

COMMENTS

THE EXPANSION OF TRADITIONAL BACKGROUND CHECKS TO SOCIAL MEDIA SCREENING: HOW TO ENSURE ADEQUATE PRIVACY PROTECTION IN CURRENT EMPLOYMENT HIRING PRACTICES

Elana Handelman

INTRODUCTION

Imagine that you are in the process of applying for your dream job. At some point in the process, either during the application stage or even after a conditional offer, the employer notifies you that it will need to conduct a background check. You might receive an email asking you to indicate past addresses, jobs, motor vehicle records, whether you have any prior convictions, and more. You might feel confident and excited about your prospects of getting the job, even after the background check. But then you are notified that you did not receive an offer. And the reason you did not receive the job was not because of something that you indicated in the background check questions; rather, it was because of the results of another background check, a social media background check, that was conducted by looking through your Facebook, Instagram, Twitter, or Snapchat accounts.¹

The methods employers use to conduct background checks have changed with the growth of social media. Background checks became an important part of the hiring process after the development of negligent hiring liability, a

* J.D., 2021, University of Pennsylvania Carey Law School; B.A., 2017, University of Maryland, College Park. Thank you to Professor Serena Mayeri for sparking my interest in employment law and for discussing initial ideas, and to Professor Jessica Simon for providing valuable guidance on early drafts.

1 See generally Stav Ziv, *8 Times Candidates Didn't Get Hired Because of Something They Put on Social Media*, THE MUSE, <https://www.themuse.com/advice/clean-up-social-media-or-risk-not-getting-job> (noting one candidate who did not get the job because of his Facebook posts about sports that included curse words and another whose offer was rescinded when he posted about being excited to “party all summer” at his upcoming internship).

form of legal liability that can be traced back over 100 years.² Since then, background checks have become a device for protecting employees and customers from workplace violence and maintaining employers' positive reputations.³ As technology has changed and the use of social media has grown, employers have also turned to social media as a tool for further screening job applicants.⁴ However, the expansion of traditional background checks to encompassing social media screening creates increased challenges to applicants' privacy and the laws that regulate traditional background checks are not sufficient to protect applicants in this context. Some legal advancements have increased protection for applicants subjected to social media background checks; however, the law should recognize how social media presents challenges to privacy protection that are distinct from those challenges presented by traditional background checks.

This comment considers the historical developments of background checking processes in the 20th and 21st centuries and how the law has failed to adequately track these developments from more traditional processes to the current phenomenon of the social media background check. Part I outlines the use of traditional background checks in the employment context, from the purpose behind background checks to the current legal landscape, including a description of federal and state laws regulating background checks and their constitutionality. Part II describes the extension from traditional background checks to the social media background check, including benefits and consequences of employers using social media to screen applicants, and explaining why social media screening requires greater privacy protection. Part III considers avenues for ensuring adequate protection, including some recent statutory solutions and suggests the need for either an express constitutional right to informational privacy or a new understanding of what a reasonable expectation of privacy should be under the Fourth Amendment.

2 See *How We Got Here: A Brief History of Background Screening*, CLEARSTAR (July 26, 2016), <https://www.clearstar.net/how-we-got-here-a-brief-history-of-background-screening/> (stating that background checks grew out of negligent hiring liability, in which an employer can be held liable for the actions of an employee).

3 See Ryan Howard, *The History of Employment Background Screening*, VERIFIRST (Jan. 26, 2018), <https://blog.verifirst.com/the-history-of-employment-background-screening> ("Background checks manage risk for employers by: [b]uilding a culture and reputation of trust and good will . . . [c]reating a safe work environment.").

4 See Debbie Lamb, *Social Media Screening Continues its Upward Trend*, STERLING (Oct. 5, 2017), <https://www.sterlingcheck.com/blog/2017/10/social-media-screening-continues-upward-trend/> (citing CareerBuilder's 2017 social media recruitment survey, which found that 70% of US employers use social media to research job candidates, which is up from 60% in 2016 and only 11% a decade ago).

I. THE USE OF BACKGROUND CHECKS IN THE EMPLOYMENT CONTEXT

A. *Historical Development*

In 1908, in the case of *Ballard's Adm'x v. Louisville & N.R. Co.*, an apprentice in a machine shop pulled a prank on another employee, accidentally killing him. In its decision, the Kentucky Court of Appeals held the employer liable for the employee's actions, establishing that "the master must exercise ordinary care in the selection of his servants and if he fails to exercise such care, and one of the servants is injured by the incapacity of another servant, the master is liable"⁵ This reasoning has come to support a cause of action known as negligent hiring liability. Under the theory of negligent hiring, an employer could be held liable for hiring employees "who posed a reasonably foreseeable risk of inflicting personal harm on others."⁶ This risk of liability for negligent hiring led employers to develop and rely on background checks. The need for background checks arose because someone who is injured as a result of a negligently hired employee can obtain damages from the employer.⁷ For example, the parents of a 32-year-old quadriplegic successfully sued a healthcare company for \$26.5 million when its failure to run a background check led to a home healthcare aide, with a history of larceny convictions, killing the 32-year-old to try to cover up an additional theft.⁸ The theory of negligent hiring rests on the notion of an employer's direct negligence in its hiring rather than on vicarious liability for an employee's negligence.⁹ The doctrine was expanded to cover not only employees injured by other employees, but also third parties such as

5 *Ballard's Adm'x v. Louisville & N.R. Co.*, 110 S.W. 296 (Ky. Ct. App. 1908).

6 Restatement (Second) of Agency § 213(b) (1958).

7 *See Ponticas v. K.M.S Invs.*, 331 N.W.2d 907, 910-11 (Minn. 1983) (ruling that an employer may be held liable for a negligently hired employee).

8 *See Why Should I Run Background Checks?* BACKGROUNDCHECKS.COM, <https://www.backgroundchecks.com/whyrunabackgroundcheck> (last visited Nov. 4, 2020) (recounting a story of a man killed by a home healthcare aide).

9 *Morris v. JTM Materials, Inc.*, 78 S.W.3d 28, 49 (Tex. App. 2002) ("Negligent hiring, retention, and supervision claims are all simple negligence causes of action based on an employer's direct negligence rather than on vicarious liability.").

customers of the business,¹⁰ and has been further expanded to include members of the public who might come into contact with employees.¹¹

Courts have suggested that by conducting a reasonable investigation, an employer can avoid negligent hiring liability, and this reasonable investigation is what we know as the background check.¹² Even if an employee later causes an injury, courts have decided against a finding of negligent hiring as long as the employer conducted an adequate background check.¹³ However, a brief background check might not be sufficient for an employer to avoid liability.¹⁴ The requirements for an adequate background check differ by state, which can be exceptionally confusing for employers regarding rules around criminal history.¹⁵ Nevertheless, factors such as “habitual drinking and drug use, habitual carelessness, forgetfulness, inexperience, mental and physical defects, and a propensity for recklessness or viciousness” can show unfitness to perform a job.¹⁶ Due to the legal exposure of negligent hiring, employers now perform due diligence on candidates both when they are hired and sometimes when they change jobs or are promoted.¹⁷ Today, a variety of types of

10 Adriel Garcia, *The Kobayashi Maru of Ex-Offender Employment: Rewriting the Rules and Thinking Outside Current “Ban the Box” Legislation*, 85 TEMP. L. REV. 921, 932 (2013) (explaining that, “while not employees,” customers “were nonetheless closely connected with the employer”).

11 See *id.* (noting that the “fundamental purpose of negligent hiring law is to protect people from employers who do not exercise due care in hiring employees . . .”).

12 See *Ponticas v. K.M.S Invs.* 331 N.W.2d 907, 910 (Minn. 1983) (“Liability is predicated on the negligence of an employer in placing a person with known propensities, or propensities which should have been discovered by reasonable investigation, in an employment position in which . . . it should have been foreseeable that the hired individual posed a threat of injury to others.”) (emphasis added). See also *Phillips v. Super Servs. Holdings, LLC*, 189 F. Supp. 3d 640, 648 (S.D. Tex. 2016) (“To avoid a negligent hiring or entrustment claim, employers should make a proper investigation into an employee’s past.”).

13 See *Phillips*, 189 F. Supp. 3d at 658 (finding that because the employer conducted background checks that all came back clear, there was no proximate cause because the dangerous behavior was not foreseeable). See also *Saine v. Comcast Cablevision of Arkansas, Inc.*, 126 S.W.3d 339, 345 (Ark. 2003) (holding that because the background check did not give an indication that an employee would be a risk to customers, there cannot be a finding of negligent hiring).

14 See *Morris v. JTM Materials, Inc.*, 78 S.W.3d 28, 51–52 (Tex. App. 2002) (finding that the employer’s failure to further investigate an applicant to confirm the accuracy of his stated driving history raised an issue of fact as to whether the employer exercised reasonable care in qualifying him as a driver).

15 See generally Margaret M. Clark, *How to Address Negligent Hiring Concerns*, HR MAGAZINE (Feb. 27, 2019), <https://www.shrm.org/hr-today/news/hr-magazine/spring2019/pages/how-to-address-negligent-hiring-concerns.aspx>. See also *infra* Part II(C)(iii) (discussing various state “ban the box” laws).

16 Marian M. Extejt and William N. Bockanic, *Issues Surrounding the Theories of Negligent Hiring and Failure to Fire*, 8 BUS. & PROF. ETHICS J. 21, 26 (1989).

17 Howard, *supra* note 3.

background checks are used to investigate applicants or current employees.¹⁸ The most common background checks involve some combination of verifying identity, education, and employment, checking for criminal history, sex offender information, and conducting a pre-employment drug test.¹⁹

The desire of employers to conduct adequate investigations into potential employees led to the rise of an industry specializing in conducting background checks.²⁰ Many employers now outsource this process to these third parties rather than conducting the screenings internally.²¹ In 2003, the National Association of Professional Background Screeners (NAPBS) was founded in order to ensure high performance and ethical standards in the background check industry.²² Any “trusted professional background check company” is part of the NAPBS, and the association’s members pledge to follow the Fair Credit Reporting Act and other fair business practices.²³

Outsourcing the background checking process, rather than screening applicants internally, provides a number of benefits for employers. Outsourcing companies market themselves as being more accurate, objective, and faster due to their access to specialized resources.²⁴ In addition, they claim to be experts in handling sensitive information and emphasize that they can ensure compliance with states that might have varying privacy and disclosure laws.²⁵ However, the decision to conduct the searches internally rather than outsource this process to a third-party presents important legal distinctions, because only third-party reporting agencies are subject to the rules of the Fair Credit Reporting Act.²⁶

B. Benefits of Background Checks

In addition to limiting exposure for negligent hiring claims, background checks provide a wide range of benefits for employers. Background checks protect employee rights and generally make workplaces safer for the

18 *Id.*

19 *Id.*

20 *See Background Check Services in the US- Market Size 2004-2026*, IBIS World, <https://www.ibisworld.com/industry-statistics/market-size/background-check-services-united-states/> (updated Nov. 19, 2020) (detailing industry statistics for background check services).

21 *How We Got Here*, *supra* note 2.

22 Howard, *supra* note 3.

23 *Id.* *See also* *infra* Part II(C)(ii) (discussing the Fair Credit Reporting Act).

24 Katie Kulp, *5 Reasons to Outsource Your Pre-Employment Background Screening*, CHANE SOLUTIONS (June 29, 2018), <https://www.chanesolutions.com/2018/06/29/5-reasons-to-outsource-your-pre-employment-background-screening/>.

25 *See id.*

26 *See infra* Part II(C)(ii) (discussing compliance requirements under the Fair Credit Reporting Act).

employer, employee and customers.²⁷ In order for any business to succeed, that business needs to be safe for employees.²⁸ However, keeping a work environment safe isn't always an easy task. Millions of employees in America every year report being victims of workplace violence.²⁹ Although workplace violence is relatively rare compared to violence outside of the workplace, given how much time Americans spend at work, this is an important subset of total crime.³⁰ In addition to protecting employees, a business can only thrive if its customers are not harmed by its employees.³¹ Having effective background checks is one way to prevent violence in the workplace for both employees and customers.³²

Beyond mitigating workplace violence itself, the failure to perform background checks can result in economic losses other than those created by workplace violence. In the retail industry, theft by employees creates serious economic losses for business,³³ and performing background checks can, to an extent, protect against this kind of criminal behavior. In addition, businesses suffer economic losses when new employees cannot actually perform the skills they were hired to perform.³⁴ Losses can also come from adverse media attention when the public becomes aware of an employee who lied about a

27 See *How We Got Here*, *supra* note 2 (noting that background checks make workplaces safer for employees, employers, and customers).

28 See *Why Should I Run Background Checks?*, *supra* note 2 (“Protection of your employees is imperative in any business.”).

29 *Assaults Fourth Leading Cause of Workplace Deaths*, NAT'L SAFETY COUNCIL, <https://www.nsc.org/work-safety/safety-topics/workplace-violence> (last visited Nov. 4, 2020).

30 *2018 National Crime Victims' Rights Week Resource Guide: Crime and Victimization Fact Sheets*, OFF. OF JUST. PROGRAMS (2018). See also Rachel Premack, *17 Seriously Disturbing Facts About Your Job*, BUS. INSIDER (Aug. 2, 2018), <https://www.businessinsider.com/disturbing-facts-about-your-job-2018-2> (noting that the average American spends 90,000 hours at work over their lifetime).

31 See *Why Should I Run Background Checks?*, *supra* note 8 (noting the story of Jesse Rogers, a home healthcare aid who was hired without a background check and killed a 32-year-old quadriplegic for whom he was supposed to be caring).

32 Kara M. Maciel, *Workplace Violence Policies and Background Checks Are Essential Components of a Prevention Plan*, EPSTEIN BECKER GREEN (Apr. 22, 2012), <https://www.oshalawupdate.com/2012/04/22/workplace-violence-policies-and-background-checks-are-essential-components-of-a-prevention-plan/> (“A critical aspect of a prevention plan is the implementation of effective background checks of applicants and employees in order to ensure that individuals with a violent history are carefully screened.”).

33 *Why Should I Run Background Checks?*, *supra* note 8 (citing a study that showed an annual loss of \$15.9 billion from retail shrinkage due to employees).

34 *Id.* (citing STEVEN D. LEVITT & STEPHEN J. DUBNER, *FREAKONOMICS: A ROGUE ECONOMIST EXPLORES THE HIDDEN SIDE OF EVERYTHING* 171 (rev. ed. 2006)) (reporting that roughly 50% of the population lies on their resumes, and that 50% of “references checked in 2004 contained inaccurate information”).

past experience or expertise.³⁵ Background checks can help prevent these losses by ensuring that experience stated on an applicant's resume is accurate.

C. Current Legal Landscape

With the availability of negligent hiring claims, the potential damage to employer and customer safety, and the potential harm to business reputations, looking into the histories of job applicants to ensure that they are the right fit for the job is justified. Furthermore, a number of industries actually require background screenings, especially if those jobs require their employees to handle sensitive information.³⁶ However, an employer's need to look into the history of an applicant must be balanced against the applicant's rights, including their rights to privacy and to be free from unlawful discrimination.³⁷ As the use of background checks has grown, leaders on both the federal and state levels have passed laws and regulations to ensure that these rights are protected.

1. Federal Laws Regulating Background Checks

The primary federal regulation that oversees background checks today is the Fair Credit Reporting Act ("FCRA"). Enforced by the Federal Trade Commission, the FCRA applies when an employer outsources its background check process to a company that is "in the business of compiling background information."³⁸ This is defined broadly; even if a company insists that it is not a consumer reporting agency, if it assembles and analyzes consumer information "for the purpose of providing those reports to third parties," it is regulated by the FCRA.³⁹ If an employer conducts its own background checks

35 See Julianne Pepitone, *Yahoo Confirms CEO Is Out After Resume Scandal*, CNN MONEY (May 13, 2012, 10:00 AM), <https://money.cnn.com/2012/05/13/technology/yahoo-ceo-out/index.htm> (detailing a scandal involving Yahoo's CEO, who lied about his college degree on his resume).

36 See *Why Should I Run Background Checks?*, *supra* note 8 (noting the requirement of background checks in the home healthcare, financial, and insurance industries, among others).

37 See Pamela V. Keller, *Balancing Employer Business Interests and Employee Privacy Interests: A Survey of Kansas Intrusion on Seclusion Cases in the Employment Context*, 61 U. KAN. L. REV. 983, 1006 (2013) ("Courts seem to intuitively, if not explicitly, balance the rights of employers and employees to determine whether an employer's investigation of employee behavior intrudes on the employee's seclusion.").

38 *Background Checks: What Employers Need to Know*, U.S. EQUAL EMP. OPPORTUNITY COMM'N (Mar. 11, 2014), https://www.eeoc.gov/eeoc/publications/background_checks_employers.cfm.

39 See Tony Rodriguez and Jessica Lyon, *Background Screening Reports and the FCRA: Just Saying You're Not a Consumer Reporting Agency Isn't Enough*, FED. TRADE COMM'N (Jan. 10, 2013), <https://www.ftc.gov/news-events/blogs/business-blog/2013/01/background-screening-reports-fcra->

internally, the FCRA does not apply.⁴⁰ However, given the standardization of outsourcing background checks to third parties⁴¹, the FCRA likely has broad scope in regulating background checks.

The FCRA regulates the use of consumer reports, which are defined as “any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s . . . character, general reputation, personal characteristics, or mode of living”⁴² The Act includes a set of requirements when an employer uses third parties to conduct background checks. An employer must give notice of and get consent from the applicant to conduct the background check.⁴³ This disclosure document must consist solely of the disclosure and cannot be used to release the employer from liability connected to the background check.⁴⁴ The employer must also inform the applicant that the information might be used for employment decisions.⁴⁵ If the employer decides not to hire an applicant because of something in the report, it must provide the applicant with a copy of the report and a “Summary of Rights,” which gives the applicant instructions for contacting the company that conducted the background check in order to look for mistakes in the report.⁴⁶ The FCRA also contains a “Disposal Rule,” which provides guidance for employers and consumer agencies for how to dispose of background checks and other consumer reports in order to maintain the privacy of the person on whom the background check was conducted.⁴⁷

just-saying-youre-not (detailing the FTC’s settlement with Fiquarian Publishing, whereby the FTC found the company to be a consumer reporting agency despite its disclaimer that its reports should not be used for employment purposes and are non-FCRA compliant).

40 Ryan B. Frazier, *Employers: Check the Law Before Checking an Applicant’s Background*, 21 UTAH EMP. L. LETTER, no. 6, 2015.

41 *How Outsourcing Background Checks Provides Increased Security*, VICTIG SCREENING SOLUTIONS, <https://www.victig.com/how-outsourcing-background-checks-provides-increased-security/> (last visited Nov. 11, 2020).

42 15 U.S.C 1681 § 603(d)(1) (2018).

43 FED. TRADE COMM’N, *BACKGROUND CHECKS: TIPS FOR JOB APPLICANTS AND EMPLOYEES 2* (2016), <https://www.consumer.ftc.gov/articles/pdf-0044-background-checks.pdf>.

44 See *Harris v. Home Depot U.S.A., Inc.*, 114 F. Supp. 3d 868, 870 (N.D. Cal. 2015) (“[A] release of liability is separate and distinct from the disclosure and authorization.”).

45 *BACKGROUND CHECKS: TIPS FOR JOB APPLICANTS AND EMPLOYEES*, *supra* note 43, at 2.

46 An applicant’s rights might differ depending on the type of negative information discovered. For example, if the employer finds adverse criminal history or financial information, the applicant has the right to dispute the accuracy of the information, and if they find adverse medical history, the applicant has the right to show the employer that they can still do the job. *Id.* at 3-7.

47 *Disposing of Consumer Report Information? Rule Tells How*, FED. TRADE COMM’N (June 2005), <https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how>.

Background checks are also regulated by federal antidiscrimination laws, which are enforced by the Equal Employment Opportunity Commission (“EEOC”).⁴⁸ These laws prohibit discrimination based on race, national origin, sex, religion, disability, genetic information such as family medical history, and age.⁴⁹ These laws include Title VII of the Civil Rights Act of 1964, the Age Discrimination in Employment Act, the Americans with Disabilities Act, the Equal Pay Act of 1963, the Pregnancy Discrimination Act, and more.⁵⁰ Certain states, such as California, have expanded protected categories under state law, such as marriage status, gender identity and expression, and political affiliations.⁵¹ Background checks can violate these laws when an employer, through the background check, becomes aware of an applicant’s characteristics that are protected by these laws, and then makes employment decisions on the basis of these protected characteristics.⁵²

Unlike in the FCRA context, in the federal antidiscrimination law context it does not matter whether an employer uses a third party to run a background check or whether the employer conducts the check internally. Regardless of how it obtained the information, an employer cannot use the information to discriminate in making its employment decisions.⁵³ Furthermore, an employer cannot base its decision to conduct a background check on an applicant’s race or gender.⁵⁴ Compliance with antidiscrimination laws is another reason why employers prefer to outsource the background checking process to third-parties; when background checks are conducted internally, the employer is

48 See *Background Checks: What Employers Need to Know*, *supra* note 38 (stating that if an employer is using an applicant’s background information to make an employment decision, it must comply with federal laws that protect applicants from discrimination).

49 *Id.*

50 *Laws Enforced by the EEOC*, U.S. EQUAL EMP. OPPORTUNITY COMM’N, <https://www.eeoc.gov/statutes/laws-enforced-eeoc> (last visited Nov. 2, 2020).

51 Elizabeth M. Levy & Michael Wahlander, *Is Looking For Applicants on Social Media Looking For Trouble?*, SEYFARTH SHAW LLP (Feb. 6, 2019), <https://www.calpeculiarities.com/2019/02/06/is-looking-for-applicants-on-social-media-looking-for-trouble/>.

52 See *Background Checks: What Employers Need to Know*, *supra* note 38 (“Any background information you receive from any source must not be used to discriminate in violation of federal law.”). See also *Employers’ Evolving Use of Background and Credit Checks*, 19 N.M. Emp. L. Letter, no. 12, 2013 (“[S]tatistics show that without proper consideration, the use of background and credit checks can disproportionately affect members of groups protected by employment discrimination laws.”).

53 See *Background Checks: What Employers Need to Know*, *supra* note 38 (“[A]ny time you use an applicant’s or employee’s background information to make an employment decision, regardless of how you got the information, you must comply with federal laws that protect applicants and employees from discrimination.”).

54 See *id.* (using as an example an employer who only asks applicants of a certain race about their financial or criminal history).

aware of protected characteristics and could be more likely to make decisions based on them.⁵⁵

In addition to the FCRA and federal antidiscrimination laws, international laws influence the way in which an employer can conduct background checks. If the background check involves personal information from non-US sources, the check might be subject to data privacy laws, such as the General Data Protection Regulation (“GDPR”).⁵⁶ The GDPR has made screening applicants more complicated, and in order to conduct a background check, these laws require more specific indications of consent from the applicant or employee.⁵⁷

2. State Laws Regulating Background Checks

States also have varying laws regulating how an employer can conduct background checks. The primary difference among states today is the extent to which they allow consideration of an applicant’s criminal history. These laws are known as “Ban the Box” laws, and they encourage employers to remove questions about criminal history from the initial job application to prevent “blanket ban[s]” on people with criminal records from accessing employment opportunities.⁵⁸ One rationale for this policy is to prevent criminal recidivism by helping people with criminal records obtain jobs.⁵⁹ Additionally, proponents suggest that preventing recidivism helps everyone, not just the individual with a criminal history; they help everyone because providing more people with jobs is good for families, communities, and the overall economy.⁶⁰

55 See Katie Kulp, *5 Reasons to Outsource Your Pre-Employment Background Screening*, CHANE SOLUTIONS (June 29, 2018), <https://www.chanesolutions.com/2018/06/29/5-reasons-to-outsource-your-pre-employment-background-screening/> (noting the potential for bias with in-house screening, because interviewers and managers have met the applicant).

56 See Barbara A. Lee & Nancy H. Van der Veer, *Supreme Court Rules for Employers and Upholds Constitutionality of Government Background Checks*, LEXOLOGY (Jan. 28, 2011), <https://www.lexology.com/library/detail.aspx?g=9efcf841-b262-44b8-94ea-3c9b72ac6acd> (noting the application of these laws to European Union member countries). See also Jagriti Patwari, *How GDPR Affects Background Checking*, TLNT (Feb. 14, 2019), <https://www.tlnt.com/how-gdpr-affects-background-checking/> (noting that the GDPR, although a set of EU privacy rules, has such broad reach that “companies everywhere are taking steps to comply”).

57 Lee & Van der Veer, *supra* note 56; Patwari, *supra* note 56.

58 *Ban the Box*, NAACP, <https://www.naacp.org/campaigns/ban-the-box/> (last visited Nov. 1, 2020).

59 See Garcia, *supra* note 10, at 922 (noting that studies show a relationship between unemployment and recidivism).

60 Beth Avery & Han Lu, *Ban the Box: U.S. Cities, Counties, and States Adopt Fair Hiring Policies*, NAT’L EMP. L. PROJECT (SEPT. 30, 2020), <https://www.nelp.org/publication/ban-the-box-fair-chance-hiring-state-and-local-guide/>.

These laws delay background checks into an applicant's criminal history until later in the hiring process, sometimes until after a conditional offer is made.⁶¹ For example, in 2014 the District of Columbia passed the Fair Criminal Record Screening Amendment Act (FCRSA), which requires employers to delay questions about criminal history until they have made a conditional offer of employment.⁶² Then, if they become aware of criminal history, they can retract the offer as long as it is for a "legitimate business reason."⁶³ While many of these laws primarily cover the public sector, thirteen states have also mandated that private employers remove conviction history questions from applications.⁶⁴

These differences among states pose challenges for large national employers who must comply with different state laws dictating if, and when, in the hiring process the employer can consider an applicant's criminal history.⁶⁵ Furthermore, this presents a dilemma for employers in finding a balance between giving applicants the ability to be fairly evaluated despite their criminal history, and also trying to avoid liability for negligent hiring.⁶⁶ There has also been criticism of the impact of these laws. Although some states that have implemented "ban the box" laws have established state-level enforcement processes, many other states do not have explicit enforcement procedures.⁶⁷

61 *Id.*

62 *See* Fair Criminal Record Screening Amendment Act of 2014, D.C. Code 20-422 § 3(b) (2014) (providing that employers shall only ask questions after they have made a conditional offer of employment).

63 *Id.* § 3(d).

64 *See* Avery & Lu, *supra* note 59 (listing states such as California, Colorado, Massachusetts, and New Jersey).

65 *See* Roy Maurer, *Ban the Box Turns 20: What Employers Need to Know*, SHRM (Nov. 12, 2018), <https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/ban-the-box-turns-20-what-employers-need-to-know.aspx> ("With no federal ban-the-box statute applicable to private employers, companies that hire for positions around the country must comply with a hodgepodge of requirements across states and even localities."). There have been calls for a federal "ban the box" law, and the EEOC does provide guidance on how to avoid discrimination based off criminal history in the hiring process. *See* Christina O'Connell, Note, *Ban the Box: A Call to the Federal Government to Recognize a New Form of Employment Discrimination*, 83 FORDHAM L. REV. 2801 (2015) (calling for federal ban the box laws to help employer compliance). *See also* EEOC Enforcement Guidance: Consideration of Arrest and Conviction Records in Employment Decisions Under Title VII of the Civil Rights Act of 1964, U.S. EQUAL EMP. OPPORTUNITY COMM'N, https://www.eeoc.gov/laws/guidance/arrest_conviction.cfm (considering discrimination based off criminal history as a subset of unlawful discrimination on the basis of race and national origin).

66 *See* Maurer, *supra* note 64 (noting this balancing act).

67 *See* Margaret Barthel, *Employers Are Still Avoiding Former Inmates*, THE ATLANTIC (Nov. 5, 2019), <https://www.theatlantic.com/politics/archive/2019/11/are-states-complying-ban-box-laws/601240/> (noting how this poses challenges for discovering if and how these states are processing complaints of violations of these laws).

In her *Atlantic* article, Margaret Barthel notes that “[i]n some cases, state personnel either weren’t aware of [their state’s] ‘ban the box’ policies in the first place or weren’t able to explain how they were being enforced.”⁶⁸ Some studies suggest that these policies are actually having an adverse impact on job applicants who are racial minorities, because when employers aren’t able to ask about criminal history, they use race as a proxy.⁶⁹ One study suggests that these policies could have negative consequences specifically for black men who do not have criminal records.⁷⁰ EEOC commissioner Victoria Lipnic has noted that while using race as a proxy violates established antidiscrimination laws, it can be hard to prove that an employer has made its decision based on race.⁷¹

3. *The Constitutionality of Background Checks*

In addition to federal and state regulation of background checks, questions surrounding the constitutionality of background checks also raise concerns regarding applicants’ privacy. In 2011, the issue of background checks in employment was brought before the Supreme Court in the case of *NASA v. Nelson*.⁷² The Respondents in *Nelson* were federal contract employees at a government laboratory, and they objected to two parts of a standard employment background check: the first was part of a questionnaire that asked about treatment or counseling for recent illegal-drug use, and the second was a set of open-ended questions on a form that was sent to designated references.⁷³ The Respondents based their objections on *Whalen v. Roe*⁷⁴ and *Nixon v. Administrator of General Services*,⁷⁵ where the Supreme Court broadly referred to a constitutional right to informational privacy.⁷⁶ In *Nelson*, the Supreme Court assumed, without deciding, “that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*.”⁷⁷ However, the Court found that the government’s background check in this case did not

68 *Id.*

69 *See id.* (highlighting this paradox).

70 *See* Katherine English, *Conflicting Approaches to Addressing Ex-Offender Unemployment: The Work Opportunity Tax Credit and Ban the Box*, 93 IND. L.J. 513, 529 (2018).

71 *See id.*

72 *See generally* *NASA v. Nelson*, 562 U.S. 134 (2011) (addressing the issue of background checks in the employment context).

73 *See id.* at 138 (introducing Plaintiffs’ objections).

74 429 U.S. 589 (1977).

75 433 U.S. 425 (1977).

76 *See NASA*, 562 U.S. at 144 (noting that the court has acknowledged a constitutional right to informational privacy).

77 *Id.* at 138.

violate this right to privacy, because the right does not prevent the government from asking reasonable questions.⁷⁸

The Court balanced this constitutional right against the government's interests. It considered the government's interests as an employer in managing its internal operations,⁷⁹ and noted that this background check was similar to the standard background checks used by millions of private employers.⁸⁰ The Court rejected the argument that a background check must be "necessary" or the "least restrictive means," and instead analyzed whether the challenged sections of the government's background check were "reasonable" and "employment related."⁸¹ The Court cited the prevalence of similar background checks in the private sector as proof of its reasonableness.⁸² The Court also noted privacy concerns inherent in the government accumulating information about an individual for public purposes, and similar to in *Whalen* and *Nixon*, it found that sufficient statutory and regulatory protections against disclosure exist to alleviate these privacy concerns.⁸³

Nelson has numerous implications for the legality of background checks, but it also left open some questions. The Court confirmed that conducting background checks can be an efficient strategy for minimizing risk and ensuring that companies hire and promote the best people for the job.⁸⁴ However, the decision also "serves as a reminder that employers must carefully evaluate the methods by which they obtain and store background information."⁸⁵ While the Court did not conclude that employers have unlimited authority to conduct background searches, it did uphold the authority of public employers to use searches that are similar to the standard background searches conducted by employers in the private sector.⁸⁶ Probably the greatest unanswered question in *Nelson* is the status of a constitutional right to informational privacy. In *Nelson*, the Court assumed that the right

78 *Id.* at 138, 148.

79 *See id.* at 150 ("Reasonable investigations of applicants and employees aid the Government in ensuring the security of its facilities and in employing a competent, reliable work force.").

80 *See id.* at 149.

81 *Id.* at 151-53.

82 *Id.* at 154.

83 *Id.* at 155.

84 Barbara A. Lee & Nancy H. Van der Veer, *Supreme Court Rules for Employers and Upholds Constitutionality of Government Background Checks*, LEXOLOGY (Jan. 28, 2011), <https://www.lexology.com/library/detail.aspx?g=9efcf841-b262-44b8-94ea-3c9b72ac6acd>.

85 *Id.*

86 *Supreme Court Says Public Employers May Conduct Background Checks on Applicants*, PARKER POE (Jan. 18, 2011), <https://www.parkerpoe.com/news/2011/01/supreme-court-says-public-employers-may-conduct-background>.

exists, and since then there has been no resolution regarding the status of this right.⁸⁷ While the Court in *Nelson* was able to gloss over the question, a decade later it cannot be so easy; the threat of technological advancements in the hiring process on applicants' privacy has made this question of a right to informational privacy imminent.

II. EXTENSION TO SOCIAL MEDIA SCREENING

A. Current Trends, Benefits, and Criticism

One of the biggest developments in hiring practices in the 21st century has been the impact of social media on employers' abilities to connect with potential applicants and gain information about an applicant.⁸⁸ According to a national study that surveyed over 1,000 hiring managers across industries and company sizes, 70% of employers use social media sites to research job candidates, and this has come to be known as a "social media background check."⁸⁹ The availability of social media for screening applicants has significantly changed the hiring process. Through a traditional background check, an employer could obtain information about an applicant's legal status, employment, education, motor vehicle records, criminal charges, and credit history.⁹⁰ However, this background search did not provide information about the "more social and interactive aspects" of an applicant.⁹¹ While it used to take an in-person interview, where an applicant is typically on their best

87 See Wade A. Schilling, Note, *You Want to Know What?: NASA v Nelson and the Constitutional Right to Informational Privacy in an Ever-Changing World*, 82 UMKC L. REV. 823, 824 (2014) ("The status of a constitutional right to informational privacy is an unequivocal 'who knows.'").

88 See Kimberlee Morrison, *Survey: 92% of Recruiters Use Social Media to Find High-Quality Candidates*, ADWEEK (Sept. 22, 2015), <http://www.adweek.com/digital/survey-96-of-recruiters-use-social-media-to-find-high-quality-candidates/> (noting the large role social media plays in the job recruitment process). See also Tom Starmer, *Criminal-Background Checks, Social-Media Screening on the Rise*, HUM. RES. EXEC. (Mar. 20, 2019), <https://hrexecutive.com/criminal-background-checks-social-media-screening-on-the-rise/> (explaining how employers have increased background screening through social media).

89 *Employers Continue Rejecting Job Seekers Because of Social Media Content*, CBIA (Aug. 16, 2018), <https://www.cbia.com/news/hr-safety/employers-continue-rejecting-jobseekers-social-media/>. See also *A Complete Understanding of Social Media Background Checks*, CFIRST (Jun. 18, 2019), <https://www.cfirstcorp.com/understanding-social-media-background-checks/> (noting that employers searching through social media has become a "key element in our everyday lives").

90 Howard, *supra* note 3.

91 Ryan Howard, *Can You Include Social Media in Background Checks?*, VERIFIRST BACKGROUND SCREENING (Feb. 9, 2019), <https://blog.verifirst.com/can-you-include-social-media-in-background-checks>.

behavior, for an employer to learn these aspects of person, they can now see an applicant's personality and personal preferences via a social media background search.⁹²

These social media background checks have led to positive and negative results for applicants, as employers have found content on social networking sites that has led them to either not hire or hire a candidate.⁹³ Some of the content that has led employers to not hire candidates includes posts with inappropriate photographs or information (40%), information about the applicant drinking or using drugs (36%), discriminatory comments related to race, gender, or religion (31%), evidence of poor communication skills (27%), an unprofessional screen name (22%), and posting too frequently (12%).⁹⁴ In addition, almost half of all employers say that they are less likely to call an applicant in for an interview if they cannot find them online, either because they expect the candidate to have an online presence or because they like to gather more information before calling the candidate in for an interview.⁹⁵ On the other hand, the survey showed that social media searches can help an applicant. For example, some content that caused employers to hire applicants includes posts that support their professional qualifications for the job (37%), prove creativity (34%), convey a professional image (33%), show a wide range of interests (31%), and prove the candidate's personality fits with the company's culture (31%).⁹⁶

Employers have turned to social media to screen applicants because of the numerous benefits it provides. As previously highlighted, an employer is expected to make a reasonable investigation into an applicant's history to help avoid liability for negligent hiring. Therefore, including social media background checks can be a reasonable way to check if an applicant is dangerous or unproductive.⁹⁷ Screening an applicant's social media might even become a requirement to preventing negligent hiring liability, given the ease with which employers can conduct these searches. In addition, social media background checks can illustrate an applicant's skills in ways a traditional background check cannot. For example, more job candidates are

92 *Id.*

93 *See Employers Continue Rejecting Jobseekers Because of Social Media Content*, *supra* note 89 (noting that some employers have decided not to hire candidates due to content found on their social media accounts).

94 *Id.*

95 *Id.*

96 *Id.*

97 Chad Brooks, *The Pros and Cons of Social Media Background Checks*, BUS. NEWS DAILY (Aug. 2, 2016), <https://www.businessnewsdaily.com/9289-social-media-background-checks.html>.

using blog posts on LinkedIn or videos on YouTube to “show off their portfolio of work.”⁹⁸ These posts arguably show who the applicant “really is,” as opposed to just the version of themselves they choose to present through a resume and interview.⁹⁹

While using social media to screen applicants does have its benefits, it also poses a number of challenges. Some experts suggest that, because this is such a new phenomenon, there is no actual data showing that social media background checks actually identify people who are good fits for a certain job.¹⁰⁰ These searches could be causing a loss of qualified candidates, but since they are mostly used to reject candidates, it is difficult to test this; since the candidate was not hired, it is hard to know whether they would have actually failed if they had been hired.¹⁰¹ These experts suggest that the rise of social media background checks has to do with the easy access to this information, but warn that availability of social information does not necessarily mean it is a good measure for assessing job performance.¹⁰² Furthermore, many employers don’t have well-developed processes for screening applicants on social media the way they did for traditional background check methods.¹⁰³ Without applicable training, employers don’t necessarily know how to assess factors that are not job related or how to maintain consistency in assessing multiple candidates.¹⁰⁴

Employers generally use two methods for screening applicants on social media, and each poses different potential legal challenges. An employer conducting the search internally is the most common method for accessing information about an applicant online.¹⁰⁵ This method is quick, convenient,

98 *Id.*

99 Michael Klazema, *The Pros and Cons of Doing Social Media Background Checks on Potential Employees*, SOC. MEDIA TODAY (Mar. 8, 2017), <https://www.socialmediatoday.com/social-networks/pros-and-cons-doing-social-media-background-checks-potential-employees>.

100 See John Sullivan, *The Top 10 Reasons Why Social Media Background Checks Are a Dumb Idea*, ERE RECRUITING INTEL (Aug. 20, 2018), <https://www.ere.net/the-top-10-reasons-why-social-media-background-checks-are-a-dumb-idea/> (“Currently, there is no publicly available business or academic data on the effectiveness of social media background checking.”).

101 See *id.* (arguing that because employers typically use social media content to reject candidates, it is difficult to determine whether a rejected candidate would have been successful at the job had they been hired).

102 *Id.*

103 See *id.* (noting that most hiring managers conduct social media background checks using “their own self-developed process”).

104 *Id.*

105 Rachel E. Lusk, *Facebook’s Newest Friend—Employers: Use of Social Networking in Hiring Challenges U.S. Privacy Constructs*, 42 CAP. U. L. REV. 709, 721 (2014).

and anonymous.¹⁰⁶ All an employer needs to do is type the applicant's name into the Google, Facebook, or LinkedIn search bar, and they will likely be able to find the applicant's personal profile.¹⁰⁷ However, this method poses serious legal risks for employers. When individuals use social media, they "meld the personal and the professional," and it is easy for employers to become aware of personal characteristics that are inappropriate to take into consideration when making hiring decisions.¹⁰⁸

The second method involves going through a third-party company that conducts the social media background check on behalf of the employer. One example of this is Social Intelligence Corporation, which is an internet and social media background screening service that is used by employers to conduct background checks via social media.¹⁰⁹ These companies create reports that include public information collected from social networking sites.¹¹⁰ However, because these companies are considered consumer reporting agencies, they must comply with the FCRA, which includes notifying applicants of adverse actions taken because of the report.¹¹¹ In 2011, the FTC investigated Social Intelligence to determine whether it was complying with the FCRA.¹¹² The FTC ultimately suspended its investigation, albeit without determining whether a violation had occurred. Nevertheless, this likely

106 Nathan J. Ebnet, Note, *It Can Do More Than Protect Your Credit Score: Regulating Social Media Pre-Employment Screening with the Fair Credit Reporting Act*, 97 MINN. L. REV. 306, 320 (2012).

107 The extent to which they will be able to see information related to the applicant might depend on the applicant's utilization of the social media site's privacy setting. Lusk, *supra* note 104, at 721.

108 For example, a hiring manager might search someone's Twitter feed and through that become aware that the applicant has a medical condition. The manager might be concerned that the applicant will have to miss work because of this, and therefore decides not to hire the applicant. However, under the ADA this is unlawful discrimination. Meredith Levinson, *Social Networks: A New Hotbed for Hiring Discrimination Claims*, CIO (Apr. 18, 2011, 7:00 AM), <https://www.cio.com/article/2409045/social-networks--a-new-hotbed-for-hiring-discrimination-claims.html>. See also *Hardin v. Dadlani*, 221 F. Supp. 3d 87, 102 (D.D.C. 2016) (concluding that since Dadlani had previously expressed a preference for white female employees, his instructions to an employee to look up an applicant on Facebook and invite her in for an interview "if she looks good" can be reasonably construed to refer to her race, which can establish discriminatory animus).

109 *The Social Intelligence Story*, SOC. INTEL., <https://www.socialintel.com/about> (last visited Nov. 1, 2020).

110 Letter from Maneesha Mithal, Associate Director, Division of Privacy and Identity Protection, Bureau of Consumer Protection, FTC, to Renee Jackson, Nixon Peabody LLP (May 9, 2011), https://www.ftc.gov/sites/default/files/documents/closing_letters/social-intelligence-corporation/110509socialintelligenceletter.pdf.

111 *Id.*

112 *Id.*

indicates that these social media screening companies are legal, as long as they comply with the FCRA.¹¹³

B. Privacy Implications

The expansion of background checks to the realm of social media has created immense implications for the privacy of anyone applying for a job. While the traditional background check has a rather narrow focus on factors related to the workplace, screening an applicant on social media tells the employer much more about the applicant than what is immediately relevant to most jobs.¹¹⁴ Although some people believe that it is important for employers to understand everything about a person before making a hiring decision,¹¹⁵ others believe that there should be a separation between the personal and the professional.¹¹⁶ A key element to the argument against using social media to screen applicants is job-relatedness; employers' hiring decisions should not depend on whose "lifestyle choices resonate with, or least offend, an employer," but rather who is most qualified for the job.¹¹⁷ While some might think this issue of job-relatedness is not important, greater concerns for society arise when people are not able to get jobs because of reasons unrelated to their skills.¹¹⁸

113 Kashmir Hill, *Feds Okay Start-up That Monitors Employees' Internet and Social Media Footprints*, FORBES (June 15, 2011, 3:34 PM), <https://www.forbes.com/sites/kashmirhill/2011/06/15/start-up-that-monitors-employees-internet-and-social-media-footprints-gets-gov-approval/#539aa2d56411>.

114 See Sullivan, *supra* note 100 ("Most of the information that is found on social media sites covers areas that are 'social,' which means that they cover activities mostly outside of work.")₂.

115 See *Are Social Media Background Checks Worth the Risk?*, TRUSTED EMPs. (Aug. 21, 2019), <https://www.trustedemployees.com/learning-center/articles-news/social-media-background-checks/> ("When you get the whole picture of your candidate's character, you'll know if this is the person best suited for the job.")

116 See Michael Klazema, *From Discrimination to Invasions of Privacy: The Dangers of Social Media Background Checks*, BETA NEWS (2018), <https://betanews.com/2018/07/10/social-media-background-checks/> (arguing that while posting photos of oneself drinking or wearing provocative clothing might be distasteful, if they aren't happening on work property or during business hours then they aren't relevant to hiring decisions). See also Teri Root and Sandra McKay, *Student Awareness of the Use of Social Media Screening by Prospective Employers*, 89 J. OF EDUC. FOR BUS. 202, 203 (2014) (noting that people felt comfortable with employers looking at professional networking sites but didn't think it was reasonable for them to screen social media sites).

117 Ebnet, *supra* note 106, at 322. See also Corey M. Dennis, *Legal Implications of Employee Social Media Use*, 93 MASS. L. REV. 380, 381-92 (2011) (arguing that although social media screens might satisfy employers' curiosity about an applicant, traditional background checks are sufficient for meeting most employers' need to hire the best candidate).

118 See Eugene Frid, *Background Checks and Employment Discrimination: Distant Parallels Between U.S. and EU Privacy Regimes*, 40 HASTINGS INT'L & COMP. L. REV. 159, 160 (2017) (explaining that it distorts the market when people cannot contribute financially to the market, and that on an

Consider the story of Emily Clow, who applied for a marketing position in a Texas start-up.¹¹⁹ The company recommended that Clow follow them on social media, since social media is a major aspect of marketing these days.¹²⁰ However, Clow later saw the company photo-shame her on their own Instagram account, saying that a picture she posted on her personal Instagram account in a bathing suit was unprofessional.¹²¹ One journalist's comment on the story reflects why this situation upset so many: "It's 2019, and posting bikini photos (or any photo wearing whatever the heck you want) should not disqualify you from being hired."¹²²

Ultimately, the availability of vast amounts of information on the internet has changed the way people interact with one another and define themselves.¹²³ What was once a society of forgiving and forgetting has become a society where "the permanent memory bank of the Web increasingly means there are *no* second chances."¹²⁴ However, people differ in their opinions of whether a decrease in privacy has become the norm, or whether, despite the easy access to information, people maintain a desire for privacy. Facebook founder Mark Zuckerberg has suggested that current social norms favor exposure over privacy.¹²⁵ He believes that society has evolved to a point where people are comfortable sharing information more openly with different types of people.¹²⁶ However, some studies suggest otherwise. A University of California study from April 2011 found that a majority of people surveyed

individual level this prevents people from living out their "core American privilege" of being able to "engage in any common occupations of life").

119 Minyvonne Burke & Courtney Brogle, *Texas Woman Says Potential Employer Shamed Her over Bikini Photo*, NBC (Oct. 3, 2019, 12:13 PM), <https://www.nbcnews.com/news/us-news/texas-woman-says-potential-employer-shamed-her-over-bikini-photo-n1061946>.

120 *Id.*

121 *Id.*

122 Faith Brar, *This Woman Was Shamed By Her Potential Employer for Posting Bikini Pics On Her Instagram*, SHAPE (Oct. 4, 2019), <https://www.shape.com/lifestyle/mind-and-body/emily-clow-shamed-by-employer-for-bikini-photos-instagram>.

123 See Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES MAG. (July 21, 2010), <https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html> ("Facebook users share more than 25 billion pieces of content each month . . . and the Library of Congress recently announced it will be acquiring—and permanently storing—the entire archive of public Twitter posts since 2006.").

124 Citing cyberscholar Viktor Mayer-Schönberger, Rosen shares that forgetting and forgiving has allowed human beings to learn from past experiences and adjust behavior accordingly. *Id.* However, the Web is making it increasingly more difficult to move on from our mistakes and forgive others. *See id.*

125 *See id.* (remarking that Facebook has an obligation to reflect current social norms, which favor exposure over privacy).

126 *See id.* ("People have really gotten comfortable not only sharing more information and different kinds but more openly and with more people, and that social norm is just something that has evolved over time.").

between the ages of 18 and 22 think there should be laws that “require Web sites to delete all stored information about individuals (88 percent)” and that “give people the right to know all the information Web sites know about them (62 percent).”¹²⁷ Another study found that individuals between the ages of 18 and 29 are actually more concerned than older people with the image of themselves that is displayed online.¹²⁸ These studies suggest that not everyone is willing to accept the idea that there should be blanket permission for anyone to access information about others on social media.¹²⁹

C. Pitfalls of Traditional Background Check Regulation in Its Application to Social Media Background Checks

Although social media background checks have become a typical part of the hiring process, the laws that regulate traditional background checks have failed to keep up; rather, they are inadequate for combating the challenges associated with screening applicants on social media. The combination of the FCRA and federal antidiscrimination laws, which provide protection for applicants regardless of whether an employer conducts a background check internally or outsources to screening agency, leaves a gap when it comes to social media. The FTC’s inclusion of social media screening agencies such as Social Intelligence into the category of agencies that must comply with the FCRA does provide protection when these third-party screening agencies are actually used.¹³⁰ However, the ease with which employers can access this information themselves encourages them to conduct quick social media searches internally rather than outsourcing to these third-party agencies.¹³¹ Employers can still run into trouble with federal antidiscrimination laws if they screen an applicant on social media and become aware of a protected characteristic; however, it might be hard to prove that this was the reason the

127 *Id.*

128 *See id.* (finding that adults between the ages of 18 and 29 are “coming to understand the dangers of oversharing.”).

129 *See generally id.* (“[A] humane society values privacy, because it allows people to cultivate different aspects of their personalities in different contexts.”).

130 *See* SOCIAL INTELLIGENCE, *supra* note 109 (discussing FCRA protections that apply to social media screening agencies, such as the requirement to provide notice of the background check, and to give the applicant the opportunity to correct any mistakes in the background check); *see also* Lesley Fair, *The Fair Credit Reporting Act & social media: What businesses should know*, FTC.gov (June 23, 2011), <https://www.ftc.gov/news-events/blogs/business-blog/2011/06/fair-credit-reporting-act-social-media-what-businesses>.

131 *See* Nathan J. Ebnet, Note, *It Can Do More Than Protect Your Credit Score: Regulating Social Media Pre-Employment Screening with the Fair Credit Reporting Act*, 97 MINN. L. REV. 306, 329 (2012) (describing the convenience of browsing social media pages in-house rather than outsourcing to third-party agencies).

employer didn't hire the candidate.¹³² Therefore, applicants run the risk of employers conducting social background checks on them with, and potentially without notice if they don't receive the job because of information discovered through the search.

The scope of current laws regulating background checks also poses challenges. For example, federal antidiscrimination laws only apply to people who fit into a specifically defined protected category, and many applicants who desire greater privacy in the information on their social media accounts might not fit into a specific protected category.¹³³ In addition, these laws do not reach what many believe is a major downside to employers using social media to screen applicants; employers are not necessarily looking for information about the applicants' age, race or religion, but they are looking for social and personality traits.¹³⁴ While these aren't protected characteristics under antidiscrimination laws, many applicants still believe that whether they occasionally drink alcohol or wear certain clothing on weekends shouldn't be taken into consideration in hiring decisions.¹³⁵ It is also possible that some employers' judgments about what they find on social media may contain implicit gender biases based on unlawful sex stereotyping or other biases, but they are still able to maintain that their decision was made because of unprofessionalism rather than sex or other forms of discrimination.¹³⁶

III. AVENUES FOR ENSURING ADEQUATE PROTECTION

The laws regulating traditional background checks are inadequate for providing much needed and desired privacy for applicants in the context of

132 Not every case will involve such a clear sign as a Post-It note on an applicant's file that states he was "too old" for the job. See Meridith Levinson, *Social Networks: A New Hotbed for Hiring Discrimination Claims*, IDG COMM. (Apr. 18, 2011), <https://www.cio.com/article/2409045/social-networks--a-new-hotbed-for-hiring-discrimination-claims.html>.

133 See *Protections Against Discrimination and Other Prohibited Practices*, FTC.gov, <https://www.ftc.gov/site-information/no-fear-act/protections-against-discrimination> (noting prohibitions on discriminating against applicants and employees "on the bases of race, color, religion, sex, national origin, disability, or age").

134 See Ebnet, *supra* note 131, at 321-22 ("Employers turn to social media in an effort to learn all manners of personal information . . .").

135 *Id.* at 320, 322 (allowing employers to exclude job applicants from consideration because of information found on their social media pages).

136 See Steven Strauss, *Applying for a Job? Better Delete Your Social Media Accounts*, L.A. TIMES (Jan. 7, 2016), <https://www.latimes.com/opinion/op-ed/la-oe-0107-strauss-employment-discrimination-online-20160107-story.html> ("[O]nline searches can covertly facilitate [discrimination].").

social media background checks. However, a variety of possible avenues exist for ensuring privacy protection in the hiring process in the age of social media. While some potential solutions have already surfaced in recent years, others require us to think critically about the ways we have historically thought of privacy and understand that we need to update our notion of privacy in the age of social media.

A. *Constitutional Protections*

Protection for applicants in the age of social media can be found through two main constitutional avenues. The first involves looking back to the Supreme Court's reasoning behind the constitutionality of traditional background checks in *NASA v. Nelson*.¹³⁷ The second requires us to update our notion of what a reasonable expectation of privacy is under the Fourth Amendment given technological advancements in the age of social media. These avenues are somewhat limited because constitutional protections and limitations are only directly applicable to public employers.¹³⁸ However, given that the federal government employs roughly 2.1 million people, constitutional implications do have a broad scope.¹³⁹

1. *Going Back to NASA v. Nelson: A Right to Informational Privacy*

The Supreme Court's reasoning in *NASA v. Nelson* supporting the constitutionality of background checks cannot be applied equally to social media background checks. As noted above, *Nelson* did not confirm or deny the existence of a right to informational privacy, but it assumed the right exists, and then held that the background check at issue was valid because it was sufficiently job-related.¹⁴⁰ Although the Court held that the government only had to prove the more lenient standard—that the questions on the background check were job-related as opposed to “necessary” or the “least restrictive means”—this lower standard is still hard to meet when looking at social media background checks.¹⁴¹ This is because, unlike traditional background checks,

137 562 U.S. 134 (2011).

138 See Alexander Naito, Note, *A Fourth Amendment Status Update: Applying Constitutional Privacy Protection to Employees' Social Media Use*, 14 U. PA. J. CONST. L. 849, 852 (2012) (noting that constitutional protections and limitations are directly applicable only to public employees).

139 CONG. RES. SERV., FEDERAL WORKFORCE STATISTICS SOURCES: OPM AND OMB 1 (2020).

140 See *Nelson*, 562 U.S. at 138, 148 (assuming the right to informational privacy exists, but holding that the background check at issue is valid as sufficiently job-related).

141 *Id.* at 151–53.

social media background checks are not always looking for skills that are related to the specific job for which the applicant is applying.¹⁴²

The *Nelson* court avoided addressing whether there exists a right to informational privacy because it found the background check at issue to be sufficiently job-related. However, the lack of job-relatedness in social media background checks forces us to confront the question of whether there should be a right to informational privacy.¹⁴³ Although the court did not confirm the existence of the right in *Nelson*, it did identify that the right exists in the cases of *Whalen v. Roe*¹⁴⁴ and *Nixon v. Administrator of General Services*¹⁴⁵ without defining the scope of the right.¹⁴⁶ Furthermore, despite the lack of clarity from the Supreme Court in *Nelson*, every circuit (other than the D.C. Circuit) has recognized a constitutional right to informational privacy.¹⁴⁷ Given this consensus that the right exists, albeit with differing approaches on the scope of the right, the Supreme Court should revisit this question to both establish that a right to informational privacy exists and define the scope of this right.¹⁴⁸ In doing so, the Court would be providing much needed constitutional protection for private information contained on the web, which, at least for applicants to public jobs, would provide a shield against unreasonable employer access to personal information.

142 See John Sullivan, *The Top 10 Reasons Why Social Media Background Checks Are a Dumb Idea*, ERE MEDIA (Aug. 20, 2018), <https://www.ere.net/the-top-10-reasons-why-social-media-background-checks-are-a-dumb-idea/> (noting that social media background checks do not “verify positive job-related information”).

143 A right to informational privacy would fall under the Fourteenth Amendment substantive due process doctrine as opposed to the Fourth Amendment privacy doctrine. See Sara E. Stratton, Note, *Passwords Please: Rethinking the Constitutional Right to Informational Privacy in the Context of Social Media*, 41 HASTINGS CONST. L.Q. 649, 652 (2014) (arguing in favor of this right from a Fourteenth Amendment perspective).

144 In *Whalen*, the court recognized the “threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files,” but found that the New York statutory scheme provided sufficient protection of this right. 429 U.S. 589, 605 (1977).

145 In *Nixon*, the court recognized that public officials have a constitutionally protected privacy right in “matters of personal life,” and balanced this right against the public interest. 433 U.S. 425, 457–58 (1977).

146 See Stratton, *supra* note 140, at 668 (“While the Court in both cases identified the existence of a right to informational privacy, the Court did not define the scope of that right.”).

147 *Id.* at 672.

148 Stratton argues that the Supreme Court should establish a constitutional right to informational privacy. She further argues that, in analyzing a violation of this right, the Court should first consider whether an individual has a reasonable expectation of privacy. Then, if the right is implicated, the court should apply an intermediate scrutiny balancing test to determine if the right was violated. See *id.* at 677.

2. *A New Understanding of a Reasonable Expectation of Privacy Under the Fourth Amendment*

In addition to possible constitutional protection in the form of a right to informational privacy, another avenue for protecting applicants in the age of social media derives from courts coming to terms with a new understanding of what a reasonable expectation of privacy is under the Fourth Amendment, given the normalization of social media use. What constitutes a reasonable expectation of privacy has changed since its inception in the case of *Katz v. United States*.¹⁴⁹ Although at times the Court has restricted the definition of a reasonable expectation of privacy,¹⁵⁰ the Court has also been skeptical of the government's use of new technology in invading individuals' right to privacy.¹⁵¹ Specifically, when it comes to information disseminated on the internet, courts have been reluctant to find that every instance falls under the traditional third-party doctrine, whereby people concede their expectations of privacy when they give information over to a third party.¹⁵²

Courts have placed limitations on finding an objectively reasonable expectation of privacy in the information one shares on social media.¹⁵³ In *United States v. Meregildo*, the District Court in the Southern District of New York found that when an individual shares a picture on Facebook, they surrender their expectation of privacy because the possibility always exists that one of their "friends," who has access to the information they post, will share

149 389 U.S. 347 (1967) (finding warrantless searches and seizures that violate a reasonable expectation of privacy to be violative of the Fourth Amendment).

150 See *Florida v. Riley*, 488 U.S. 445, 450–51 (1989) (holding that the plaintiff did not have a reasonable expectation of privacy because he knowingly exposed his greenhouse to public observation from a helicopter flying overhead). See also *United States v. White*, 401 U.S. 745, 752 (1971) (finding that wiretapping an informant is not a violation of the Fourth Amendment because one does not have a reasonable expectation of privacy in the information they tell someone else, since they assume the risk that the person they talk to will report to the police).

151 In *Carpenter v. United States*, the Supreme Court discussed how the developing technology involving cellular phone site location tracking poses novel challenges. The Court declined to extend precedents to the case, and instead found that an individual does have a reasonable expectation of privacy in the record of his physical movements as captured by cell site location information technology. 138 S. Ct. 2206, 2216 (2018).

152 See *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 561 (S.D.N.Y. 2008) (holding that, despite the fact that emails go through a third-party service provider, an employee has a reasonable expectation of privacy in his personal email account and therefore his employer cannot access it without his permission).

153 Justice Harlan's guiding concurrence in *Katz* outlined a two-step approach; the first involved determining whether the individual has a subjective expectation of privacy, and the second being whether society has recognized that expectation as objectively reasonable. 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

the information with the public.¹⁵⁴ In *Chaney v. Fayette County Public School District*, the District Court in the Northern District of Georgia similarly found that individuals lose their expectation of privacy when they post photographs to Facebook, especially if, like in this case, the individuals have elected to share their posts with not only their friends, but also their friends' friends.¹⁵⁵

However, these lower court holdings ignore the reality of how many people use and understand social media forums. In her article *Facebook's Newest Friend - Employers: Use of Social Networking in Hiring Challenges U.S. Privacy Constructs*, Rachel E. Lusk discusses the importance of privacy statements in providing users with an expectation that their information will be kept private.¹⁵⁶ For example, the email service AOL has a privacy statement which assures users that their communication will be kept private, and in *United States v. Maxwell*, the court cited the existence of this policy in supporting its finding that users of AOL do maintain a reasonable expectation of privacy in their online communication.¹⁵⁷ Similarly, Facebook contains a privacy policy that "indicates that it is reasonable for users to expect a realm of privacy within the site."¹⁵⁸ For example, Facebook allows users to access, change, and erase their data,¹⁵⁹ and it allows users to control who sees their posts, choose whether to be tagged in photographs posted by others, and whether search engines outside of Facebook can link to their profile.¹⁶⁰ Like the AOL policy cited in *Maxwell*, these features suggest that users of social media platforms maintain an expectation of privacy in their use of these forums.¹⁶¹

Simply because an individual posts information on social media doesn't mean that they have lost all expectation of privacy in this information. One

154 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) (holding that the government can access Facebook posts through a cooperating witness who is a "friend" without violating the Fourth Amendment).

155 977 F. Supp. 2d 1308, 1316 (N.D. Ga. 2013) (noting that when the defendant posted to Facebook, she shared a photograph with "the broadest audience available to her").

156 42 CAP. U. L. REV. 709, 739-40 (2014).

157 See Lusk, *Facebook's Newest Friend—Employers* *supra* note 105, at 739 (citing *United States v. Maxwell*, 45 M.J. 406, 417 (C.A.A.F. 1996)).

158 *Id.* at 739.

159 *Data Policy: How can I manage or delete information about me?*, FACEBOOK (Aug. 21, 2020), <https://www.facebook.com/policy.php>.

160 *Privacy Settings and Tools*, FACEBOOK, <https://www.facebook.com/settings?tab=privacy> (last visited Nov. 5, 2020).

161 There is a recognized distinction between those that utilize the privacy features and those that allow their profiles to be set on "public." See Naito, *supra* note 138 at 876 (noting that when a user limits their online profile by requiring a password or allowing only certain other users to view their posts, then they have "an expectation that society is ready to recognize as reasonable," but if they do not take advantage of privacy features, "the expectation is no longer reasonable").

specific element of this argument involves the settings an individual chooses for their social media accounts. In *Oracle Am. Inc. v. Google Inc.*, which involved counsel searching jurors' social media in order to inform their peremptory challenges, the District Court for the Northern District of California discussed the importance of maintaining jurors' privacy.¹⁶² The court rejected the assertion that jurors, through their social media privacy settings, have chosen to expose their profiles to searches.¹⁶³ The court reasoned that "navigating privacy settings and fully understanding default settings is more a matter of blind faith than conscious choice."¹⁶⁴ In the discovery context, courts have also taken into account the expectation of privacy with regards to information posted on social media. For example, in *Landau v. Lamas*, the court considered the intimate and personal nature of social media in composing its social media discovery guidelines.¹⁶⁵ The court then held that the social media discovery requests failed for being overly broad.¹⁶⁶ These expectations of privacy on social media articulated by courts in both the jury selection and discovery contexts are similarly relevant in the social media background check context.

The way we think about expectations of privacy in public spaces can also inform how we should conceptualize an individual's expectation of privacy in the social media context. It is well established in Fourth Amendment jurisprudence that an individual does not maintain an expectation of privacy in the information they knowingly expose to the public.¹⁶⁷ Some judges have analogized the internet and social media to a public street, and therefore held that information that is posted on the internet is akin to information that is knowingly exposed to the public.¹⁶⁸ However, equating public streets to social media platforms on the internet, and thereby using the same legal analysis for

162 172 F. Supp. 3d 1100, 1103 (N.D. Cal. 2016).

163 *See id.* (stating that jurors have a protected right to privacy which "should yield only as necessary to reveal bias or a reluctance to follow the Court's instructions," and does not allow counsel to mine jurors' social media in order to make "calculated personal appeals" to them).

164 *Id.*

165 No. 3:15-CV-1327, 2017 U.S. Dist. LEXIS 206158, at *13 (M.D. Pa. Dec. 15, 2017).

166 *See Landau*, 2017 U.S. Dist. LEXIS 206158, at *21 (denying a plaintiff's request to inspect the defendant correctional officer's cell phone because the plaintiff relied on broad speculation as to the sexual activities and motives of the defendant and other correctional officers).

167 *See Katz v. United States*, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."). *See also* *Oliver v. United States*, 466 U.S. 170, 179 (1984) (holding that society does not recognize a reasonable expectation of privacy in activity that occurs in open fields).

168 *See People v. Harris*, 36 Misc. 3d 868, 873 (Crim. Ct. 2012) ("[T]oday, the street is an online, information superhighway, and the witnesses can be the third-party providers like Twitter, Facebook, Instagram [sic], Pinterest, or the next hot social media application.").

both, ignores important differences and challenges presented by online technology. The Supreme Court has acknowledged that technology poses novel challenges, as it has changed the ways we communicate with one another.¹⁶⁹ The Court has further acknowledged that the rise of technology impacts what society accepts as reasonable, which could strengthen arguments in favor of expectations of privacy, even on the internet.¹⁷⁰

Even if one looks at social media as a public forum, whereby an individual is knowingly exposing their information to the public, legal precedent regarding government surveillance can still support limitations on public employers' ability to broadly screen applicants on social media. In *Nader v. General Motors Corp.*, the Court of Appeals of New York noted that “[a] person does not automatically make public everything he does merely by being in a public place,” and that extensive surveillance can be an invasion on an individual’s right to privacy even if the surveillance is conducted in public.¹⁷¹ The Supreme Court has recognized a distinction between short-term monitoring and long-term surveillance, finding that long-term GPS monitoring that creates a mosaic of an individual’s life is an invasion of that individual’s reasonable expectation of privacy.¹⁷² Although social media screening is not the same as GPS surveillance, an in-depth search conducted on social media can provide a mosaic of an individual’s private life that surpasses what the employer generally needs to know in order to make an informed hiring decision. As with the importance of the scope of GPS surveillance in determining its invasion of privacy, the scope of an employer’s social media background check similarly impacts whether the search is invasive. Therefore, even if social media is considered to be a public forum, applicants maintain a recognized expectation of privacy and should not be subjected to broad social media background checks.

169 See *Riley v. California*, 573 U.S. 373, 403 (2014) (“The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.”).

170 See *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 760 (2010) (“Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy.”).

171 25 N.Y.2d 560, 570 (1970).

172 See *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring) (“[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.”). See also *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018) (holding that the depth, breadth, comprehensive reach, and deeply revealing nature of Cell Site Location Information require Fourth Amendment protection).

Recognizing that social media users have a reasonable expectation of privacy does not mean that employers can never screen applicants using social media without violating their privacy rights. In fact, employers might need to conduct some screening on social media in order to limit liability for negligent hiring. Recognizing a constitutionally protected right allows for a balancing test between the applicants' rights and the legitimate need of the public employer to screen that applicant's social media.¹⁷³ This balancing test ultimately creates a nexus to job-relatedness, which is the crucial factor of traditional background checks that is missing in social media background checks. If public employers are required to consider, and potentially defend, their legitimate need to screen an applicant on social media, it is likely that they will restrict their searches to those that are related to the job for which the applicant is applying.

B. Statutory Solutions

Increased statutory protection is another possible avenue for protecting job applicants' privacy that has already proven to be relatively reliable. On the state level, notable laws have already been implemented that provide applicants with protection from employers trying to access their social media accounts. For example, prior to 2012 many employers required applicants to provide them with their usernames and passwords to their social media accounts.¹⁷⁴ Since then, almost half of all states have passed laws that prohibit employers from "asking applicants and employees for their social media login information, to bring up their social media pages in the employer's presence, to change their privacy settings to make the page accessible to the employer, or to add anyone as a 'friend' or contact to a social media page."¹⁷⁵ In 2019, five more states introduced legislation.¹⁷⁶ However, no federal law exists that prohibits employers from asking applicants to provide passwords to their

173 See Marisa Kay, *Reviving the Fourth Amendment: Reasonable Expectation of Privacy in a Cell Phone Age*, 50 J. MARSHALL L. REV. 555, 581 (2017) (asserting that the constitutionality of a governmental action should be determined by balancing governmental and individual interests in light of "society's privacy expectations").

174 See Lusk, *Facebook's Newest Friend—Employers*, *supra* note 105, at 726–27 (2014) (discussing federal government investigations and governmental actions against this practice beginning in 2012).

175 Sachi Barreiro, *State Laws on Social Media Password Requests By Employers*, NOLO, <https://www.nolo.com/legal-encyclopedia/state-laws-on-social-media-password-requests-by-employers.html> (last visited Nov. 4, 2020).

176 See *Access to Social Media Usernames and Passwords*, NAT'L CONF. OF STATE LEGISLATURES, <https://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx> (last visited Nov. 14, 2020) (providing an updated list of state bills and legislation regarding social media privacy).

social media accounts, and each state law provides varying levels of protection.¹⁷⁷

Updating the FCRA is a potential statutory solution on the federal level. While the FTC has stated that the Act should apply to third-party agencies that conduct social media background checks, a gap in protection still exists for employers who conduct these searches themselves. In his article *It Can Do More Than Protect Your Credit Score: Regulating Social Media Pre-Employment Screening with the Fair Credit Reporting Act*, Nathan J. Ebnet suggests amending the FCRA to require employers to use third parties when conducting social media background checks.¹⁷⁸ He suggests that this would also help create a market whereby many companies are competing for these services, and therefore provide better service at lower prices.¹⁷⁹ However, this solution poses potential enforcement challenges, because it would likely be very difficult to monitor employers to ensure that they are not conducting quick searches of applicants on social media.

C. Technological Solutions

Perhaps the solution to providing job applicants with greater privacy lies outside of the scope of what the law has to offer; rather, it is up to individuals themselves to understand and utilize security features on social media sites to afford themselves the utmost privacy in the hiring process.¹⁸⁰ The prevalence of news articles about data privacy and privacy breaches, especially by social media sites, has led to a greater concern among Americans regarding how

177 See *Social Networking & Computer Privacy*, WORKPLACE FAIRNESS, <https://www.workplacefairness.org/social-network-computer-privacy-workplace#3> (last visited Nov. 14, 2020) (advising employees asked for social media passwords by employers to check whether their state has protective laws for social media privacy, and, if so, the degree of protection offered). See also Lusk, *Facebook's Newest Friend—Employers* *supra* note 105, at 726 (noting federal attempts to amend the Federal Communications Process Reform Act, and the introduction of the Social Networking Online Protection Act and the Password Protection Act).

178 See Nathan J. Ebnet, Note, *It Can Do More Than Protect Your Credit Score: Regulating Social Media Pre-Employment Screening with the Fair Credit Reporting Act*, 97 MINN. L. REV. 306, 330, 336 (2012) (noting that the FCRA has the ability to effectively restrict, without prohibiting, the use of social media background checks).

179 See *id.* at 328.

180 See Rosen, *The Web Means the End of Forgetting*, *supra* note 123 (“[T]he most promising solutions to the problem of embarrassing but true information online may be not legal but technological ones. Instead of suing after the damage is done . . . we need to explore ways of pre-emptively making the offending words or pictures disappear.”).

personal information is collected and used online.¹⁸¹ This increased awareness might lead to greater utilization of privacy features. Ultimately, without constitutional protections surrounding data privacy as it relates to social media background checks, the best solution might be a combination of statutory and technological solutions. Job applicants should utilize privacy features and ensure that their information is not available to anyone in the general public, and laws such as those prohibiting employers from asking for usernames and passwords can close any loopholes that employers might attempt to go through.

CONCLUSION

While the use of background checks to prevent liability for negligent hiring has remained consistent throughout the past century, the method of conducting background checks has changed significantly. What was once a formalized process conducted primarily through third-party companies regulated by the FCRA has become a more informal process with the expansion to the social media background check. Looking into an applicant's personal history has always raised privacy concerns, but the laws that protected applicants in the era of traditional background checks have been insufficient for providing adequate protection for applicants subjected to social media background checks. Through some combination of recognizing a new right to privacy or changing our current understanding of privacy, enacting statutory protections, and developing privacy-enhancing technology, we must find a way in the age of social media to balance an employer's need to look into a candidate's history with that candidate's need for privacy.

181 See Lee Rainie, *Americans' Complicated Feelings About Social Media in an Era of Privacy Concerns*, PEW RSCH. CTR. (Mar. 27, 2018), <https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/> (citing a 2014 survey indicating that 80 percent of American social media users are "concerned about advertisers and businesses accessing the data they share on social media platforms").