (1987) ("In deciding to strike the ['written or oral honesty tests'] language from the definition, the Committee concludes that this issue should be handled separately from the lie detector.").

338. *See* H.R. REP. NO. 89-198, at 43 (1965) (emphasizing the "mental wiretapping" and "insidious search of the human mind" conducted by lie detectors to urge the adoption of the EPPA (quoting Rep. Cornelius E. Gallagher (D-NJ))).

339. Christine M. Wiseman, *Invasion by Polygraph: An Assessment of Constitutional and Common Law Parameters*, 32 ST. LOUIS U. L.J. 27, 33 (1987).

industry, traditional screening and testing procedures had to be updated for an entirely digital and remote hiring process.[340] In this transition, vendors and employers have branched out from the traditional testing procedures to introduce more advanced assessments, including customized predictive assessment tools.[341] It is likely that employers' assumed video-interviewing screens were a more sophisticated iteration of the written integrity tests, only with algorithms instead of human reviewers trained to identify preferred character traits within a large pool of candidates.[342] However, the overlay of affect-recognition technology is a critical departure from past practice. The collection of data points on involuntary communications, such as facial movements and voice tonality, indicates the technology is similar to the lie detector and thus distinguishable from a written multiple-choice exam. As such, these modern affect-screening tests are resurrecting the same unproven methods that underpin lie detector tests: analyzing psychophysiological responses to reach a conclusion about an individual's character.

B. SAME THEORY, SAME CRITICISMS

In adopting the EPPA, Congress clarified that its opposition to the use of lie detectors tracked two predominant concerns: (1) a renewed faith in pseudoscience disproven by a lack of validation, and experts who concluded the foundational scientific basis for the technology was dubious; and (2) the acceleration of privacy harms inflicted on individuals subjected to this random and humiliating testing. These same concerns predominate the use of video-interviewing screens and affect-recognition technology. Finally, the widespread adoption of these algorithmic screens reflects a concerning dependence on technological solutions—believed to be silver-bullet fixes to intractable policy problems—without sufficient concern for the broader societal consequences.

1. Renewed Faith in Pseudoscience

Proponents of video-interviewing screens that rely on affect recognition boast that the technology is capable of determining the "fit" of an individual based on measures of emotional perception revealed by our physical movements.[343] But there is no scientific foundation to support the idea that physiological responses can be sufficiently correlated with an emotional state so as to render a diagnostic opinion about a person's character.[344] It is pseudoscience masquerading behind a

340. *See* BOGEN & RIEKE, *supra* note 13, at 5–6.

341. *See* BOGEN & RIEKE, *supra* note 13, at 29–30; Dave Zielinski, *Predictive Assessments Give Companies Insight into Candidates' Potential*, SHRM (Jan. 22, 2018), https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/predictive-assessments-insight-candidates-potential.aspx [https://perma.cc/7QLA-BRXJ].

342. *See* BOGEN & RIEKE, *supra* note 13, at 29–36; Cheesman, *supra* note 70 (quoting Mark Newman, founder and (at that time) CEO of HireVue: "HireVue has brought much needed structure, data and consistency to the interview experience and now we're bringing a new level of assessment science to it . . . . Many assessments used today were created 50 years ago and deployed to make up for terrible interviewing processes").

343. *See* Harwell, *supra* note 38.

344. CRAWFORD ET AL., *supra* note 4, at 50–51; *see* Harwell, *supra* note 38; Knight, *supra* note 4.

good marketing pitch. A 2019 academic study found that "very little is known about how and why certain facial movements express instances of emotion, particularly at a level of detail sufficient for such conclusions to be used in important, real-world applications."[345] And "there is a substantial amount of variance in how" individuals express their emotional state—across cultures, contexts, and individuals.[346] The authors of the 2019 study concluded, "no matter how sophisticated the computational algorithms. . . . [I]t is premature to use this technology to reach conclusions about what people feel on the basis of their facial movements."[347]

A study conducted by researchers at the University of California, Berkeley found that detecting emotions with any accuracy necessarily requires additional context beyond merely observing a person's face or body.[348] For example, an outwardly smiling face could be communicating different emotions depending on the context: "[I]t could be faked to hide nervousness in an interview setting; it could signal friendliness when celebrating other people's success, and it could also show hostility when teasing or mocking others."[349] In the real world, humans infer emotions by analyzing more than just facial features; however, computer vision may only focus on those surface-level reactions and not incorporate additional context.[350] Given the limited timeframe of an initial screening interview and the lack of control over when, how, where, and with whom the interviews are conducted—an intentional design of the mobile self-schedule interview approach—the necessary context is likely missing.[351] At a recent conference on affect computing, researchers from the University of Southern California warned that the use of emotion analytics should be paused: "[T]his facial expression recognition technology is picking up on something — it's just not very well correlated with what people want to use it for. So they're just going to be making errors, and in some cases, those errors cause harm."[352]

345. Lisa Feldman Barrett, Ralph Adolphs, Stacy Marsella, Aleix M. Martinez & Seth D. Pollak, *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements*, 20 PSYCHOL. SCI. PUB. INT. 1, 48 (2019).

346. CRAWFORD ET AL., *supra* note 4, at 51. For example, research has found that Westerners and East Asians share similar expressions to display pain, but they differ on how to express pleasure. Douglas Heaven, *Why Faces Don't Always Tell the Truth About Feelings*, NATURE (Feb. 26, 2020), https://www.nature.com/articles/d41586-020-00507-5 [https://perma.cc/XN8C-RW3D].

347. Barrett et al., *supra* note 345.

348. Zhimin Chen & David Whitney, *Tracking the Affective State of Unseen Persons*, 116 PNAS 7559, 7563 (2019).

349. *Id.* at 7559.

350. *See id.* at 7563.

351. *Cf.* CRAWFORD ET AL., *supra* note 4, at 51.

352. *Id.* (quoting Professor Jonathan Gratch); *see* Jayne Williamson-Lee, *Amazon's A.I. Emotion-Recognition Software Confuses Expressions for Feelings*, MEDIUM: ONEZERO (Oct. 28, 2019), https://onezero.medium.com/amazons-a-i-emotion-recognition-software-confuses-expressions-for-feelings-53e96007ca63.

Despite these dubious scientific grounds, companies continue to laud the face as "an emotion oracle."[353] Despite recent research questioning the scientific foundations of affect-recognition technology, American psychologist Paul Ekman's influential findings from the 1960s and 1970s that "humans could reliably infer emotional states from [facial] expressions" went unchallenged for a generation.[354] The lingering "scientific aura" of these methods has unmistakably been used to bolster the perceived legitimacy of the technology.[355] For example, the developers of these screens still maintain that their methods are scientifically based, with numerous Industrial Organizational (IO) psychologists, data scientists, and engineers on staff.[356]

2. Accelerating Privacy Harms

Even if the accuracy problems could be solved, the privacy concerns would remain. The average American worker already enjoys precious little privacy in the workplace.[357] The growing use of AI and video-interviewing screens is poised to further erode what remains. In addition to the privacy concerns implicit in all lie detector tests,[358] affect-recognition screens also inspire critiques similar to those mounted against the surveillance economy and facial-recognition technology.[359]

---

353. Heaven, *supra* note 346.

354. *Id.*

355. *See, e.g.*, *The Science Behind Yobs*, *supra* note 85 (detailing the technology developed by Yobs); *How to Prepare for Your HireVue Assessment*, *supra* note 77 (detailing the technology developed by HireVue). As previously noted, HireVue has suspended its use of facial analysis; however, the company continues to use automated voice analysis. *See* Knight, *supra* note 4.

356. *See The Science Behind Yobs*, *supra* note 85; *How to Prepare for Your HireVue Assessment*, *supra* note 77. HireVue's Chief Technology Officer, Loren Larsen, rejected criticism that their AI technology is pseudoscience in saying "most AI researchers have a limited understanding" of the psychology. Harwell, *supra* note 38. Recently, HireVue published a blog, seemingly in response to the research of Dr. Lisa Feldmann Barrett and peers, Barrett et al., *supra* note 345, acknowledging the uncertainty of correlating nonverbal communication detected through facial movements with emotional states or predictions of certain character traits. Lindsey Zuloaga, *Nonverbal Communication in Interview Assessments*, HIREVUE: BLOG (Mar. 31, 2020), https://www.hirevue.com/blog/hiring/industry-leadership-new-audit-results-and-decision-on-visual-analysis [https://perma.cc/JY8X-5APS]. Despite later announcing the halt of using facial analysis, the company never denounced the technology as inaccurate. *See* Knight, *supra* note 4. Instead, HireVue placed the blame on "public outcry"—without addressing whether the objections of privacy and technology experts were legitimate. *See id.*

357. *See, e.g.*, Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CALIF. L. REV. 735, 738 (2017); Elizabeth D. De Armond, *To Cloak the Within: Protecting Employees from Personality Testing*, 61 DEPAUL L. REV. 1129, 1129 (2012); Brishen Rogers, *The Law and Political Economy of Workplace Technological Change*, 55 HARV. C.R.-C.L. L. REV. 531, 532 (2020).

358. *See* discussion *supra* Section II.B.2.

359. *See* CRAWFORD ET AL. *supra* note 4, at 6, 12 (calling for a ban on "the use of affect recognition in important decisions that impact people's lives and access to opportunities" and citing concerns over the lack of scientific validity and risk of bias and misuse, which are common criticisms, of facial recognition technology); *see also* Julia Powles, *We Are Citizens, Not Mere Physical Masses of Data for Harvesting*, GUARDIAN (Mar. 11, 2015, 11:04 AM), https://www.theguardian.com/technology/2015/mar/11/we-are-citizens-not-mere-physical-masses-of-data-for-harvesting (detailing the lecture of Professor Julie E. Cohen at the annual Law and Media and Communications lecture at the London School of Economics). For a more in-depth discussion, see generally Julie E. Cohen, *How (Not) to Write a Privacy Law*,

"[T]echnological and cultural developments," within the past decade, "have made intellectual surveillance easier."[360] Our increasing reliance on an interconnected web of digital devices is being exploited for commercial gain, with private sector business models turning enormous profits off the mass collection and mining of personal data of every individual. The ability to monitor an individual's inner thoughts, and thus understand what motivates their decisionmaking, used to be guesswork.[361] However, the mass marketing model of the 1950s and 1960s has been replaced by the era of big data and sophisticated microtargeting in the era of big data.[362] Digital tracking tools now provide "a record of our intellectual activities —a close proxy for our thoughts—in unprecedented ways and to an unprecedented degree."[363] The more information that is collected, the better companies are able to understand and predict our thoughts and emotions, and therefore, our consumer habits.[364]

The treatment of individuals as conduits for data harvesting raises profound challenges for privacy,[365] specifically our *intellectual* privacy, that are only accelerated by the onset of affect-recognition screens. "Intellectual privacy is the ability . . . to develop ideas and beliefs away from the unwanted gaze or interference of others."[366] Under the tradition of liberal political theory, privacy exists as a "vital enabler of positive liberty," establishing a "boundary . . . through which the capacity for self-determination develops."[367] Absent those protections, surveillance can "warp the integrity of our freedom of thought and can skew the way we think, with clear repercussions for the content of our subsequent speech or writing."[368] But the gateway to a promising career may now run directly through

---

KNIGHT FIRST AMEND. INST. COLUM. U. (Mar. 23, 2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law [https://perma.cc/MR3Q-7QZM] (calling for the regulation of the surveillance-based business model).

360. Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 389 (2008).

361. For example, the popular television series *Mad Men* dramatized the behind-the-scenes work of "ad men" trying (or failing) to create marketing campaigns that could drive millions of people to buy a product or service. *See* Emily Steel, *'Mad Men' and the Era That Changed Advertising*, N.Y. TIMES (Apr. 3, 2015), https://www.nytimes.com/2015/04/04/business/media/mad-men-and-the-era-that-changed-advertising.html.

362. Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 138–40 (2017) (discussing structural changes in the architecture of contemporary network communications that enabled a shift from a model of mass-audience advertisement to targeted marketing, which resulted in "the everyday lives of network users [becoming] increasingly datafied—converted into structured flows of data suitable for continuous collection and analysis").

363. Richards, *supra* note 360.

364. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1402 (2000). The purpose of data processing is often to make logical sense of information about individuals, such as measuring predictability and risk. *See id.* at 1405. Thus, the data-processing industry presumes individuals can be "reducible to the sum of their transactions, genetic markers, and other measurable attributes, and that these attributes are good predictors of risk and reward in future dealings." *Id.* However, as Cohen argues, a critical factor in whether sufficient prediction is possible is "who controls the *modes of prediction*—in other words, about power over knowledge." *Id.* at 1406.

365. *See* Powles, *supra* note 359.

366. Richards, *supra* note 360.

367. Julie E. Cohen, *What Privacy Is for*, 126 HARV. L. REV. 1904, 1905, 1907 (2013).

368. Richards, *supra* note 360.

a mind-reading machine trained to uncover a person's innermost thoughts and detect whether those thoughts align with his or her outward communications. The boundaries have been dissolved. There is no longer an intermediary or thought-adjacent criterion that is being extrapolated to determine our private feelings: the screens are directly invading our intellectual privacy.

The conclusions reached by these algorithms, after analyzing thousands of sensitive data points, are also being used to sort and categorize individuals in problematic ways. Privacy scholars have raised similar concerns over data and informational privacy,[369] especially in an increasingly surveilled and automated world where decisions about goods and services are increasingly being decided by algorithms.[370] As Professor Julie Cohen argues:

> [D]ata subjects may behave as they please, but will be judged against standards of rationality not of their own choosing. The view of human nature reinforced by data-processing algorithms is both unforgiving and ungenerous. There is little room, or tolerance, for randomness, idiosyncrasy, or mistake, and little allowance for learning effects and second chances.[371]

The prospect of sorting job applicants based on immutable characteristics—such as personal appearance and other superficial categories that even a human reviewer could not detect—runs counter to liberal democratic norms. It is an endorsement of technical shortcuts used to determine an individual's self-worth and integrity quite literally in the tremor of their voice or flickering movement of their eyes. And yet, that is what these screens purport to do: make glib judgments on "fit" based upon hidden qualities that only AI can surface from a person's hidden subconsciousness.

A plausible counterargument is that humans irrationally judge others by superficial characteristics all the time, and although it is still problematic, an algorithm performing this function is not a radical departure. Proponents claim algorithms can eliminate some of the more egregious examples.[372] But this would ignore Professor Cohen's thesis: an algorithm treats its data subjects *more harshly* and with *more finality* than a human, all while applying a certain set of rules and standards that are unknown to the individual.[373] The algorithm may be unable to factor in context, or it may misinterpret or misread some physical movements or

369. *See, e.g.*, Cohen, *supra* note 364, at 1407.

370. *See* Citron & Pasquale, *supra* note 95, at 2–4.

371. Cohen, *supra* note 364, at 1408.

372. *See* Harwell, *supra* note 38. As HireVue's Chief Technology Officer, Loren Larson, explains: "People are rejected all the time based on how they look, their shoes, how they tucked in their shirts and how 'hot' they are," and "[a]lgorithms eliminate most of that in a way that hasn't been possible before." *Id.*

373. *See* Cohen, *supra* note 364, at 1408; *see also* Cathy O'Neil, *The Era of Blind Faith in Big Data Must End*, TED (Apr. 2017), https://www.ted.com/talks/cathy_o_neil_the_era_of_blind_faith_in_big_data_must_end?language=en (explaining that "[w]e're being scored with secret formulas that we don't understand that often don't have systems of appeal" and describing algorithms as "opinions embedded in code," not "objective and true and scientific" criteria).

word choices as undesirable. For example, an individual may process an interview question by looking off-screen repeatedly, a normal movement—especially in a virtual environment without another person to maintain eye contact with—but this could be flagged as problematic. Additionally, the algorithm may not account for improvements over the course of an interview as an individual becomes more comfortable and confident. And, the nature of one-way interviewing screens eliminates the possibility of a candidate to respond to any social cues from a human interviewer, which could signal the need to make a performance adjustment or engender greater confidence during the interview. All of these reliability concerns and risks of inaccurate results are exacerbated for people of color or people of different cultural and ethnic backgrounds, whose facial expressions, tone of voice, and other measured criteria would differ from the default subjects used to train the algorithm, usually white men.[374]

Additionally, some have argued that "facial recognition technology"—of which affect-recognition technology is a subset—"is the most uniquely dangerous surveillance mechanism ever invented."[375] It has been called the "plutonium of AI"[376] and the "end [of] all individual privacy."[377] Such surveillance systems—which are often invisible to the public—are *by design* oppressive and threaten civil liberties because "people will act differently if they suspect they're being surveilled."[378] The resulting self-censorship could impede "crucial opportunities for human flourishing by dampening expressive . . . conduct."[379] The threat of facial-recognition technology grows exponentially the larger the database of images becomes. Under the unflinching eye of a facial-recognition system, large corporations and government actors are no longer limited to tracking online activities, but can use street-level surveillance systems to follow the movements of individuals and categorize their emotions and identities based on facial expressions.[380] The increasingly porous boundary between the online

374. *See The Future of Work: Protecting Workers' Civil Rights in the Digital Age: Hearing Before the Subcomm. on Civil Rights & Human Servs. of the H. Comm. on Educ. & Labor*, 116th Cong. 8 (2020) (testimony of Dr. Ifeoma Ajunwa, Assistant Professor, Cornell University).

375. Woodrow Hartzog, *Facial Recognition Is the Perfect Tool for Oppression*, MEDIUM (Aug. 2, 2018), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.

376. Sigal Samuel, *San Francisco Banned Facial Recognition Tech. Here's Why Other Cities Should Too.*, VOX (May 16, 2019, 7:00 AM), https://www.vox.com/future-perfect/2019/5/16/18625137/ai-facial-recognition-ban-san-francisco-surveillance [https://perma.cc/X2NH-43K5] (quoting Luke Stark, a digital media scholar working for Microsoft Research Montreal, who argues that "[f]acial recognition, simply by being designed and built, is intrinsically socially toxic, regardless of the intentions of its makers; it needs controls so strict that it should be banned for almost all practical purposes").

377. David Davis, Opinion, *Facial Recognition Technology Threatens to End All Individual Privacy*, GUARDIAN (Sept. 20, 2019, 5:20 PM), https://www.theguardian.com/commentisfree/2019/sep/20/facial-recognition-technology-privacy; *see* Jonathan Zittrain, *A World Without Privacy Will Revive the Masquerade*, ATLANTIC (Feb. 7, 2020), https://www.theatlantic.com/technology/archive/2020/02/we-may-have-no-privacy-things-can-always-get-worse/606250/.

378. Hartzog, *supra* note 375; *see* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013) (discussing how surveillance can "chill the exercise of our civil liberties").

379. Hartzog, *supra* note 375.

380. *See* Evan Selinger & Woodrow Hartzog, Opinion, *What Happens When Employers Can Read Your Facial Expressions?*, N.Y. TIMES (Oct. 17, 2019), https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html. Facial-recognition systems are being installed in "city streets, airports,

and offline identity of a person may now be fully unraveled, with the information collected used to enforce social norms, to deny economic opportunities, or to label someone as a malcontent.[381]

For example, millions of people across the country (and the world) attended Black Lives Matter protests following the killings of George Floyd, Ahmaud Arbery, and Breonna Taylor.[382] Concerns were raised that police departments would use facial-recognition tools to identify and arrest protesters after the fact or retaliate against them by adding their names to databases and singling them out for selective enforcement of other petty crimes.[383] These concerns are well-founded; back in 2016, following the killing of Freddie Gray, police in Baltimore used facial-recognition technology to find and arrest protestors who they believed had outstanding warrants.[384] And there are serious risks of an algorithm misidentifying a suspect. In 2020, Robert Williams may have been the first known case

retail stores, restaurants, hotels, sporting events, churches, and presumably lots of other places we just don't know about." Lane Brown, *There Will Be No Turning Back on Facial Recognition: It's Not Perfect Yet, but It's Already Changing the World.*, N.Y. MAG: INTELLIGENCER (Nov. 12, 2019), https://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html.

381. *See* Brown, *supra* note 380. "The worst-case scenario for facial recognition" would resemble "China's . . . 'social credit system,'" where millions of cameras around the country "track citizens' behavior and assign each of them a social score." *Id.* (emphasis omitted). The score is calculated taking into account infractions such as "jaywalking and buying too many video games" and the results may make it harder to obtain a bank loan. *Id.*

382. *See* Maneesh Arora, *How the Coronavirus Pandemic Helped the Floyd Protests Become the Biggest in U.S. History*, WASH. POST (Aug. 5, 2020, 7:00 AM), https://www.washingtonpost.com/politics/2020/08/05/how-coronavirus-pandemic-helped-floyd-protests-become-biggest-us-history/; Audra D. S. Burch, Weiyi Cai, Gabriel Gianordoli, Morrigan McCarthy & Jugal K. Katel, *How Black Lives Matter Reached Every Corner of America*, N.Y. TIMES (June 13, 2020), https://www.nytimes.com/interactive/2020/06/13/us/george-floyd-protests-cities-photos.html; Laurin-Whitney Gottbrath, *In 2020, the Black Lives Matter Movement Shook the World*, AL JAZEERA (Dec. 31, 2020), https://www.aljazeera.com/features/2020/12/31/2020-the-year-black-lives-matter-shook-the-world; Elliot C. McLaughlin, *How George Floyd's Death Ignited a Racial Reckoning That Shows No Signs of Slowing Down*, CNN (Aug. 9, 2020, 11:31 AM), https://www.cnn.com/2020/08/09/us/george-floyd-protests-different-why/index.html (estimating that as many as 21 million adults attended a Black Lives Matter or police brutality protest).

383. *See* Jake Laperruque, *How to Respond to Risk of Surveillance While Protesting*, PROJECT ON GOV'T OVERSIGHT (June 4, 2020), https://www.pogo.org/analysis/2020/10/how-to-respond-to-risk-of-surveillance-while-protesting/ [https://perma.cc/Y4QF-PLA3]; Evan Selinger & Albert Fox Cahn, Opinion, *Did You Protest Recently? Your Face Might be in a Database*, GUARDIAN (July 17, 2020, 6:27 PM), https://www.theguardian.com/commentisfree/2020/jul/17/protest-black-lives-matter-database. Privacy and civil rights advocates are also raising alarm at the use of facial recognition technology to confirm the identities of individuals who stormed the U.S. Capitol on January 6, 2021. *See* Joan Donovan & Chris Gilliard, *Facial Recognition Technology Isn't Good Just Because It's Used to Arrest Neo-Nazis*, SLATE (Jan. 12, 2021, 12:54 PM), https://slate.com/technology/2021/01/facial-recognition-technology-capitol-siege.html. While the Internet sleuthing to track down insurrectionists and neo-Nazis undoubtedly feels satisfying, there is concern its popularity in this context will further entrench a deeply flawed and racist technology. *Id.*

384. *See* Clare Garvie & Neema Singh Guliani, Opinion, *Op-Ed: Lawmakers Need to Curb Face Recognition Searches by Police*, L.A. TIMES (Oct. 24, 2016, 4:00 AM), https://www.latimes.com/opinion/op-ed/la-oe-garvie-guliani-face-recognition-20161024-snap-story.html; *see also* CLARE GARVIE, ALVARO M. BEDOYA & JONATHAN FRANKLE, GEORGETOWN LAW CTR. ON PRIVACY & TECH., THE PERPETUAL LINE-UP 42 (2016), https://www.perpetuallineup.org/ [https://perma.cc/UB54-VEH2] ("In 2015, the FBI admitted that it conducted surveillance flights over Ferguson and Baltimore during protests of police use of force.").

of someone arrested for a crime he did not commit based solely on a faulty facial-recognition match—an incident likely to occur again in the future given the number of police departments using facial-recognition systems.[385] Moreover, individuals have warned that facial-recognitions systems could worsen online harassment and lead to an increase in offline stalking and violence.[386]

In the employment context, the use of facial-recognition systems does not operate independently from other surveillance systems. Some employers have started to use facial-recognition systems to identify workers, citing workplace security and convenience benefits.[387] In response to the COVID-19 pandemic, many employers are now rushing to adopt virus-screening programs, including using facial-recognition systems to check in workers and a fever-detection software to gauge temperatures.[388] But with near "ubiquitous network records, browser history retention, phone apps, electronic sensors, wearable fitness trackers, thermal sensors, and facial recognition systems," all creating rich data histories for employers to collect and analyze, "there truly could be limitless worker surveillance."[389] Employers could theoretically cross-check each job applicant against the growing number of facial-recognition databases that have amassed profiles on millions of people.[390] This would be similar to the way employers currently reference information about an applicant's online social media habits and behaviors, only with greater privacy concerns.[391]

3. Technological Solutionism

Finally, the rush to embrace AI-powered hiring screens reflects the broader trend in contemporary culture of relying upon technology to fix every intractable

385. *See* Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

386. *See* Courtney Hinkle, *The End of Anonymity—How Facial Recognition Technology Will Worsen Online Harassment*, 21 GEO. J. GENDER & L. ONLINE (2020); Jessica Mason, *The App That Lets People Search You via Your Face Is Real and Terrifying*, MARY SUE (Jan. 21, 2020, 3:48 PM), https://www.themarysue.com/clearview-ai-facial-recognition-app-terrifying [https://perma.cc/762H-4GM8]; Maya Shwayder, *Clearview AI's Facial-Recognition App Is a Nightmare for Stalking Victims*, DIGITAL TRENDS (Jan. 22, 2020), https://www.digitaltrends.com/news/clearview-ai-facial-recognition-domestic-violence-stalking/ [https://perma.cc/8SZE-94ZS].

387. *See* Mike Rogoway, *Intel Starts Using Facial Recognition Technology to ID Workers, Visitors*, OREGONIAN (Mar. 11, 2020), https://www.oregonlive.com/silicon-forest/2020/03/intel-starts-using-facial-recognition-technology-to-scan-workers-visitors.html.

388. *See* Natasha Singer, *Employers Rush to Adopt Virus Screening. The Tools May Not Help Much.*, N.Y. TIMES (May 14, 2020), https://www.nytimes.com/2020/05/11/technology/coronavirus-worker-testing-privacy.html.

389. Ajunwa et al., *supra* note 357, at 743.

390. *See* Kaveh Waddell, *Half of American Adults Are in Police Facial-Recognition Databases*, ATLANTIC (Oct. 19, 2016), https://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560/. A report by Georgetown Law's Center for Privacy and Technology found that more than 117 million American adults are subject to facial-recognition scanning systems, with eighty percent of the photos being of law-abiding citizens. *Id.* (citing GARVIE ET AL., *supra* note 384, at 2, 21).

391. *See* Saige Driver, *Keep It Clean: Social Media Screenings Gain in Popularity*, BUS. NEWS DAILY (Mar. 23, 2020), https://www.businessnewsdaily.com/2377-social-media-hiring.html [https://perma.cc/3RKE-W556].

problem. Some innovators in Silicon Valley express a technological solutionism approach, presuming that with a sophisticated AI system, the world's most stubborn political and social challenges could be solved.[392] This view is increasingly reflected in the employment context.[393] Some employers who recognize human decisionmakers' inherent biases and predilections may be well-intentioned in their desire for technocratic solutions to fix the many long-standing deficiencies in hiring. But as previously discussed, algorithms are neither neutral nor objective. Instead, they merely reproduce the political and ideological choices of their developers—choices that are likely to carry forward structural biases.[394] Moreover, they likely reflect an (failed) attempt to encode amorphous and unscientific criteria, such as "cultural fit," without first confronting the real-world difficulties of hiring.[395] With the appeal of an easy fix, we risk becoming overconfident in the benefits of a technology and indifferent to its broader societal consequences, which may not be worth trading for convenience.

This technological-solutionist ideology has thwarted attempts to adopt robust privacy legislation. An all-too-common refrain in privacy policymaking is how the law should strike a measured balance between the value of convenience and technological innovation with the dwindling privacy and civil rights enjoyed by the average American. The policy default has historically been to embrace a lighter touch approach, with more ambitious ex ante substantive protections abandoned in favor of procedural safeguards and ex post enforcement regimes. There remains "continuing optimism" among policymakers that imposing new procedural requirements in the form individual control rights, combined with heightened transparency and accountability rules, are a sufficient check on the privacy abuses.[396] But what is the most politically palatable is not necessarily good for privacy law. This is why U.S. privacy law remains perpetually stuck in notice and choice land, even as the world of technology is rapidly changing on a

392. *See* Will Knight, *Could AI Solve the World's Biggest Problems?*, MIT TECH. REV. (Jan. 12, 2016), https://www.technologyreview.com/2016/01/12/163910/could-ai-solve-the-worlds-biggest-problems/.

393. *See* Bornstein, *supra* note 5, at 570 (arguing that if the algorithms are properly built, they can "suppress, interrupt, or remove protected class stereotypes from decisions"); Alex P. Miller, *Want Less-Biased Decisions? Use Algorithms*., HARV. BUS. REV. (July 26, 2018), https://hbr.org/2018/07/want-less-biased-decisions-use-algorithms (arguing that "[a]lgorithms are less biased and more accurate than the humans they are replacing").

394. *See* Ajunwa, *An Auditing Imperative*, *supra* note 5, at 18, 22.

395. *See* Ajunwa, *The Paradox of Automation*, *supra* note 5, at 1707–08, 1712–17 (arguing "the current framing of algorithmic bias as a technical problem" has led to "ineffective techno-solutionist approaches" that ignore how "the biased results of algorithmic hiring systems are not merely technical deficiencies, rather, they reveal legal anachronisms, such as an American tradition of deference to the employer and what amounts to a legal shrug when it comes to addressing the nebulous concept of 'cultural fit' as hiring criterion").

396. *See* Cohen, *supra* note 359 (expressing concerns over the "aggregate efficacy" of "consent-based approaches to privacy governance," which predominate recent federal and state efforts to regulate privacy, concluding "[a]tomistic, post hoc assertions of individual control rights, however, cannot meaningfully discipline networked processes that operate at scale"); *see also* Selinger & Hartzog, *supra* note 380.

massive scale, leaving privacy protections hanging by the thread of vague disclaimers and the promised good intentions of large companies.[397]

But "when technologies become so dangerous and the harm-to-benefit ratio becomes so imbalanced," an outright prohibition should be considered.[398] As the novelist Zadie Smith warned: "[I]n the Anglo-American world we race ahead with technology and hope the ideas will look after themselves."[399] Too much faith is placed in our capacity to correct for any problems that (most certainly) will arise in the future. Without a robust regulatory framework that forces a contemporary reckoning on the substantive effects and desired limits of a technology, we risk unleashing some harms into society that cannot be undone. For example, proponents of the hiring screens address concerns over disparate impact by emphasizing ex post validation studies that use regression analysis to identify the precise variable(s) causing the disproportionate exclusion of certain candidates and "solve" the problem by de-ranking those variable(s) in the algorithm; many developers and scholars believe this would be sufficient.[400] So long as there is no disparate impact, the convenience of cheaper and more efficient hiring is a good thing that cannot—and should not—be denied to employers.

This narrow view would be painfully shortsighted. First, it is merely a doubling down of technological solutionism: the solution to the problem is technology, and the solution to the problems caused by the technology is also technology. Second, it would be a failure of imagination to not see the possible nefarious uses and harmful consequences arising from affect-recognition technology and not just that it may replicate biased outcomes. As Dr. Giorgio Ganis, a researcher of lie-

397. *See* Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/#_edn3 [https://perma.cc/HY5N-Y7M3].

398. Hartzog, *supra* note 375.

399. NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 3 (2015).

400. For example, on February 5, 2020, the House Education & Labor Committee—Subcommittee on Civil Rights and Human Services held a hearing on "The Future of Work: Protecting Workers' Civil Rights in the Digital Age." Civil Rights & Human Servs. Subcomm., *The Future of Work: Protecting Workers' Civil Rights in the Digital Age*, HOUSE REPRESENTATIVES: EDUC. & LAB. COMMITTEE (Feb. 5, 2020, 2:00 PM), https://edlabor.house.gov/hearings/the-future-of-work-protecting-workers-civil-rights-in-the-digital-age- [https://perma.cc/2EJL-DWRQ]. Witnesses included civil rights advocates and a management-side employment lawyer. *Id.* Despite their differing perspectives on policy solutions—such as additional protections beyond ex post validation studies, a worker's bill of rights, and ex ante algorithmic auditing and design mandates—there was nevertheless agreement across the board that so long as automated screening technologies, *see supra* Section I.A., are sufficiently validated to ensure job-relatedness and no adverse impact, these technologies should be readily deployed and used by employers, *see* Civil Rights & Human Servs. Subcomm., *supra*. Absent from the hearing was a robust discussion of the kinds of privacy concerns raised in this Note, in particular, as applied to video-interviewing screens, and whether those harms caused by screens outweigh the efficiency benefits, although two witnesses (Jenny R. Yang and Professor Ifeoma Ajunwa) noted privacy concerns about personality trait screening and the need for limits on access to sensitive employee information. *See id.*, *supra* at 57:40–1:03:26. Even so, the framing of these issues was overwhelmingly positive. For instance, in her closing statements, Subcommittee Chair Rep. Suzanne Bonamici (D-OR) framed the "key questions" moving forward will be whether these screens can be "used properly" or "done correctly." *Id.* at 1:28:55. But this is an entirely different framing of the issues from that posed by this Note.

detection technology, warns: "Scientists don't think much about who is going to use these methods."[401] But if a person's face is an observable proxy for all kinds of sensitive information, the possible misuses of the technology to target the vulnerable or to sort the disfavorables can have impacts beyond just a single hiring decision.[402] The importance of framing has been stridently argued by Evan Selinger and Woodrow Hartzog in the context of facial recognition.[403] As they contend, this technology threatens our collective interest in obscurity—a threat to which we can never truly give consent.[404] Given the "panoply of harms," they argue a total ban on the technology would be the only sufficient policy solution.[405] Although not necessarily responding to their argument or to the larger debate over how to regulate facial recognition, the EPPA—at least in the context of affect screening—does offer a potentially sufficient policy response that accounts for the full scope of potential harms.

C. SAME RESULT: THE RETURN OF THE LIE DETECTOR

The similarities between traditional lie detectors, such as the polygraph, and affect-recognition screens are numerous. Just like a polygraph, the screens purport to render a conclusion about an individual based on involuntary physiological responses by drawing upon unfounded science, which has severe consequences for privacy. And just like a polygraph, the screens are prohibited by the EPPA. Congress demonstrated prescient insight to anticipate future methods of lie detection and drafted the EPPA's provisions broadly to apply to both existing and prospective technological advancements.[406] Specifically, the expansive, flexible definition of "lie detector" is key to applying the EPPA's mandate to AI-powered affect-screening algorithms.

A plain reading of the statute illustrates that the definitional category of lie detector is broad. Despite "polygraph" being featured most prominently in the name of the statute, Congress intended the prohibitions to apply to all types of lie detector tests, including those specifically identified, such as the "deceptograph" or "voice stress analyzer," as well as the expansive catch-all provision, "or any other similar device."[407] Here, there is a heavy emphasis on the intended uses of the device: "[F]or the purpose of rendering a diagnostic opinion regarding the

401. Katwala, *supra* note 201.

402. *See* Sam Levin, *Face-Reading AI Will Be Able to Detect Your Politics and IQ, Professor Says*, GUARDIAN (Sept. 12, 2017, 3:00 PM), https://www.theguardian.com/technology/2017/sep/12/artificial-intelligence-face-recognition-michal-kosinski (explaining some researchers believe that AI technology will soon be able to identify an individual's political ideology, sexual orientation, IQ, or criminal predisposition based on photos of their faces).

403. *See* Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 101, 112–15 (2019).

404. *See id*. at 113–15.

405. *Id*. at 120.

406. *See* Employee Polygraph Protection Act of 1988, 29 U.S.C. § 2001(3) (2018) (not limiting the EPPA's prohibitions to only an enumerated list of technologies but critically barring the use of any technology if used for a lie-detection purpose); H.R. REP. NO. 100-659, at 11 (1988) (Conf. Rep.).

407. *See* 29 U.S.C. § 2001(3).

honesty or dishonesty of an individual."[408] The polygraph is, by its nature, intended to make such conclusions. The catch-all provision, however, could encompass technologies that ordinarily might have various uses, but if used for this specific purpose, are impermissible.

There is a dearth of case law interpreting the scope of these definitional requirements, and the existing guidance supports a broad construction of the EPPA's definitional requirements for a lie detector, including the catch-all provision. The Department of Labor (DOL), tasked with issuing guidance interpreting provisions of the EPPA, offers little direction, except a rule stipulating "[v]oice stress analyzers, or psychological stress evaluators, include any systems that utilize voice stress analysis, whether or not an opinion on honesty or dishonesty is specifically rendered."[409] This rule indicates the DOL interpreted the statute's purpose requirement to apply only to the "or any other similar devices" category of lie detectors, making the use of a voice stress analyzer, and likely the polygraph or deceptograph, a per se violation of the EPPA.

In *Veazey v. Communications & Cable of Chicago, Inc.*, the Seventh Circuit held that the "EPPA's definition of 'lie detector' [did] not, as a matter of law, exclude the use of" a tape-recorded voice exemplar.[410] The defendant, LaSalle Communications, fired Darryl Veazey for insubordination after Veazey refused to provide a tape-recorded voice exemplar of himself reading a transcript of a hostile and threatening message left on the voicemail of a coworker.[411] Veazey denied leaving the voice-mail message and filed suit against LaSalle, alleging violation of the EPPA.[412] The district court granted LaSalle's motion to dismiss, holding the use of a tape recorder did not qualify as a "lie detector test" under the statute.[413] The Seventh Circuit reversed, rejecting LaSalle's arguments that a simple tape recorder, which on its own is unable to render a diagnostic opinion about honesty or dishonesty, falls outside of the scope of the definitional requirements.[414]

The Seventh Circuit based its holding on a plain reading of the statutory language as well as the purpose and intent of the statute. Judge Coffey reasoned, "Congress intended the prohibition on the use of lie detectors [as defined in the

408. *Id.*

409. *See* 29 C.F.R. § 801.2(d)(1) (2019). In addition, "*lie detector* does *not* include medical tests used to determine the presence or absence of controlled substances or alcohol" or "paper and pencil" tests that are machine scored or otherwise. *Id.* at § 801.2(d)(2) (second emphasis added).

410. 194 F.3d 850, 860 (7th Cir. 1999).

411. *Id.* at 853.

412. *Id.*

413. *Id.*

414. *Id.* at 859 (holding a tape recorder, "when used in conjunction with one of the devices enumerated in the [EPPA] . . . may fit within the definition of a 'lie detector'").

EPPA] to be interpreted broadly."[415] In particular, the court emphasized that the term lie detector includes "*any other similar device (whether mechanical or electrical)* that is used, or the results of which are used, *for the purpose of rendering a diagnostic opinion regarding the honesty or dishonesty of an individual*."[416] This catch-all provision necessarily envisions a broader category of technologies which, if used for an impermissible purpose, would still qualify as a lie detector. Here, the tape recording, when used "*in conjunction with other devices*," namely a stress analyzer, would achieve the same results as a lie detector—permitting the "rendering [of] a diagnostic opinion regarding the honesty or dishonesty of an individual" being evaluated.[417] Specifically, LaSalle could use the voice stress analyzer to draw an inference about whether Veazey was telling the truth when he denied leaving the voice-mail message.[418] The court concluded that "[w]e are of the opinion that . . . basic logic necessitates" this conclusion.[419] A narrower reading of the statute would render the EPPA's protections null, as any clever employer could filter its intended purpose through a secondary device.[420] This approach would defy traditional notions of statutory interpretation because "it is extremely unlikely that [a reading] that allows a statute to be so easily evaded would be the correct one."[421] Judge Coffey acknowledged, however, that "those devices which only indirectly indicate whether a person is lying should not be included in the definition."[422] For example, machines that analyze DNA samples from a crime scene that reveal whether a suspected perpetrator's statements of innocence are true or false would not be considered a lie detector.[423] This flexible interpretation of the EPPA, which allows for advancements or different uses of technology, aligns not only with the plain language of the statute, but also with Congress's intent to protect worker privacy.

The EPPA's flexible provisions are directly applicable to the types of video-interviewing screens currently available in the marketplace. Although most algorithms notoriously operate as a "black box," and the opacity of the precise variables considered in rendering an opinion on each applicant still poses a challenge,[424] the types of technology being used, and the background norms that inform hiring decisions, are illustrative of the conclusions made about each

415. *Id.* (citing H.R. Rep. No. 100–659, at 11 (1988) (Conf. Rep.) ("The conferees . . . *intend that the prohibition on a lie detector test be construed broadly to include any use of a lie detector*.")).

416. *Id.* at 858 (quoting 29 U.S.C. § 2001(3) (2018)).

417. *See id.* at 858–59.

418. *Id.* at 859.

419. *Id.*

420. *See id.*

421. *Id.* (citing Hathorn v. Lovorn, 457 U.S. 255, 265 n.16 (1982) (holding Section 5 of the Voting Rights Act could not be interpreted to provide covered jurisdictions a way to easily evade the statute)).

422. *Id.* at 860.

423. *Id.*

424. *See* Bahar Gholipour, *We Need to Open the AI Black Box Before It's Too Late*, FUTURISM (Jan. 18, 2018), https://futurism.com/ai-bias-black-box.

applicant.[425] First, the affect-recognition software used by the most popular vendors falls within the expansive category of a lie detector device that can be used to render an opinion about the honesty or dishonesty of an applicant. The type of technology used is either a "voice stress analyzer," or is alternatively, under the catch-all provision, "any other similar device (whether mechanical or electrical)."[426] Many of the vendors expressly use voice stress analyzers[427] or at least claim to measure tone of voice, which implies the use of some type of stress analyzer.[428] The catch-all provision also applies because the algorithms are powered by electrical devices (computers) that are designed to render a conclusion about each applicant.[429]

Second, the types of technology used by vendors reveal an interest in detecting deception. All of the vendors in this space purport to surface hidden traits in verbal or nonverbal communications—just as a polygraph machine is intended to reveal the unspoken "truth" hidden in verbal responses. For example, the stated purpose of affect-recognition technology is to decode a person's mood or emotional state by searching their facial micro expressions to determine their inner thoughts or emotions and, in turn, identify correlating character traits, such as integrity.[430] The purpose of analyzing tone of voice is to reveal "vocal dissonance markers" or signs of discomfort that occur when an individual is not being honest.[431] The purpose of analyzing word choice could be to extrapolate a certain level of education or to determine if a person is overinflating her qualifications or

425. *See* Minda Zetlin, *AI Is Now Analyzing Candidates' Facial Expressions During Video Job Interviews*, INC. https://www.inc.com/minda-zetlin/ai-is-now-analyzing-candidates-facial-expressions-during-video-job-interviews.html (last visited Mar. 22, 2021).

426. Employee Polygraph Protection Act of 1988, 29 U.S.C. § 2001(3) (2018); *see* Katwala, *supra* note 201.

427. *See The Science Behind Yobs*, *supra* note 85 ("The speech's content is then analyzed linguistically for word choice, sentence construction preferences and more using natural language processing."). For example, Yobs Technologies boasts its algorithm analyzes "not just what is said but how it is said," including tone, emotion, and nonverbal elements of communication. *Id.* This nonverbal content of speech could include insights about the physiological or psychological state of the speaker, including stress level.

428. *See, e.g.*, Butcher, *supra* note 91 (explaining VCV's technology detects nervousness and mood —which often correlate with stress level—when analyzing an applicant's tone of voice); Harwell, *supra* note 38 (explaining HireVue's technology analyzes voice tone); *The Science Behind Yobs*, *supra* note 85 (explaining that Yobs' technology analyzes voice tone); *Video Interview Software*, *supra* note 88 (explaining that Talview's technology analyzes voice tone).

429. *See* 29 U.S.C. § 2001(3); Will Knight, *Prepare for Artificial Intelligence to Produce Less Wizardry*, WIRED (July 11, 2020, 7:00 AM), https://www.wired.com/story/prepare-artificial-intelligence-produce-less-wizardry/ (discussing reliance on specialized computer chips to power AI and the staggering increase in demand for computing power).

430. *See* Dom Galeon, *A New AI That Detects "Deception" May Bring an End to Lying as We Know It*, FUTURISM (Jan. 9, 2018), https://futurism.com/new-ai-detects-deception-bring-end-lying-know-it; Levin, *supra* note 402; Zetlin, *supra* note 425.

431. *See* Damphousse, *supra* note 227; Katwala, *supra* note 201; Memmott, *supra* note 227; *cf.* McCormick, *supra* note 227 (discussing an insurance company's use of "voice-stress analysis technology" to reveal a "combination of markers" that may indicate deception); Mishra & Sharma, *supra* note 227, at 253 (discussing researchers who used "automated vocal emotional analysis software" to reveal "vocal dissonance markers" to support a finding of deception in speech).

giving a canned response.[432] All of these purposes share a common goal: to determine if the applicant is an honest person providing honest answers. Consider the company Talview. The company claims its proprietary TBI engine "analyses *the subtext* of a candidate's video" to determine if a candidate is being disingenuous in her responses by providing "socially accepted answers."[433] In other words, the algorithm is trained to analyze a candidate's facial movements and render an opinion on whether a candidate is faking an answer or deceiving the computer regarding the sincerity of the answer.

Finally, the background norms of employee hiring further supports this conclusion. Given the express or implied interest in hiring workers with integrity—character traits long desired by employers—the honesty or dishonesty of every job candidate is almost certainly being assessed by these algorithms.[434] Of the thousands of data points collected and analyzed, the algorithm may either evaluate expressly for honesty or use a broader set of variables as proxies that correlate closely with a propensity for honesty. Collectively, these data points will be used to render an overall diagnostic opinion for each job candidate: is this person honest, and therefore, a predictably good employee?[435] Consider the company HireVue. Until recently,[436] the company's algorithm purported to measure each candidate's facial micro expressions, tone of voice, and word choice, which can be used to decipher various emotions.[437] Like all vendors, the precise data points HireVue uses to distinguish a future top performer are unclear because disclosure is limited for trade secret purposes and transparency is often counter to the black-box nature of the algorithm itself.[438] In consultation with each client, however,

---

432. Word choice is often analyzed closely with voice patterns (tone) and facial action units (movements of the face), such that vendors caution against overly expressive behaviors or actions, including fake smiles. *See* Alan Jones, Suzan Harkness & Nathan Mondragon, *Acts of Meaning: How AI-Based Interviewing Will Transform Career Preparation in Higher Education*, EDUCAUSE REV. (Jun. 10, 2020), https://er.educause.edu/articles/2020/6/acts-of-meaning-how-ai-based-interviewing-will-transform-career-preparation-in-higher-education#fn7 [https://perma.cc/6LVQ-SMSD]; *cf.* Jan Dönges, *What Your Choice of Words Says About Your Personality*, SCI. AM. (July 1, 2009), https://www.scientificamerican.com/article/you-are-what-you-say/ (suggesting that the choice of articles and pronouns are "less subject to conscious manipulation"); James W. Pennebaker, *Your Use of Pronouns Reveals Your Personality*, HARV. BUS. REV. (Dec. 2011), https://hbr.org/2011/12/your-use-of-pronouns-reveals-your-personality (suggesting that a speaker's choice of articles and pronouns—among other basic parts of speech—may offer insight into their character). Presumably, this advice—to use genuine speech and to act naturally—is intended to signal that the algorithm may interpret some performances as not genuine or deceptive. *See id.* However, HireVue has only given vague explanations for how word choice and other behaviors impact a candidate's score. *See* Harwell, *supra* note 38.

433. *Talview Behavioral Insights*, *supra* note 89 (emphasis added).

434. *See* Sundheim, *supra* note 43.

435. *See* Zetlin, *supra* note 425.

436. *See* Knight, *supra* note 4. As of January 2021, HireVue's AI software will no longer analyze facial expressions. *Id.*

437. *See* Harwell, *supra* note 38.

438. *See id. See generally* PASQUALE, *supra* note 114 (explaining the "black box" is a useful metaphor for these proprietary systems whose inner workings are mysterious by design—that is, the inputs and outputs may be observed, but how that data transforms from one into the other is intentionally masked, both from users and regulators).

HireVue will identify the desired characteristics to train the algorithm to analyze and to preference within "tens of thousands of factors" on each candidate.[439] Given the strong interest in honest employees, the algorithms are almost certainly screening for this core character trait in every applicant.[440] Consider the company Yobs. The company touts its platform as capable of "unlock[ing] the behavior, soft skills and personality data trapped" in voice and video interviews.[441] Yobs advertises that its software is trained to analyze five character traits, including conscientiousness.[442] Conscientiousness is defined as a "person's attitude towards doing the right thing, such as doing a full detailed job, even when the boss isn't watching."[443] In other words, it is the integrity, trustworthiness, and honesty of the applicant.

The use of affect-recognition technology, therefore, constitutes an express violation of the EPPA's sweeping prohibitions. If the Department of Labor brought an enforcement action, an injunction could halt the use of these screens and an employer could be assessed a fine of up to $10,000 per violation. Moreover, any candidate could bring a claim because the EPPA creates a private right of action. Considering that these vendors have collectively conducted tens of millions of interviews, the potential liability is staggering.

CONCLUSION

The promise of swift and efficient hiring using affect-recognition technology comes with steep costs to the privacy and dignity of individuals. Time and again, employers have crafted new ways to crack the minds of job applicants to create shortcuts for sorting the good employees from the bad. From polygraphs to written integrity tests and now with AI analyzing facial expressions and tone of voice, the quest for the perfect lie detector is unrelenting. But individuals deserve protection from pernicious invasions into their most fundamental and consequential realm of privacy that is essential for autonomy and free expression: their private thoughts and feelings. The law should—and must—guard against these privacy invasions. The EPPA's broad prohibitions offer a rebuke to employer practices that violate such norms, and its provisions should be enforced to drive the most intrusive screening tools from the marketplace. The ability to secure a job should not require subjecting one's mind for evaluation and categorization. This information is worthy of shielding from the prying eyes of employers.

439. *See* Harwell, *supra* note 38.
440. Zetlin, *supra* note 425.
441. *Yobs Technology*, *supra* note 86.
442. *The Science Behind Yobs*, *supra* note 85.
443. *Id.*