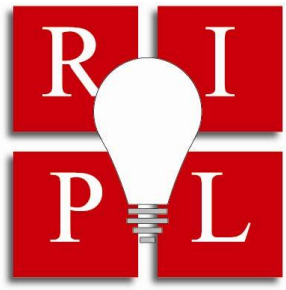
THE JOHN MARSHALL
REVIEW OF INTELLECTUAL PROPERTY LAW



THE EMERGING REALITY OF SOCIAL MEDIA: EROSION OF INDIVIDUAL PRIVACY THROUGH CYBER-VETTING AND LAW'S INABILITY TO CATCH UP

DR. SABY GHOSHRAY

ABSTRACT

The rise of social media means that data about a large number of people is available in public and quasi-public digital locations. Employers, keen on taking advantage of this additional data to decrease the risk associated with an offer of employment, are engaging in "cyber-vetting"—non-consenting social media searches conducted by third parties or the employers themselves. To the extent that current law applies to this practice, the regulation it provides is weak and attacks only part of the problem. Left unchecked, cyber-vetting has the potential to fundamentally alter the scope of prospective employees' rights. This article surveys the legal and practical implications of cyber-vetting and suggests broad reforms focused on intelligently balancing individual rights and legitimate employer interests.

Cite as Dr. Saby Ghoshray, *The Emerging Reality of Social Media: Erosion of Individual Privacy Through Cyber-vetting and Law's Inability to Catch Up*, 12 J. MARSHALL REV. INTELL. PROP. L. 551 (2013).

THE EMERGING REALITY OF SOCIAL MEDIA: EROSION OF INDIVIDUAL PRIVACY THROUGH CYBER-VETTING AND LAW'S INABILITY TO CATCH UP

DR. SABY GHOSHRAY

THE EMERGING REALITY OF SOCIAL MEDIA: EROSION OF INDIVIDUAL PRIVACY THROUGH CYBER-VETTING AND LAW'S INABILITY TO CATCH UP

DR. SABY GHOSHRAY*

INTRODUCTION

One of the significant technological advancements of contemporary society manifests itself in the access, ease and speed of communication in cyberspace.[1] The development of this game-changing technology allowed economies of scale to shape pricing in favor of widespread use of search engines and social networking sites, unleashing a pervasive digital immersion within society. As public agencies and governmental entities continue to make public records available online,[2] individual exuberance in social media has generated a culture of rampant sharing of private affairs with strangers on the Internet.[3] Against this dynamic backdrop, this article examines the danger to individual privacy emanating from the emerging practice of employment screening based on an individual's online activities. As instantaneous

---

* © Dr. Saby Ghoshray 2013. Dr. Saby Ghoshray's scholarship focuses on subsets of International Law, Constitutional Law, Cyberspace Law, Technology & Fourth Amendment, among others. His work has appeared in a number of publications including Albany Law Review, ILSA Journal of International and Comparative Law, European Law Journal ERA-Forum, Toledo Law Review, Georgetown International Environmental Law Review, Temple Political & Civil Rights Law Review, Fordham International Law Journal, Santa Clara Law Review, Michigan State International Law Journal, Loyola Law Journal and Washburn Law Journal, among others. The author would like to thank Jennifer Schulke for her assistance in legal research and typing of the manuscript. Much love to his beautiful children, Shreyoshi and Sayantan, for their patience and understanding. I offer much appreciation to the members of the John Marshall Review of Intellectual Property Law for their dedication in the edit process. Dr. Ghoshray can be reached at sabyghoshray@sbcglobal.net.

[1] *See Net Impact: US Becomes a Facebook Nation*, BUS. NEWS DAILY (Apr. 6, 2011, 4:20 PM), http://www.businessnewsdaily.com/840-facebook-smartphone-majority-americans-online-.html (describing the multitude of ways Americans use technology in their everyday lives).

[2] Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1139 (2002).

[3] *See* Kieron O'Hara et al., *Lifelogging: Privacy and Empowerment with Memories for Life*, 1 IDENTITY IN INFO. SOC'Y 155, 157 (2008), *available at* http://link.springer.com/content/pdf/10.1007%2Fs12394-009-0008-4.pdf. Technological advancement has allowed rapid enhancement in the functional aspects of information acquisition, sensor capacity, data streaming, and data storage and retrieval in the digital environment. *Id.* at 156. Mediated through the use of HDTV, smartphones, the Internet, and other devices, technology has allowed pervasive use and acclimatization of digital communication, empowering individuals to disseminate an unedited and non-discriminatory collection of personal information in cyberspace. This allows entities outside of the original intended recipient to access and investigate an abundance of personal information by following the digital trails of a person's online exchanges, enabling various entities to reconstruct a new locus of online identity. *Id.* at 156–58. Digital footprint refers to this locus of online identity an individual leaves behind in cyberspace crated through that individual's online interactions that ranges from shopping, email communication, cyberspace chat, social media interaction, sharing YouTube videos, etc. *Id.* at 156, 165 (observing the various modes and modicums of individual exchanges in cyberspace that enables the development of an emerging culture of online social presence where individuals shed personal privacy in documenting their lives in front of strangers).

access to information seeks to fundamentally alter society's behavioral norms, employment screening has almost become an organic extension of traditional background checks.[4] Yet, employment law has failed to adequately address privacy concerns in this context.[5]

The Internet offers an efficient method by which to obtain background information about prospective employees.[6] Because viewing an individual's social media activities may enable a potential employer to gain valuable insight into the applicant's behavioral profile, cyber-vetting has become the norm as opposed to an exception.[7] Cyber-vetting, however, is fundamentally different from the traditional employment screening in more significant ways than are currently acknowledged.[8]

What is the objective of employment screening? Whether performed via the traditional background check, or through the emerging practice of cyber-vetting, the objective of applicant screening is to analyze the submitted individual's profile for suitability with the hiring entity's corporate culture.[9] Widespread access to individuals' online activities has changed the employment screening landscape, as the search for the right candidate for a position based on expertise and qualifications has transmogrified into an exercise in seeking a desired behavioral profile. This development has created a much wider scope for discrimination based on behavioral norms.

---

[4] *See* Rosemary Haefner, *More Employers Screening Candidates via Social Networking Sites*, CAREERBUILDER.COM, http://www.careerbuilder.com/Article/CB-1337-Getting-Hired-More-Employers-Screening-Candidates-via-Social-Networking-Sites/?ArticleID=1337 (last updated June 10, 2009, 4:20 PM) (finding that forty-five percent of employers admitted to using social media to pre-screen job applicants).

[5] *See* DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 71, 75 (2004), *available at* http://docs.law.gwu.edu/facweb/dsolove/Digital-Person/text/Digital-Person-CH4.pdf (presenting a number of privacy issues that need to be addressed by employment law with the advent of social media).

[6] *See* Victoria R. Brown & E. Daly Vaughn, *The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decisions*, 26 J. BUS. & PSYCHOL. 219, 219 (2011), http://link.springer.com/content/pdf/10.1007%2Fs10869-011-9221-x (listing Facebook, LinkedIn, MySpace, and Twitter as popular platforms for employee background checks). Potential employers have dismissed employees based on information obtained via their social media content, revealing details that included, among others, provocative or inappropriate photographs or information, images showing drug or alcohol related activities, negative comments about prior employment, and discriminatory comments, which are all areas that can be covered within broader speech protection rights, unless prohibited by contractual obligations. *See, e.g.*, P. Haans Mulder & Nicholas R. Dekker, *Social Networking: Your Business Clients and Their Employees are Doing It*, MICH. BUS. L.J., Summer 2010, at 44, 45, *available at* www.michbar.org/business/BLJ/Summer%202010/mulder_dekker.pdf.

[7] *See* ANDRÉE ROSE ET AL., INT'L ASS'N OF CHIEFS OF POLICE, DEVELOPING A CYBERVETTING STRATEGY FOR LAW ENFORCEMENT 1 (2010), *available at* http://www.iacpsocialmedia.org/Portals/1/documents/CybervettingReport.pdf ("Cybervetting is an assessment of a person's suitability to hold a position using information found on the Internet to help make that determination.").

[8] *See* Brenda Berkelaar, Cyber-Vetting (Potential) Employees: An Emerging Area of Study for Organizational Communication, Paper Presented at the Annual Meeting of the International Communication Association, Montreal, Canada 5 (May 22, 2008) (unpublished manuscript), *available at* http://dpclo.defense.gov/civil/docs/ArticleCybervettingPotentialEmployees.pdf.

[9] Robert Sprague, *Rethinking Information Privacy in an Age of Online Transparency*, 25 HOFSTRA LAB. & EMP. L.J. 395, 397–98 (2008).

The emerging online-based employment screening differs significantly from its traditional counterpart. The traditional employment screening typically focuses on criminal records, financial credit scores, civil judgments against the candidate, and other process driven outcomes of deterministic events, mostly generated through judicial proceedings and consent-driven disclosures.[10] On the other hand, personal behavior based information collected on the Internet is predominantly an exercise in seeking individuals' digital footprints.[11] As detailed below, such a screening often times relies on imprecise, incomplete, and static data. On the other hand, records reviewed for traditional employment screens are typically based on deterministic outcomes of individual actions.[12] Both the results and the procedures to arrive at such outcomes can be challenged by the affected individual within a due process framework.[13] Individual records generated based on reviewing online activities and profiles result from non-deterministic events, which the affected individual may not get the opportunity to dispute or challenge. Thus, cyber-vetting may result in erroneous inferences based on generating informational vignettes lacking a deterministic element or a source with any possessory connection. Let us examine the following three illustrative scenarios.

> Scenario 1: It is the morning after Super Bowl 2013 and Jack is hung over. He has photos to upload to his public website, lots of photos which highlight Jack's night of partying with whisky, wine, and women. A weekend later, Jack finds himself uploading more photos showcasing his "drink of choice." He is quick to tag photos on his Facebook account. Over the next six-months, this routine is repeated numerous times. Jack's Facebook account reflects a guy who has lots of friends, enjoys socializing with whisky, and is always surrounded by many party girls. His Facebook page is full of tagged photos of his 115 friends, and his page includes a link to a famous bourbon company's Facebook page. Jack has no criminal record whatsoever and never drinks during the week. He simply likes to party on weekends. Jack is also in full-time pursuit of a new position. He is a well-qualified accountant with a Master's degree and a CPA license. He has worked at the same firm for three years, but is looking to relocate. At his last interview, he had impressed the team of first level interviewers and was called back for a second round of interviews by the senior executives. Jack was feeling confident. However, Jack was shocked to be informed by Human Resources ("HR") that the company was no longer interested. Jack thinks that his photo collage on his Facebook page may have influenced the HR Department's decision not to pursue him. Could this be true?

---

[10] *See* Elizabeth D. De Armond, *To Cloak the Within: Protecting Employees from Personality Testing*, 61 DEPAUL L. REV. 1129, 1134–36 (2012).

[11] *See* Sprague, *supra* note 9, at 399.

[12] *See* De Armond, *supra* note 10, at 1134–35.

[13] *Employment Background Checks*, FED. TRADE COMMISSION (Feb. 2013), http://www.consumer.ftc.gov/articles/0157-employment-background-checks.

Scenario 2: Jill was a front line analyst at an investment bank, but was laid off over a year ago when the economy went into decline. She has incredible talent, excellent references, and even received an additional certificate in project management while laid off. Nonetheless, she has not gotten any interview call backs. To earn a little money while unemployed, Jill has taken some glamour shots and posted them on her Facebook website. It has been her hope to break into modeling. Her glamour shots are not nude, but revealing. Some of her shots include poses on motorcycles and cars, in various outfits, and also with other models. Jill's Facebook page also describes her volunteerism, travels, and poetry. But Jill still thinks that every time she submits her resume, the company is first looking at her Facebook page and not calling her in for an interview. Could she be right?

Scenario 3: Eric is a mid-level executive at a Big Four firm. He uses social media very sparingly. He does not have a fan following. He does not have a Facebook page, and he does not tweet. For all practical purposes, he is virtually non-existent in the social media world. A couple of years earlier, Eric attended a controversial court proceeding in his hometown. He had no connection to the case whatsoever, other than mere curiosity, as the case received nationwide coverage. Eric attended only a few hour-long sessions of the case and, upon leaving the courtroom was stopped by a local television journalist and asked a few questions. He did not say anything extreme, but he did speak about his contrarian view of the case. Little did Eric know that his two minute interview would go viral, as his comments made nationwide news. His controversial views upset a lot of people, and the two-minute interview was uploaded to numerous websites, which played and replayed on popular news channels. Eric even received multiple requests to appear on television about his comments. He declined them all. Now, every time Eric types his own name in any search engine, the viral video always comes up first. The results always appear negative because of the viral video. Yet, Eric is an excellent employee and a devoted father of three, yet, he has not been given a raise in the last several years, whereas other, less qualified, employees are being promoted. He believes the HR department has done a search on him, and that the viral video is hurting his chances for promotion. Could he be right?

Of course, the above scenarios are merely hypothetical. Yet, they represent prototypical employment decisions unfolding in contemporary employment practices. At the core, the scenarios represent how the societal landscape is being shaped by individuals' immersion in social media. More importantly, they prompt us to reflect on how technology has changed our lives. Because contemporary individuals conduct aspects of their lives through electronic means, important decisions on their careers could be made based on a search of their digital footprints.[14] This dystopian reality is

[14] Michael Jones et al., *The Ethics of Pre-Employment Screening Through the Use of the Internet*, *in* THE ETHICAL IMPERATIVE IN THE CONTEXT OF EVOLVING TECHNOLOGIES 43 (Dan McIntosh et. al., eds., 2004).

a stark reminder of the uncertainties currently percolating through the employee-employer relationship. As this Pandora's box of legal indeterminacy opens up into corporate conference rooms, it has the potential to trickle into the Nation's courtrooms and administrative tribunals. Unless emerging employment law takes due cognizance of individuals' privacy rights by restraining employers' unbridled search of their online activities, judges and administrators will be thrust into the unenviable role of making significant decisions regarding people's lives and livelihoods, with only scarce legislative guidance.

As noted above, cyber-vetting is the search and examination of potential employees' digital footprints.[15] By uncovering information that is not readily available from the submitted application, an online search of a candidate's profile helps employers narrow their lists of candidates.[16] On the surface, however, cyber-vetting is premised on conducting legitimate due diligence in furtherance of a legitimate business interest. Yet, much more is implicated via cyber-vetting—an aspect that is missing in contemporary discussions. Smartphones, Android, Facebook, Twitter, and iChat, each represent a dimension through which post-modern individuals communicate.[17] As they live their lives wired, by connecting, uploading, downloading, and streaming online, not only do these individuals form communities, but they also exhibit emotions and share private details with their community members. Along the way, potential employees leave a digital footprint—of themselves and their friends—all of which is subject to inspection via cyber-vetting.

This disturbing trend toward über-surveillance of potential employees is an outgrowth of contemporary society's digital immersion into social media. By giving up a part of her privacy, through her social media activities, the applicant opens herself to an all-out investigation of her online persona. The lack of legislative guidelines compounds the conflict between an individual's privacy right and an employer's legitimate business interests. As enhanced functionalities within cyberspace have reconfigured the way individuals interact online, and in practically all aspects of modern life, yet the legal protection for such private communications has not evolved accordingly.[18]

The legal issues raised by this phenomenon go beyond an individual's right to privacy, viewing information outside of an applicant's submitted information, which exposes the employer to privileged information that it has no right to view. When an employer examines the content of an applicant's digital life conducted in cyberspace with her selected "friends," the employer could be exposed to a range of liabilities.[19] These could include having improper awareness of the protected status of an applicant,[20] making negligent and discriminatory hiring decisions based on

---

[15] *See* ROSE ET AL., *supra* note 7, at 1.

[16] *See* Sprague, *supra* note 9, at 399.

[17] *See How Social Media has Changed the Way We Communicate*, INFO. GATEWAY (Jan. 24, 2013, 6:00 PM), http://www.informationgateway.org/social-media-changed-communicate/.

[18] Alissa Del Riego et al., *Your Password or Your Paycheck? A Job Applicant's Murky Right to Social Media Privacy*, J. INTERNET L., Sept. 2012, 1, 18, 21–22 ("It is no secret that privacy law has had trouble catching up with modern technology.").

[19] *See id.* at 18.

[20] *See, e.g.*, Gaskell v. Univ. of Ky., No. 09-244-KSF, 2010 WL 4867630, at *1–5 (E.D. Ky. Nov. 23, 2010) (explaining that a potential employee was a great candidate based on his application, but

inaccurate or misleading information,[21] and intruding on an applicant's personal space.[22] For these applicants, searching for a job must not mean relinquishing their fundamental right to protect their online privacy, which includes their protected status in social media. This article, therefore, intends to trace the locus of this emerging disconnect between an individual's fundamental right and an employer's current practice against the emerging social media exuberance. It will proceed as follows.

Part II examines the current landscape of digital immersion in contemporary society to better understand the background that facilitated the emergence of this newer social media exuberance. Although the linkages between social media exuberance and employer surveillance has not been established as a matter of law, their relationship would be informative to analyze. Part II also analyzes the reasons and examines societal factors that have given rise to the law's evolution in this direction.

Part III examines how current Fourth Amendment jurisprudence can be applicable in identifying how individual behaviors may be framed within the confines of settled jurisprudence. By analyzing the aspirational dimensions of constitutional cases to find analogous behavior in the post-modern era, this section develops a nuanced understanding of the employer's current penchant for über-surveillance.

Part IV examines individual behavior in social media, which may have a definite link in abrogating individuals' subjective expectation of privacy. By developing a set of fundamentals, this section drives home the point that the contemporary society's digital immersion is a natural outgrowth of human evolution. Yet, technology-fuelled surveillance of ordinary citizens must not be allowed to implicate fundamental liberties of individuals. The discussion above leads to a development in Part V, outlining the allowable trajectory of online searches for cyber-vetting of potential applicants.

Finally, Part VI concludes that Fourth Amendment jurisprudence may still be robust enough to address complexities arising out of social media behavior and its implications in applicant-employer relationships.

I. SETTING THE LANDSCAPE OF APPLICANT—EMPLOYEE RELATIONSHIP

Combining efficiency in data mining algorithms with enhancement in computational speed and storage capability, data analytics can extract behavioral patterns from conglomeration of personal information.[23] Fast transitioning from an emerging phenomenon to a conventional practice, the combination of data

---

was not hired after an Internet search was conducted, which revealed the candidate's religious preferences).

[21] *See* Laurie Ruettimann, *Don't Facebook Me: Why You Shouldn't Google During the Recruiting Process*, TLNT (Oct. 4, 2010, 8:07 AM), http://www.tlnt.com/2010/10/04/dont-facebook-me-why-you-shouldnt-google-during-the-recruiting-process/.

[22] *See* Del Riego et al., *supra* note 18, at 18.

[23] Tal Z. Zarsky, *Government Data Mining and its Alternatives*, 116 PENN ST. L. REV. 285, 287 (2011) (stating that data mining may not only be successful in the commercial realm, but also for governmental actions).

aggregation and personal profile searches has come to be known as "big data."[24] In the absence of mature privacy laws, operating outside the ethical bounds of society, big data has given rise to a digital war against privacy.[25] Emboldened by its ease of access and cost advantage, corporate entities utilize big data to access private information on individuals. Their social media exuberance, often times unbeknownst to them, compels individuals to leave behind personal details via digital exchanges in cyberspace.[26] Big data is more than happy to collect and process such information, enabling corporations and government agencies to utilize them for behavioral prediction modeling.[27] Cyber-vetting of a potential employee must be seen through this emerging reality.

Having everyone's privacy at the click of a mouse allows a potential employer to conduct pre-employment screening of individuals by reviewing minute details of their private affairs. We must prompt ourselves to explore the fundamental question: Just how little are we prepared to value our individual privacy? At its root, big data-driven exploration into an individual's zone of private seclusion is really an intrusion into the individual's personal space—a classic search and seizure without any warrant or probable cause.[28] If more employers utilize data mining and social media searches to screen potential employees, intrusion into individual's private personal space will become a conventional practice in society. Must a civilized society allow this?

Privacy is a fundamental liberty component.[29] For each unique individual, conceptualization of privacy varies for different stages of life and society. Yet, every individual has an inherent right to be left alone within her personal confines.[30] Thus, there is a fundamental distinction between employee surveillance within the work place and violating an applicant's privacy during pre-employment screening.[31] Given

---

[24] *Big Data—What Is It?*, SAS, http://www.sas.com/big-data/ (last visited May 21, 2013).

[25] *See* Joseph S. Fulda, *Data Mining and Privacy*, 11 ALB. L.J. SCI. & TECH. 105, 106 (2000) (questioning whether data mining is a violation of privacy that should be limited by law).

[26] *See* John Soma, Melodi Mosley Gates & Michael Smith, *Bit-Wise But Privacy Foolish: Smarter E-Messaging Technologies Call for a Return to Core Privacy Principles,* 20 ALB. L.J. SCI. & TECH. 487, 504–05 (2010).

[27] *See* Zarsky, *supra* note 23, at 287 (indicating that data mining is vastly becoming a tool that government agencies use on individuals, which poses risks to security).

[28] *See* Wayne N. Renke, *Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy*, 43 ALBERTA L. REV. 779, 789, 812 (2006) (explaining specifically that data mining is highly intrusive in relation to personal information).

[29] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 214–15 (1890) (discussing the need for privacy as technology developed in 1890). The sanctity of privacy as a fundamental right has illuminated the U.S. Constitution for more than a century. *Id*. at 193–95. The core privacy fundamental had emerged from a much deeper right-to-life interpretation with its roots embedded in the conception of liberty. *Id*. at 193–94. Therefore, individual privacy is recognized as an essential component of liberty. *Id*. at 193–94. Long before the technological onslaught of the post-modern era, Justice Warren and Justice Brandeis invoked a deeper fundamental right to privacy that has since been muted somewhat under the attack of states' heightened interests. *See id.* at 193.

[30] *See id*. at 195.

[31] Jon Vegosan, *Employee Monitoring and Pre-employment Screening*, RISK MGMT. MAG. (Oct. 1, 2010, 3:40 PM), http://www.rmmagazine.com/2010/10/01/employee-monitoring-and-pre-employment-screening (describing the distinction between employee monitoring and pre-employment screening, including the obligations and consequences of each).

how her deliberate immersion into online activities may have shaped her subjective expectation of privacy, the thresholds of privacy may vary amongst individuals.[32] This may prompt an employer to conduct limited surveillance at the workplace within allowable limits.[33] Such right to surveillance, however, cannot extend to an individual's private affairs during employment screening. Recognition of this distinction will do much to protect employers from liability for privacy violations.

Often times, an employer might be tempted to extend its surveillance mechanism for conducting a background search of a potential employee. Such surveillance should be recognized as falling outside the bounds of legal limits, as an employer may not intrude into the private affairs of a common citizen. This is particularly important because social media based networking sites have ushered in a new era of accessibility for private information. As more individuals immerse themselves in extensive online communications, they leave behind their digital footprints.[34] Although an individual's online behavior may signal changes in contemporary society's subjective expectation of privacy at the workplace, it certainly does not change the fundamental contours of the individual right to privacy.[35] Therefore, before engaging in a full-scale online search of a prospective employee, an employer must review its search criteria to ensure the privacy of that individual is not jeopardized.[36]

Search of a candidate's digital footprint is a valuable tool for employment screening.[37] Yet, an unbounded search of such a footprint may constitute an intrusion into an individual's privacy.[38] Thus, the scope of such a search must be carefully limited to insulate the employer from compliance violations, as legal risks could arise in multiple dimensions—from violation of consent requirements for third party screeners[39] to violation of online privacy.[40] Because the Internet is saturated with imprecise information and incomplete personal data, online background

---

[32] *See* Alexander Naito, *A Fourth Amendment Status Update: Applying Constitutional Privacy Protection to Employees' Social Media Use*, 14 U. PA. J. CONST. L. 849, 876 (2012).

[33] *See infra* Part V. *But see* Naito, *supra* note 32, at 863–64.

[34] *See supra* note 3 and accompanying text.

[35] *See* Naito, *supra* note 32, at 881–82.

[36] *See infra* Part IV; Naito, *supra* note 32, at 865 (explaining that a Fourth Amendment analysis into an employee's privacy should "involve a balance of the employer's interests and an evaluation as to the method by which the employer obtains the information").

[37] Naito, *supra* note 32, at 863–64.

[38] *See Employer Access to Social Media Usernames and Passwords: 2012 Legislation*, NAT'L CONF. ST. LEGISLATURES (Jan. 17, 2013), http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx (summarizing amended legislation from fourteen states that would restrict employers from requesting access to social networking usernames and passwords of applicants, students, or employees due to an invasion of privacy).

[39] *See* 18 U.S.C. § 2701 (2012) (subjecting anyone who intentionally accesses without authorization or exceeds an authorization to access the contents of electronic communication to punishments listed in 18 U.S.C. § 2701(b)).

[40] *See* 18 U.S.C. § 2702(a)(1)–(2) ("[A] person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service" or "the contents of any communication which is carried or maintained on that service.").

searches often provide the basis for erroneous inferences,[41] acting on which may expose an employer to potential liability for breach of anti-discrimination laws.[42]

Often times, individuals vent their frustrations or indulge in disparaging remarks during exchanges with members of their selected online communities.[43] This may result in prejudicial information getting stored online, especially within the pages of social media sites. Thus, social media driven pre-employment screening may result in the generation of an incomplete or faulty applicant profile.[44] This would certainly make employment decisions based on social media data prone to judgmental error and may lead to legal liability. Therefore, data collection for employment screening has several drawbacks. Besides the danger of being prejudicial and incomplete, data derived from online communication, often times, lack the proper context as the full exchange may not be readily available.[45] This data is qualitatively different from deterministic personal data obtained from criminal records or transactional databases like credit reports. Simply put, this data may not have originated through a verifiable dispute resolution mechanism.[46] Moreover, conducting background searches based on criminal registry or credit reports may have different consent requirements than social media based behavioral profile searches.[47]

---

[41] Dave Marcus & Patricia Kitchen, *Employers Scour Web for Details on Applicants*, NEWSDAY (July 23, 2010, 11:28 AM), http://www.newsday.com/classifieds/jobs/employers-scour-web-for-details-on-applicants-1.2133284 (discussing how employers would generate erroneous inferences from online background searches).

[42] *See* Sprague, *supra* note 9, at 416 (emphasizing that online background searches of potential employees may violate states' antidiscrimination prohibitions).

[43] *See, e.g.*, *Facebook Post Gets Worker Fired*, ESPN NFL (Mar. 9, 2009, 5:41 PM), http://sports.espn.go.com/nfl/news/story?id=3965039 ("A Facebook post criticizing his employer, the Philadelphia Eagles, cost a stadium operations worker his job . . . . According to the newspaper, Leone posted the following on his Facebook page: 'Dan is [expletive] devastated about Dawkins signing with Denver . . . Dam Eagles R Retarted [sic]!!'"); David Kravets, *AP Reporter Reprimanded for Facebook Posts; Union Protests*, WIRED (June 9, 2009, 4:40 PM), http://www.wired.com/threatlevel/2009/06/facebooksword (discussing how an Associated Press reporter's reprimand over a comment on his Facebook page sparked a demand that the Associated Press clarify its ethics guidelines).

[44] *See* Marcus & Kitchen, *supra* note 41.

[45] Sprague, *supra* note 9, at 397 n.19.

[46] *See infra* Part IV.

[47] See, for example, The Fair Credit Reporting Act ('FCRA"), 15 U.S.C. §§ 1681–1681x (2012), which imposes certain consent requirements on "consumer reporting agencies," a term which the Act defines broadly. 15 U.S.C. § 1681a ("The term 'consumer reporting agency' means any person which . . . regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ."); 15 U.S.C. § 1681b(b) (requiring consumer reporting agencies to obtain from the employers to whom they furnish reports certifications to the effect that the existence and nature of the reports have been disclosed to the subject consumers, and that the consumers have authorized the reports in writing, and requiring that the reports themselves be disclosed to any applicants or employees against whom the employers take adverse action). The Federal Trade Commission has stated its position that the FCRA applies to third party social media searches. Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Prot., Bureau of Consumer Prot., Fed. Trade Comm'n, to Renee Jackson, Nixon Peabody LLP (May 9, 2011) [hereinafter Mithal Letter], *available at* http://www.ftc.gov/os/closings/110509socialintelligenceletter.pdf. It is unclear what requirements would apply to a search conducted by the employer itself.

Thus, the emerging phenomenon of cyber-vetting is the creation of pervasive digital immersion in contemporary society and social media is shaping the future of employment relationships. Some reports suggest that as many as eighty percent of employers use social media to screen applicants.[48] Legal risks for employers, therefore, could escalate in the not too distant future, as the consequences of making hiring decisions based on information revealed via online searches becomes more widely understood by the affected individuals. Here, risks could come from obtaining inaccurate profile information or from becoming privy to privileged information based on age, gender, sexual orientation, or any other protected status, which may be in conflict with state and federal laws.[49] Acting upon information gleaned from cached websites, outdated links, and incomplete vignettes of online activities may bring in legal liabilities from violating anti-discrimination laws,[50] violating third party consent requirements,[51] and not complying with requirements under the Fair Credit Reporting Act ("FCRA"),[52] among others.

A. Accurate Information Gathering and Challenges

Identifying an applicant's behavioral profile from a search of an individual's digital footprint is akin to creating a profile via mosaic theory.[53] Mosaic theory is a practice in which incomplete and partial information vignettes are aggregated through an intelligent matching process to create a composite profile of an individual.[54] Here, the process is conducive to an outcome wherein no single piece of information may provide a complete signal about the person. Employers insist on using a designated third party screening agency to do a background check, either for ease of processing, or to introduce efficiency in completing the process, or simply due

---

[48] Robert Sprague, *Invasion of the Social Networks: Blurring the Line Between Personal Life and the Employment Relationship*, 50 U. LOUISVILLE L. REV. 1, 4 (2011); *see also, e.g.*, Lora Bentley, *Screening Job Applicants with Social Networks? Establish Procedures First*, IT BUS. EDGE (July 10, 2009), http://www.itbusinessedge.com/cm/blogs/bentley/screening-job-applicants-with-social-networks-establish-procedures-first/?cs=34014 (stating that a city in Montana asks job applicants to disclose usernames and passwords for their social networking sites to see if applicants were of "solid enough moral character"). *But see Thirty-Seven Percent of Companies Use Social Networks to Research Potential Job Candidates, According to New CareerBuilder Survey*, CAREERBUILDER.COM (Apr. 18, 2012), http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr691&sd=4%2F18%2F2012&ed=4%2F18%2F2099.

[49] Scott Brutocao, *Issue Spotting: The Multitude of Ways Social Media Impacts Employment Law and Litigation*, THE ADVOC.: LITIG. SEC. ST. B. TEX., Fall 2012, at 8, 8.

[50] *See supra* note 42 and accompanying text.

[51] Linda D. Schwartz, *Social Media—Friend or Foe?*, MD. B.J., Mar.–Apr. 2011, at 15–16 (providing examples of improper use of third parties to glean information from social media).

[52] *See* Douglas B. M. Ehlke, *The Fair Credit Reporting Act (FCRA) and the Investigation of Employee Misconduct*, FINDLAW (Mar. 26, 2008), http://library.findlaw.com/2004/Feb/1/231211.html; 15 U.S.C. § 1681b(b)(3)(A)–(B) (2012).

[53] *See* Michael P. Goodwin, *A National Security Puzzle: Mosaic Theory and the First Amendment Right of Access in the Federal Courts*, 32 HASTINGS COMM. & ENT. L.J. 179, 180–81 (2010).

[54] *Id*. at 185.

to a lack of relevant expertise.[55] When the screening is performed based on an analysis and evaluation of social media profiles, the utilized methodology is fundamentally different than a traditional background check consisting of credit reports and criminal profiles.[56] The reliability and accuracy of the process is suspect for various reasons: Cyberspace and social networking sites may contain a wide range of information, digital exchanges, personal musings, and retorts that a potential screener may take out of context or misunderstand.[57]

Generally, a third party background screening service assists a potential employer in navigating the divergent and disparate streams of online information by developing a composite profile based on social media and networking sites.[58] In aggregating background information available in profiles on social networking sites like Facebook, MySpace, LinkedIn, personal websites, and other online information sources, the third party aggregator matches scattered and incomplete information to a specific applicant.[59] Online searches are replete with potential errors for mismatched information.[60] For example, some search engines may provide archived versions of websites, revealing inaccurate, incomplete, or false information for which the updated version has not been reviewed by a third party background information provider. Similarly, some search engines may provide mirror websites with archived and outdated personal information that suffers from lack of temporal synchronization.[61] An employer making employment decisions based on such information could erroneously draw inferences on the suitability of an applicant, which may expose the employer to liability for discriminatory employment practices.

Often times, background information obtained from social media sites consists of incomplete thoughts, innuendos, and imprecise snapshots of an individual's personal profile. Thus, information gathered from a social media profile may be neither

---

[55] *See, e.g.*, EMP. SCREENING SERVICES, INC., http://www.employscreen.com/ (last visited May 21, 2013) (providing a third-party screening service to assist employers with the burdens of the hiring process).

[56] Sherry D. Sanders, *Privacy is Dead: The Birth of Social Media Background Checks,* 39 S.U. L. REV. 243, 255 (2012) (stating that information from a "social media background check cannot be verified as easily as information from a basic background check").

[57] *See* Jones et al., *supra* note 14, at 3, 5.

[58] *See, e.g.*, Jennifer Preston, *Social Media History Becomes a New Job Hurdle*, N.Y. TIMES, July 21, 2011, at B1 (explaining that Social Intelligence, a third party reporting agency, assembles a "dossier with examples of professional honors and charitable work, along with negative information that meets specific criteria" including racist remarks, sexually explicit photos, or displays of weapons or bombs).

[59] *See id.*

[60] *See* Bentley, *supra* note 48.

[61] *See Blumenthal, Franken Call on Social Intelligence Corp to Clarify Privacy Practices*, RICHARD BLUMENTHAL, U.S. SENATOR FOR CONN. (Sept. 19, 2011), http://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-franken-call-on-social-intelligence-corp-to-clarify-privacy-practice. Senators Richard Blumenthal and Al Franken wrote to Social Intelligence, a company that provides third-party social media search to employers, pressing the firm on concerns that its business practices violate individuals' online privacy and may be unfairly detrimental to their employment prospects *Id.* The Senators highlighted the fact that an online search has the potential to turn up cached pages that house information that has since been updated and questioned the company as to whether it is able to identify and verify information coming from such a page before giving that information to an employer. *Id.*

correct nor deterministic. This is because that type of derived information is not based on legal proceedings, like the outcome of a criminal trial, nor from universally accepted indices, like a credit score provided by an established agency. Social media captures an individual's behavioral snapshots in a more informal setting. Such information may be difficult to verify, challenge, and review.[62] As social media adoption enables employers to change the rules of engagement, the law has been slow to protect an applicant from discrimination and the denial of rights arising from employer decisions based on dubious data.[63]

When a third party accumulates social media based information related to an individual's profile, most times, the process does not have a deterministic verification mechanism like credit reporting. In the existing framework, an affected applicant cannot challenge the results of the third party verification process in the way she can challenge the inaccurate information generated by the credit agencies.[64] Similarly, when an individual enters the criminal justice system, such individual is accorded a robust due process that allows for multiple steps of appellate review before a final determination. Therefore, information available in criminal registries is mostly accurate and deterministic and as such, has a lower chance of providing faulty inferences on an individual than does a social media profile.

With the above in the backdrop, let us take the case of an individual engaged in informal and casual conversations with friends in his living room. If the transcript of such conversation became available to a potential employer, it could reveal inner thoughts of the candidate within a non-formal setting where an individual has the right to be left alone. This right to be left alone allows such individuals to engage in fantasy and privacy of secluded musings—often revealed in half-baked ideas, embarrassing snippets, or derogatory comments generated within the privacy of an individual's environment.[65] Today's digital immersion captures such informal moments on Facebook or MySpace. A third party background screener should not have unqualified access to such material for the purpose of employment decision making, as the issues related to privacy, search and seizure, and consent requirements are neither clear nor consistent for all applicable scenarios, especially when applied to decision making that calls for an assessment of how an individual would behave in a formal setting.

---

[62] *See* Lawrence Lessig, *Innovating Copyright*, 20 CARDOZO ARTS & ENT. L.J. 611, 615 (2002) (expounding on how easily a webpage may be changed, effectively rewriting history).

[63] Ken Strutin, *Social Media and the Vanishing Points of Ethical and Constitutional Boundaries*, 31 PACE L. REV. 228, 242 (2011) (discussing the general lack of laws directly dealing with social media and its implications under the First, Fourth and Fifth Amendment); *see also* Sprague, *supra* note 9, at 416 (explaining that current privacy laws will not protect Internet information, but statutes pertaining to "lawful conduct" may help protect that information).

[64] *See* Fair Credit Reporting Act, 15 U.S.C. §§ 1681i(a)(5)(A), (a)(6), (d) (2012) (laying out the elements for a prima facie case against a credit reporting agency, including proof of an inaccurate or incomplete report).

[65] *See* Alex Kozinski, *The Dead Past*, 64 STAN. L. REV. ONLINE 117, 123 (2012), *available at* http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-117.pdf.

B. Difference Between Traditional Credit Reporting and Social Media Screening

Many emerging legal issues come from law's inability to catch up with technology's advancement.[66] When the law is still lagging behind emerging behavioral patterns, it opens up new questions that must be answered. The answers to these emerging questions can be structured by considering existing analogous scenarios. By evaluating which one of the scenarios closely resembles the evolving fact pattern, a future pathway can be determined.[67] In this context, the road toward emerging law would require balancing two competing interests—the employer's interest in efficiently obtaining all relevant information about a prospective employee and the applicant's right to equity and fairness. Ultimately, this right to equity and fairness is enshrined within the fundamental privacy right of such an applicant, as has been manifested in government regulation of employer-employee relationships.[68]

The escalation in employers' use of social media has prompted regulatory agencies to become increasingly interested in supervising and modulating employer behavior. Driven by a heightened desire to prevent occurrences of undue discharge of employees based on their social network activities, the National Labor Relations Board ("NLRB") has become submerged in litigation.[69] Similarly, the Federal Trade Commission ("FTC") recently noted that third party screeners of an applicant's social media information must be recognized as "consumer reporting agenc[ies] under the FCRA."[70] These and other developments have opened up new areas of concern for the employers for the following reasons.

The methodology of aggregating social media based information to develop and make inferences on a profile is neither mature nor deterministic at this time.[71] Despite decades of development, criminal records and credit bureau reporting often suffer from inaccuracy.[72] In social media, information does not come in a continuous frame. Therefore, a background profile is created by aggregating a series of incomplete and scattered snapshots of an individual and injecting inaccuracy from

---

[66] Joshua S. Levy, *Towards a Brighter Fourth Amendment: Privacy and Technological Change*, 16 VA. J.L. & TECH. 499, 501–02 (2011) (stating that neither courts nor legislatures can adequately keep pace with technological change).

[67] *See* Raffi Varoujian, *Legal Issues Arising from the Use of Social Media in the Workplace*, HELIUM (July 28, 2011), http://www.helium.com/items/2204838-legal-issues-arising-from-use-of-social-media-at-work (discussing tensions which exist between the law and the capabilities of the Internet that have yet to be fully addressed by the law).

[68] Sprague, *supra* note 9, at 398–400 (discussing possible competing interests between an employer and an employee when it comes to employment pre-screening and further various restrictions imposed on an employer when pre-screening potential employees).

[69] *Rights We Protect*, NAT'L LAB. REL. BOARD, http://www.nlrb.gov/rights-we-protect (last visted May 21, 2013); *see also* Karl Knauz Motors, Inc. d/b/a Knauz BMW & Robert Becker, Case 13-CA-046452, 2012 NLRB LEXIS 679 (2012).

[70] Mithal Letter, *supra* note 47.

[71] *See* Jones et al., *supra* note 14.

[72] Ronald J. Allen & Larry Laudan, *Why Do We Convict as Many Innocent People as We Do? Deadly Dilemmas*, 41 TEX. TECH L. REV. 65, 71 (2008) ("It is hard to imagine conducting a criminal justice system that makes substantially fewer errors."); Chi Chi Wu, *Automated Injustice: How a Mechanized Dispute System Frustrates Consumers Seeking To Fix Errors In Their Credit Reports*, 14 N.C. BANKING INST. 139, 143 (2010) ("Despite the importance of accurate credit reports . . . errors are unfortunately quite common in the credit reporting system.").

slander, innuendo, and braggadocio. Reliance on such information to make employment decisions opens up the employer to time consuming and resource sensitive litigation.[73] This also brings up the issue of compliance with the Fourth Amendment.

C. Risk from Federal Anti-Discrimination Laws

While cyber-vetting is not fundamentally illegal, it may introduce heightened risks for an employer for possible violation of federal laws. Under Federal Employment law related to discrimination, certain characteristics are accorded protected status under federal law. For example, an employer could never ask a potential applicant in an interview about the candidate's age, marital status, race, national origin, medical issues,[74] and sexual orientation.[75] Traditional background reporting consisting of credit and criminal checks does not specifically target information concerning the protected status of the applicant.[76] Yet, in social media based surveillance and searches, an employer and its third party background provider may easily discover a potential candidate's protected status by specific identification of the candidate's age, marital status, race, etc.[77] If an applicant, upon being rejected, decides to file a discrimination claim, the employer is likely to lose if, by virtue of accessing such information in cyberspace, the employer has already become privy to the applicant's protected status.[78] In the event of an adverse employment decision, the employer's obligation to adequately respond becomes even more heightened. The employer then becomes obligated to develop a candidate profile where specific mention of such protected status has to be identified, documented, and shared with the applicant in order for the applicant to respond adequately.[79]

---

[73] *See* Sprague, *supra* note 9, at 399–400. Employers may unknowingly expose themselves to violations of various federal anti-discrimination laws. *Id.* at 416. Federal law prohibits discrimination based on race, color, religion, gender, national origin, age, disability, pregnancy, or genetic information. *See* 42 U.S.C. § 2000e-2(a) (2012) (prohibiting employment discrimination based on "race, color, religion, sex, or national origin"); 29 U.S.C. § 623(a) (prohibiting age discrimination); 42 U.S.C. § 12112(a) (prohibiting employment discrimination based on disability); 42 U.S.C. § 2000e(k) (prohibiting employment discrimination based on "pregnancy, childbirth, or related medical conditions"); Exec. Order No. 13,145, 65 Fed. Reg. 6877 (Feb. 10, 2000) (prohibiting the Federal Government from discriminating against potential employees based on genetic information).

[74] *See supra* note 73.

[75] *Sexual Orientation Discrimination—It's Illegal, At Least in D.C.*, WASH. D.C. EMP. L. LETTER (Krukowski & Costello S.C., Milwaukee, Wis.), Dec. 2001 (stating that District of Columbia Human Rights Act ("DCHRA") goes further than Title VII in that it explicitly prohibits discrimination based on sexual orientation, not just discrimination based on sex).

[76] *Performing Background Checks*, N.D. EMP. L. LETTER (Vogel, Kelly, Knutson, Weir, Bye & Hunke, Ltd., Nashville, Tenn.), Nov. 1998.

[77] Maria E. Recalde, *Be Cautious When Using Social Media in Hiring*, N.H. BUS. REV. (Aug. 12, 2011), http://www.nhbr.com/August-12-2011/Be-cautious-when-using-social-media-in-hiring/.

[78] *Id.*

[79] 15 U.S.C. § 1681m (2012); FED. TRADE COMM'N, 40 YEARS OF EXPERIENCE WITH THE FAIR CREDIT REPORTING ACT: AN FTC STAFF REPORT WITH SUMMARY OF INTERPRETATIONS 82 (2011),

II. FOURTH AMENDMENT PROTECTION AGAINST UNREASONABLE SURVEILLANCE

As noted above, technological enhancement in surveillance intrudes upon the privacy of individuals who use social media as their primary means of communication, and this effect is further magnified when one of these individuals becomes the subject of pre-employment screening. Although the erosion of such individual privacy undoubtedly conflicts with the liberty interests of an individual,[80] within the context of current employee-employer relationships, the applicant has only limited protection.[81]

Therefore, the role of the employer must be re-examined against the framework of the individual's subjective expectation of such privacy. The Supreme Court has already noted the need for a change in employers' perception of the emerging norm of digital immersion in society:

> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . .
>
> . . . Cell phone and text message communication are so pervasive that some persons may consider them to be essential means or necessary instruments

---

available at http://www.ftc.gov/os/2011/07/110720fcrareport.pdf (stating employers who use consumer reports to make employment decisions must make the adverse action disclosure by notifying applicants before and after taking an adverse action).

[80] *See* Saby Ghoshray, *Privacy Distortion Rationale for Reinterpreting the Third-Party Doctrine of the Fourth Amendment*, 13 FLA. COASTAL L. REV. 33, 34 (2011). I had argued elsewhere that, premised on an exigency of situation framework, privacy as a liberty interest has been muted under superior state interests. *Id.* at 44. This has resulted in significant abrogation of individual privacy in furtherance of state's law enforcement related objectives. *Id.* at 78. A rapidly shrinking privacy paradigm is inconsistent with Warren and Brandeis' privacy concept discussed earlier, which calls for recognizing the sacrosanct realms "of private and domestic life." *See* Warren & Brandeis, *supra* note 29, at 195. This broader connotation of the right to be left alone must be understood against an increasing threat to privacy in contemporary society, as privacy must be recognized for an individual's inherent right of privacy within the confines that an individual creates. Extrapolating this right to privacy would imply that these sacrosanct fundamentals would equally extend to the interior of the home-like community of connected individuals—be it within the Twitter community, the Facebook community, the MySpace community, or any other online community. Just because technology has allowed the quantity and frequency of information to skyrocket does not necessarily preclude individuals from exercising their right to be left alone. *See* Chip Walter, *A Little Privacy, Please*, SCI. AM. (June 17, 2007), http://www.scientificamerican.com/article.cfm?id=a-little-privacy-please.

[81] Legislative action in this emerging field has so far been limited to prohibiting employers from requesting applicants' social media passwords in an effort to circumvent privacy protections. *Employer Access to Social Media Usernames and Passwords*, *supra* note 38 (reporting that out of fourteen states that considered legislation that would restrict employers from requesting access to social networking usernames and passwords of applicants, students, or employees, only Maryland, Illinois, California, Delaware, Michigan, and New Jersey passed such a law). Additionally, as noted above, there are indications that certain actions of third-party screeners may be regulated under the FCRA. *See* Mithal Letter, *supra* note 47.

> for self-expression, even self-identification. That might strengthen the case for an expectation of privacy.[82]

This cautionary observation by the Supreme Court sheds light on the Court's view of individuals' subjective expectation of privacy. While it remains unclear what direction the Court eventually would take within the context of an applicant-employer relationship, this passage illustrates, nonetheless, that the Court is focused on two underlying principles. In the first, the Court formulates the contours of individuals' expectations of privacy indexed in the broader society's expectation in what the Court sees as society's expectation of an acceptable behavior framework.[83] In the second, the Court modulates individuals' privacy expectations based on finding a necessary ingredient of individuals' self-expression.[84] What the Court is hinting at here is the fundamental need for individuals to express themselves, an area that I have explored in detail elsewhere.[85] Certainly, the Court's observation here would sway the balance more in favor of an individual right, as opposed to employers' legitimate business concerns. Against the paucity of applicable legislative enactments, and in an environment where an employer has superior capability to track every digital footprint of an individual, it is important to chart the applicable territory of what might constitute reasonable surveillance and what protectionist paradigms may be available to an applicant.[86] Ultimately, any such paradigm must be framed based on applicable legal guidance obtained from the Constitution's Fourth Amendment.[87] It is important, therefore, to review the *Katz* doctrine.[88]

---

[82] City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2629–30 (2010).

[83] *Id.* at 2629–30.

[84] *Id.* at 2630.

[85] *See* Ghoshray, *supra* note 80, at 52, 71.

[86] *Quon*, 130 S. Ct. at 2631 (2010). The Court's observation in *Quon* is in the context of a public employee's Fourth Amendment right against his government employer's "unreasonable searches and Seizures." *Id.* at 2624. Applying this standard might provide an individual, who is yet to become an employee, a much higher protection against employer surveillance, as the *Quon* Court recognizes the employee as an individual who has a right to self-expression in social media. *Id.* at 2630. This is because the *Quon* Court's observation is applied in the context of a public employee-employer relationship, which is a rather restrictive scenario. Other Fourth Amendment cases have noted that employees' privacy protection in the workplace varies as a function of the nature of the bilateral employee-employer relationship that defines the contour of the "operational realities of the workplace." *See* O'Connor v. Ortega, 480 U.S. 709, 717–18 (1987) (linking employees' right to privacy with the operational realities of the workplace—a reality that derives its existence from the nature of employee-employer relationships). Thus, the Supreme Court jurisprudence on employee protection from privacy intrusion is neither settled nor fixed. Focusing on the interest of an applicant, there remains uncertainty with respect to the strength of an employer-employee relationship, based on whether an employer's right to search an applicant profile may be limited. On the contrary, the Court has given employers a much higher threshold with which to conduct searches of employees' communication if such searches are conducted with the objective of protecting an employer's legitimate business interests, such as investigating employee misconduct at work or probing employee misdeeds. *Quon*, 130 S. Ct. at 2632. If a potential employer can connect the online search of an applicant's digital footprints with legitimate business interests and if such a search can be conducted via the applicant's consent, the employer may have a better chance of prevailing. *See O'Connor*, 480 U.S. at 725.

[87] *See O'Connor,* 480 U.S. at 714–22.

A. Applying the Katz *Doctrine in Employer Surveillance of Employees*

Society has little or no knowledge of the particular surveillance techniques an employer has at its disposal. An individual applicant is at a disadvantage when trying to adequately develop a viewpoint on which a digital footprint may be under scrutiny and what information is within the scope of potential employer surveillance.[89] Implicit in the Supreme Court's *Katz v. United States*[90] decision is a roadmap to determine how far individuals' privacy should dictate the limits of a supervisory power—whether coming from the government or from an employer acting in a supervisory capacity.[91] In his concurrence in *Katz*, Justice Harlan set out a new standard which, except for law enforcement intrusion cases, has become the reference point for balancing individual privacy with supervisory legitimate interests as per the Fourth Amendment.[92] Justice Harlan articulated a two-prong test for Fourth Amendment protection against unreasonable searches that can be extended to employer-sponsored surveillance.[93]

Reviewing the *Katz* doctrine to evaluate the emerging surveillance trend within the employment context, we should recognize at the outset, that an applicant must have exhibited an actual or subjective expectation of privacy.[94] Then, this actual expectation must be evaluated as something that society is prepared to recognize as reasonable.[95] In articulating this two-prong test, Justice Harlan had followed the

---

[88] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). While referring to Justice Harlan's famous test in *Katz*, Professor Peter Winn observed that:

> [In] Justice Harlan's concurrence on its merits, we have seen that in working on the reasonable expectation of privacy test, he refined the test in his own way, adding both a subjective and an objective component. Perhaps he thought that the subjective component was needed to clarify that, although an objective expectation of privacy might exist, a subjective expectation might not, as when a person in his (objectively private) home is overheard intentionally speaking in a loud voice out of on open window. . . . Perhaps Justice Harlan felt the subjective component of the test was still needed to mirror the old trespass element that an intrusion lack permission. However, when applying the test in subsequent cases, even Harlan himself only referenced the objective component.

Peter Winn, *Katz and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 11 (2009).

[89] *See* Sam Kamin, *The Private is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C. L. REV. 83, 121, 145 (2004).

[90] *Katz*, 389 U.S. at 347. Taking a renewed look at the fundamentals of the privacy interests under the Katz holding, a subjective expectation of privacy by the individual must be evaluated at the next level of abstraction that requires evaluating the scope qualitatively and quantitatively. An individual's subjective expectation of privacy must be evaluated and the means of evaluation is dependent on identifying society's reasonable expectation—an objective framework. Therefore, the crux of the issue relies on identifying society's recognizable, reasonable expectations.

[91] *See Katz*, 389 U.S. at 361; Kamin, *supra* note 89, at 145.

[92] *See* Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1363, 1372 (2004).

[93] *Katz*, 389 U.S. at 361.

[94] *Id.*

[95] *Id.*

Katz majority's robust interpretation of the Fourth Amendment by noting that "the Fourth Amendment protects people, not places."[96] Since the *Katz* decision more than a half-century back, the Fourth Amendment driven individual expectation of privacy has continued to be defined by Justice Harlan's "reasonable expectation of privacy" test to decide whether unreasonable search and surveillance violates individuals' Fourth Amendment rights.[97] The doctrinal implications of *Katz* as animated within the importance of the individual's subjective expectation of privacy is still a valid concept and thus, must be re-imagined within the evolving context of the social media framework of today.[98] This calls for taking a renewed look at the fundamental privacy interests under the Fourth Amendment.[99]

A *Katz* analysis can be conceptually difficult as it requires developing a relationship between an objective framework and a subjective framework.[100] Thus, identifying a set of deterministic benchmarks is necessary to provide judicial efficiency and consistency.[101]

In trying to identify the scope of an individual's actual expectation of privacy, it is important, therefore, to develop all ancillary fact patterns surrounding such individual's behavioral pattern.[102] If, in the conduct of his or her digitally mediated behavior, the individual exhibits a shared sense of space and shows extreme reluctance to utilize available privacy settings in the digital communication pathway,[103] this could lower the threshold of such individual's actual expectation of privacy.[104] Staying within the framework of such individual's subjective expectation,

---

[96] *See id.*

[97] *See* Albright v. Oliver, 510 U.S. 266, 287 (1994) (applying the Harlan Fourth Amendment analysis to police surveillance in a drug prosecution case); United States v. Jones, 132 S. Ct. 945, 947 (2012) (discussing the Harlan concurrence in the context of a GPS tracking device); Hudson v. Palmer, 468 U.S. 517, 525 (1984) (applying the Harlan reasonableness standard to a contraband search of a prison cell).

[98] *See Net Impact: US Becomes a Facebook Nation*, BUS. NEWS DAILY (Apr. 6, 2011, 4:20 PM), http://www.businessnewsdaily.com/840-facebook-smartphone-majority-americans-online-.html (discussing the continuing rise in Facebook membership amongst Americans); Julia Angwin, *How Much Should People Worry About the Loss of Online Privacy?*, WALL ST. J. (Nov. 14, 2011, 3:56 PM), http://online.wsj.com/article/SB10001424052970204190704577024262567105738.html (discussing the impact the Internet has on daily life and why protecting the privacy of that activity is important).

[99] *See* ARI SCHWARTZ ET AL., CTR. FOR DEMOCRACY & TECH., DIGITAL SEARCH & SEIZURE: UPDATING PRIVACY PROTECTIONS TO KEEP PACE WITH TECHNOLOGY 3 (2006), https://www.cdt.org/publications/digital-search-and-seizure.pdf.

[100] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[101] *See* David A. Sklansky, *Back to the Future: Kyllo, Katz, and Common Law*, 72 MISS. L.J. 143, 207–08 (2002).

[102] *See, e.g.*, *id.* at 159–60 (providing that protection against surveillance technologies also depends on where the suspect is and whether the suspect is in his or her home).

[103] *See* Matt Markovich, *Survey: Many Facebook Users Not Using Privacy Settings*, KOMONEWS.COM (May 3, 2012, 6:15 PM), http://www.komonews.com/news/consumer/Facebook--150105135.html; *Sharing Personal Information Online*, PERPETUITY RES. (Dec. 5, 2012), http://www.perpetuityresearch.com/blog/?p=115.

[104] *See* Romano v. Steelcase Inc., 907 N.Y.S. 2d 650, 656 (N.Y. Sup. Ct. 2010) (stating that a person has a lower expectation of privacy when that person has chosen to disclose information); Kellie A. O'Shea, *Use of Social Media in Employment: Should I Fire? Should I Hire?*, CORNELL HR REV. (Oct. 30, 2012), http://www.cornellhrreview.org/use-of-social-media-in-employment-should-i-

it is possible to identify various subjective thresholds, a set of triggers left along an individual's footprint, each of which can be captured via specific questions: How much sharing of private personal communication the individual conducts? At what frequency such individual shares sensitive personal information with wider society? Does the individual use available privacy settings in her digital environment? Evaluating the answers to such questions would entail the second phase of construction to evaluate the nature, scope, and quantitative element in that subjective expectation. What makes that subjective expectation of an applicant a reasonable expectation?

There may be specific exigent business rationales that can supersede an applicant's otherwise reasonable expectation of privacy on account of a probable cause or immediately available information regarding the applicant.[105] However, the evaluation or recognition of society's reasonable expectation of privacy has been the subject of debate in various parlances. Implicit in this evaluation is the concept of the third party doctrine, an area highlighted in detail elsewhere.[106] Society's

---

fire-should-i-hire/ (asserting that users who decide to grant public access to their social media profiles "should expect little if any expectation of privacy with that employer or company"). Immersed in digital media and online social networking sites, contemporary individuals are often times driven by an exigent need to update their social networking status while signaling to the external world almost every instance of their personal lives. *See* O'Shea, *supra*; Rick Hampson, *Twitter at 7: Smart or Stupid, We Are What We Tweet*, USA TODAY (Mar. 20, 2013, 5:14 PM), http://www.usatoday.com/story/news/nation/2013/03/19/age-old-bad-judgment-lives-long-in-digital-age/2001557/ (stating that there are more than 400 million tweets a day). Because the majority of these individuals are connected to multiple other individuals via social media, a one-to-one connection can become a many-to-many connection relatively easily. *See* Kevin Lewis et al., *The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network*, 14 J. COMPUTER-MEDIATED COMM. 79 (2008), *available at* http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2008.01432.x/pdf. As a result, despite various privacy settings offered in social media, intimate personal details may no longer stay private and secluded within an individual's personal space. *See id.* Individuals may be eroding their own expectations of privacy, without even recognizing the long term consequences of their behavior. Thus, within a discussion of individual privacy erosion, we must not allow the personal responsibility of an individual to be left out of the discussion. Especially if we recognize, regardless of an ever enchanting array of digital gadgets corporations place before an individual, they also offer various privacy mechanisms that individuals can employ. Despite the ease of digital communication, individuals should adequately protect the gateway to their communications, in order to establish their right to privacy in cyberspace.

[105] *See, e.g.*, Cort v. Bristol-Myers Co., 431 N.E.2d 908, 913 (Mass. 1982) (stating that, with regard to public policy, the intrusion of the privacy rights of an employee is measured against the nature of the employee's job in regards to the reasonableness of the intrusion); French v. United Parcel Serv., Inc., 2 F. Supp. 2d 128, 131 (D. Mass. 1998) (holding that there are "circumstances in which it is legitimate for an employer to know some 'personal' information about its employees" as long as the information relates to the effectiveness of the employee's job performance and employment).

[106] *See* Ghoshray, *supra* note 80, at 36–37. The third party doctrine brings additional complexity in the pre-employment screening framework, and as such, this should remain outside the scope of the current discussion. For additional reference, see Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1311–12 (1981); Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1248–50, 1252–53 (1983); Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 19 (2008); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 213–14 (2006); Stephen E.

reasonable expectation of privacy can be attenuated based on digital communication that an individual has already engaged in by sharing personal protected information with any third party service provider. This area has doctrinal implications that might bring in additional complexities to the employee and employer relationship that shall remain outside the scope of the current discussion. Stepping away from the dichotomy between human interaction and automated interaction, the bone of contention in the doctrinal difficulty in third party doctrine, the focus can be turned to other factors that impact the relationship between an applicant's subjective expectation of privacy and society's reasonable expectation of such privacy.

Therefore, while charting the normative scope of social media screening, it is important to identify the outliers—a set of individuals whose subjective expectation of privacy may not match society's reasonable expectation of privacy. The law surrounding use and abuse of social networking must adequately address these issues; otherwise, the equality doctrine might be in jeopardy.[107]

This includes individuals who may not be active in social media. The privacy rights of such individuals must be evaluated at a more elevated threshold than the other two types of individuals discussed previously. The law must ensure that a lone ranger is immune to the deleterious impact of society—such an individual conception of a subjective expectation of privacy must not be comingled with the masses, and the employee-employer legal framework must structure reasonable protection for such individuals.[108] Because, if one is not immersed in technology even by the virtue of living in the society, this individual must not be subjected to the broader society norms.[109]

It is important, therefore, to understand how individuals' personal behavior may be shaping their expectations, an area that has not received much attention in literature or contemporary discourse. The following section will highlight this area in further detail in order to develop a more realistic linkage between an individual's

---

Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 976–77 (2007).

[107] Samuel R. Bagenstos, *Employment Law and Social Equality*, 112 MICH. L. REV. (forthcoming Spring 2013) (manuscript at 28–30), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208883.

[108] *See* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 22 (stating that in almost all analyses of an individual's reasonable expectation of privacy in their electronic communications, the analysis will be evaluated under the objective prong of what society deems to be reasonable, rather than under the subjective prong).

[109] *See* Strutin, *supra* note 63, at 252 n.69 (2011) (explaining that, simply because a certain kind of technology is used in a community as a whole, it does not mean that a particular defendant has notice of that fact). The idea of evaluating an individual's subjective expectation of privacy based on society's reasonable expectation has an inherent drawback. For example, if the majority of people within the society are sufficiently acclimatized into digital communication via social media, the majority's privacy expectation may not comport with the minority population that are consciously decoupled from pervasive digital immersion. Thus, society's reasonable expectation cannot be a proxy to these individuals' privacy expectations. The law must be structured in such a way that all individuals' privacy concerns are adequately addressed by its imposition. *See, e.g.*, Junichi P. Semitsu, *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, 31 PACE L. REV. 291, 371 (2011) (stating that an individual's expectation of privacy should be based on the individual's expectation of privacy from government surveillance, rather than on the user's individual expectations).

subjective expectation and society's reasonable expectation of privacy within the context of an applicant-employer relationship.

B. Playing the Part Versus Fourth Amendment

The practice of cyber-vetting candidates for employment presents two key problems for employers. The first comes from relying on information generated from social media, and the second comes from intrusion into the privacy of an individual. Social media has given post-modern individuals a newfound sense of empowerment. In a world where anyone with an iPad, iPhone, or laptop and an Internet connection can become a celebrity, or pretend to be one, an individual may erroneously create an online digital profile that does not truly reflect that individual's employment eligibility or credentials. By taking on different roles, the individual is engaged in a performance for his or her pre-selected community. Knowing full well that he or she is being seen, watched, and followed, the individual engages in a display of emotions and behaviors that she would not likely reveal in a formal setting.[110] This act is part of an ongoing theme—playing for the audience. Oftentimes, the audiences are self-selected community members with whom the individual has voluntarily associated.[111] These behavioral norms must be left as distinct from expected behavior in an employment setting.

Employers' use of third parties to scoop those bits of information and create a profile of the candidate is not a prudent way of judging an individual's candidacy. This aggregation process is imprecise and fraught with inaccuracy and unreliability.[112] Without training in behavioral science or social psychology, a third party aggregator of social media information is certainly not capable of creating an individual profile that accurately reflects how an individual would behave in a formal setting within an employer-employee relationship. Because social media exchanges are not reliable predictors of an individual's employment potential, hiring decisions should never be made on the basis of such information.

Besides generating erroneous conclusions, gathering social media information opens up to a broader Fourth Amendment issue. The fundamental difference between obtaining information from traditional sources, such as judicial decisions and credit reports, and obtaining information by way of social media exchanges is that the former is available in the public domain, whereas the latter is part of a

---

[110] *See* De Armond, *supra* note 10, at 1131 (likening the information taken from social media to that of personality tests and stating that this information reveals too much of an individual's private being and is an inaccurate analysis of information that an employer may need).

[111] *See, e.g.*, Brent Johnson, *More People are Turning to Internet Dating*, EZINEMARK.COM (Dec. 11, 2011), http://technology.ezinemark.com/more-people-are-turning-to-internet-dating-7d3272155e72.html (discussing how people are turning more and more to the Internet, often to conduct their most intimate and personal activities, such as finding a romantic partner).

[112] *See* State v. Bell, 882 N.E.2d 502, 512 (Ohio Ct. Com. Pl. 2008) (acknowledging that information gathered from a social media account could potentially be "incomplete, easily altered, or possibly from an unidentified third party using [one's] account").

protected private space.[113] The individual in question is a member of the common public as an applicant for a particular job who has not yet joined the employer's organization. This individual should be treated as an individual who has equal rights in every aspect. Here we are evaluating the balance between predicting an employee's future success and retaining that individual's privacy rights. However, these two scenarios are not analogous. In the case of employee monitoring, by virtue of becoming part of an organization, the employee has subjected to the employer's business interests, whereby such employee's right to privacy may have been attenuated. While a narrower threshold of privacy may apply with respect to the employer's ability to engage in surveillance of its employee,[114] a much higher threshold of privacy must insulate an applicant from employer surveillance. This applicant-employee distinction resides at the center of determining the scope of employer surveillance and the boundary of individual privacy rights. In the absence of applicable legislative enactment or specific case law to guide us, our understanding of this evolving applicant-employer relationship has to be animated by the fundamental assertion of Fourth Amendment rights enshrined in the *Katz* two-prong test.

In both pre-employment and post-employment scenarios, we are testing the equilibrium between an employer's right to legitimate business interest and an individual's right to privacy. When the relationship changes from employee-employer to applicant-employer, employers' surveillance ability must attenuate to enhance the applicant's privacy right. Because the applicant has not become part of the employee pool, she must retain her right to live freely within her selected environment—she must retain her right to be left alone.

III. EMERGING LEGAL ISSUES IN ONLINE SEARCHES

A. Privacy and Anti-Discrimination in Cyber-vetting

Because hiring individuals for employment is a paradigmatic example of investment under uncertainty,[115] developing an individual profile based on identifying signals from available, observable characteristics attached to an individual is an example of information transfer within the framework of information asymmetry in the market.[116] Scholars have noted that the employment market exhibits all of the characteristics of a market where signaling takes place in various

---

[113] *Compare* 15 U.S.C. § 1681(k) (2012) (stating that consumer reports given for employment purposes compile items of information on consumers that are matters of public record), *with* O'Shea, *supra* note 104 (stating that regardless of privacy disclosures on users' social media account settings, users still maintain an expectation of privacy in certain circumstances).

[114] *See* Michael E. Lackey Jr. & Joseph P. Minta, *Lawyers and Social Media: The Legal Ethics of Tweeting, Facebooking and Blogging*, 28 TOURO L. REV. 149, 180 (2012).

[115] Michael Spence, *Job Market Signaling*, 87 Q. J. OF ECON. 355, 356–58 (1973).

[116] *Id.* at 356–58.

forms.[117] In the pre-cyber-vetting era, such signaling took place based on an aggregation of deterministic characteristics such as educational background, employment experience, race, gender, and sex. Though these characteristics continue to be subject to manipulation and can shape decisions based on subjective assessment, cyber-vetting brings forth a more pronounced specter of discrimination potential. By transforming random subjective assessment into a more pronounced deliberate omission of individuals, this raises the issue of whether privacy and anti-discrimination are conceptually at odds with each other.[118]

Signaling in the employment marketplace is the process of distilling patterns from a spectrum of observed personal characteristics to develop a model of predictive analysis.[119] As pre-cyber-vetting hiring evaluations predominantly dealt with deterministic data, the divergence between subjective assessment and objective determination was kept within a more allowable and reasonable bound.[120] With the proliferation of social media exuberance among individuals and the enhancement in the ability of big data, a potential employer can sort and analyze a vast amount of data and mine for patterns within the conglomeration of incomplete and imprecise information to predict personalities from social networking sites.[121] As this propensity for data mining for predictive analyses becomes rampant, the distributive implication of privacy is thrust into increasing tension with the objective of anti-discrimination.[122] A significant absence of robust laws to ensure privacy protection from undue intrusion into the private affairs makes this framework more adverse for

---

[117] *See, e.g.*, Edward J. McCaffery, *Slouching Towards Equality: Gender Discrimination, Market Efficiency, and Social Change*, 103 YALE L.J. 595, 631–32 (1993); Tamara Russell, *Digging the Dirt: Digital Tips for Employers and Job Seekers*, OR. ST. B. BULL., Aug.–Sept. 2010, at 48; Robert Sprague, *Googling Job Applicants: Incorporating Personal Information into Hiring Decisions*, 23 LAB. L. 19, 20 (2007); Alan Finder, *When a Risqué Online Persona Undermines a Chance for a Job*, N.Y. TIMES (Jun. 11, 2006), http://query.nytimes.com/gst/fullpage.html?res=F30712F739550C728DDDAF0894DE404482.

[118] Michelle Sherman, *Social Medial Research + Employment Decisions: May be a Recipe for Litigation*, CYBERSPACE LAW, Apr. 2011, at 1, 1–3.

[119] *See* Spence, *supra* note 115, at 356.

[120] *Compare* Willner v. Thornburgh, 928 F.2d 1185, 1194 (D.C. Cir. 1991) (finding pre-employment drug screening for District Attorney employment to be a reasonable search under the Fourth Amendment), *and* Anderson v. Philadelphia, 845 F.2d 1216, 1225 (3d Cir. 1988) (upholding, as reasonable, the use of polygraph testing for pre-employment screening of potential police officers), *and* Stephen F. Befort, *Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place*, 14 HOFSTRA LAB. L.J. 365, 368–69 (1997) (explaining how employers use "screening-in" to vet for qualities they seek in an employee and "screening-out" using recorded past events as an indication of how the employee with perform in employment duties), *with* Elefant, *Do Employers Using Facebook for Background Checks Face Legal Risks?*, LAW.COM LEGAL BLOG WATCH (Mar. 1, 2008), http://legalblogwatch.typepad.com/legal_blog_watch/2008/03/do-employers-us.html (explaining employers' use of social media to perform subjective and speculative personality background checks).

[121] Stephanie Mlot, *Raytheon Riot Software Predicts Behavior Based on Social Media*, PCMag, (Feb. 12, 2013, 2:46 PM), http://www.pcmag.com/article2/0,2817,2415340,00.asp (describing claims by a security company to predict potential and current employee behavior by tracking all possible online activity).

[122] *See* De Armond, *supra* note 10, at 1133–34 (likening determinations based on social media to those of a personality test and arguing that such determinations are likely to contain inaccuracies).

individuals within the cyber-vetting context.[123] While social networking has created ease of communication and provided access to multiple and simultaneous exchanges, it has also coaxed individuals in leaving vast amounts of digital data in cyberspace,[124] for employers to search and distill patterns for predictive employment based analyses.

Although law's objective is to ensure equity—equity manifested in similar scenarios having equal outcomes[125]—employers continue to focus on a flawed conceptual apparatus for signaling and information transfer. These subjective evaluations are tainted by the preponderance of incomplete, imprecise, and unverifiable information that percolates through the random musing of social networking sites.[126] Because law has not caught up with technology's evolution,[127] some behavioral norms, such as employers' penchant to engage in random and rampant searches, have remained outside the purview of legal sanctions.[128] This intrusion into individual privacy has opened the door for expansive discrimination. For example, a particular employer can search in various social media sites to distill a pattern for a particular individual and thereby make judgments on the individual's suitability for a particular employment role—all without obtaining the individual's consent to such a search. In the absence of adequate individual privacy protection law, denial of employment based on matching an individual's privately obtained profile with a desired profile raises the specter of discrimination. Although federal

---

[123] Raffi Varoujian, *Legal Issues Arising from the Use of Social Media in the Workplace*, HELIUM (July 28, 2011), http://www.helium.com/items/2204838-legal-issues-arising-from-the-use-of-social-media-in-the-workplace (discussing current tensions which exist between the law and the capabilities of the Internet that have yet to be fully addressed by the law); *see also* Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 389 (1997) (explaining that even in the early days of technological privacy issues, courts needed to reassess privacy interests); Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep Up with Technological Change*, 2007 U. ILL. J.L. TECH. & POL'Y 239, 241 (2007) (noting that the law has fallen behind technology).

[124] Zack Whittaker, *How Much Data is Consumed Every Minute?*, ZDNET (June 22, 2012, 8:52 PM), http://www.zdnet.com/blog/btl/how-much-data-is-consumed-every-minute/80666. The amount of data running through the Internet is "baffling, and downright crazy." *Id.* For example, each day, "[e]mail users send more than 204 million messages; . . . Google receives over 2 million search queries; YouTube users upload 48 hours of new video; Facebook users share 684,000 bits of content; [and] Twitter users send more than 100,000 tweets." *Id.* Moreover, Technology-enabled communication has moved beyond the point-to-point communication of yesteryear to a combination of distributed transmission and third-party-enabled communication, where various third-party providers are not only storing data, but also processing it to make the system more efficient and enhance the experience of users. *See* Connie Davis Powell, *"You Already Have Zero Privacy. Get Over It!" Would Warren and Brandeis Argue for Privacy for Social Networking*?, 31 PACE L. REV. 146, 166 n.107, 167, 173 (2011) (describing details on various third-party mechanisms in communication, social media, and Internet).

[125] *See* Saby Ghoshray, *Hijacked by Statistics, Rescued by* Wal-Mart v. Dukes*: Probing Commonality and Due Process Concerns in Modern Class Action Litigation*, 44 LOY. U. CHI. L.J. 467, 471–72 (2012).

[126] *See supra* note 112 and accompanying text.

[127] *Supra* note 123 and accompanying text.

[128] *See* Bentley, *supra* note 48.

law prohibits discrimination based on race, sex, and gender,[129] no current law clearly proscribes discrimination based on derived and inferred personality traits.

B. Legal Liability for Statistical Discrimination Based on Observable Characteristics

This phenomenon of social media-aided employment screening implicates two important constitutional protections—the First Amendment freedom of expression and the Fourth Amendment right of privacy.[130] While the Fourth Amendment issue arising out of intrusive searches has found its voice in contemporary discourse, First Amendment issues related to employment screening have not been part of the contemporary discussion.[131]

The First Amendment protects citizens' speech. The existing constitutional cases discuss the employee's First Amendment right of speech protection in the workplace context while the employee is gainfully employed within an organization.[132] Yet, because social media thrusts pre-employment expressive conduct and speech into the hiring context, the question of whether First Amendment protection may apply in this context is a valid discussion point that has not been addressed.

As an individual becomes aware of a digital war against privacy, in a new economy perhaps, freedom of expression may become subject to suppression as individuals become aware of the broader reach of employment screening. Individuals may become reluctant to express their opinions for fear of the potential effect of those opinions on their employment prospects. Such a development runs counter to each individual's fundamental right to express her opinion and affect the democratic process. If a potential employee recognizes *a priori* that anything he or she expresses in a public forum could be found in a future search as part of digital data mining for distilling patterns for a "suitable" employee, the individual will be more inclined to suppress her thoughts than to express them.

This again brings us to an emerging tension between the right to employment and the right to expression.[133] The fundamental question is whether the right to

---

[129] *See supra* note 73 and accompanying text.

[130] *Compare* U.S. CONST. amend. I (providing protection for the freedom of speech), *and* U.S. CONST. amend. IV (providing protection from unreasonable search and seizure), *with* Alan Finder, *For Some, Online Persona Undermines a Résumé*, N.Y. TIMES (June 11, 2006), http://www.nytimes.com/2006/06/11/us/11recruit.html?_r=2&oref=slogin&# (explaining that even in the early years of Facebook and MySpace, employers were screening potential employees using their assumptively privacy-protected social media profiles).

[131] *Cf.* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (applying a Fourth Amendment analysis to a situation involving information transmitted from a telephone booth); New Jersey v. T.L.O., 469 U.S. 325, 337 (1985) (applying a Fourth Amendment analysis to a situation involving searching a student's purse for suspected cigarettes).

[132] *See* Garcetti v. Ceballos, 547 U.S. 410, 417 (2006) (explaining that the Supreme Court has been clear that employees do not surrender their First Amendment rights at the door of their places of employment).

[133] *See, e.g.*, Bd. of Regents of State Colls. v. Roth, 408 U.S. 564, 576–77 (1972) (discussing the property interest that tenured or contracted professors have in continued employment when a professor's contract was not renewed after he criticized the administration).

expression in the new digital economy is being subsumed under the right to employment. While the Fourth Amendment privacy right within the employment search context is a more pronounced and tangible issue, how the First Amendment right is being implicated within a broader privacy encroachment via digital searches of individual footprints is not as clear in the contemporary discourse. This observation, therefore, is intended to bring awareness that there is a danger to freedom of speech and freedom of thought currently arising out of cyber-vetting.[134]

C. Cyber-vetting and the Conflict with Social Contract Theory

Almost as old as modern civilization, social contract theory originated from Plato and Socrates.[135] Nurtured in the modern era by Hobbes,[136] Rousseau,[137] and Hume,[138] social contract theory posits that individuals in a society surrender some of their freedoms and submit to the authority of a supervisory entity in exchange for the protection of their remaining—fundamental—rights. Implicit in this paradigm is the core belief of individual consent.[139] Yet, the digital explosion and the ease of technology have created a dystopian nightmare.[140] The related supervisory entities, the government, the big corporations, and even the smaller employers have rejected social contract theory as a paradigm,[141] whereby the right to consent by an individual has been sublimated within the right of an employer. Yet, the individual has a concomitant right to a meaningful employment for which she should be allowed to expose her credentials, but not her private affairs. This emerging inconsistency must be evaluated for its full implications within the context of cyber-vetting with the objective of refining labor practices and employment law.

---

[134] *See* Stephen J. Kobrin, *With Technology Growing, Our Privacy is Shrinking*, PHILA. INQUIRER (Jan. 3, 2001), https://mgmt.wharton.upenn.edu/files/?whdmsaction=public:main.file&fileID=3992 (providing a discussion on the shrinking privacy space with the advent of technology in communication); James D. Phillips & Katharine E. Kohm, *Current and Emerging Transportation Technology: Final Nails in the Coffin of the Dying Right of Privacy?*, 18 RICH. J.L. & TECH. 1, 10 (2011) (arguing that advances in technology have led to Supreme Court decisions that have created confusion about Fourth Amendment privacy law).

[135] Celeste Friend, *Social Contract Theory*, INTERNET ENCYCLOPEDIA OF PHIL. (Oct. 15, 2004), http://www.iep.utm.edu/soc-cont/.

[136] *Id.*; *see generally* THOMAS HOBBES, LEVIATHAN (C. Crawford Brough Macpherson ed., Centraal Boekhuis 1985) (1651).

[137] Friend, *supra* note 135; *see generally* JEAN-JACQUES ROUSSEAU, THE BASIC POLITICAL WRITINGS (Donald A. Cress ed., 2d ed., Hackett Publ'g Co. 1987).

[138] *See* DAVID HUME, ESSAYS, MORAL, POLITICAL, AND LITERARY (Eugene F. Miller, ed., Liberty Fund, Inc. 1987) (1742), *available at* http://www.econlib.org/library/LFBooks/Hume/hmMPL35.html.

[139] *See* Friend, *supra* note 135.

[140] *See* Daniel J. Solove, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 27 (2004) (noting how the "Big Brother" figure of George Orwell's dystopian novel *1984* has become a central metaphor in discussions concerning privacy and technology).

[141] *See* Haefner, *supra* note 4 (describing instances in which employers will deny a candidate employment based on conduct revealed through social media); *see also* Sanders, *supra* note 56, at 258 (suggesting that employers obtain written consent before initiating a social media background check).

In yet another reversal for distributive implications of privacy, in the absence of deterministic behavioral history such as a criminal history registry or a credit score, employer-sponsored cyber-vetting engages in the search of a potential employee's digital footprint[142] by navigating imprecise information gleaned from social networking sites. Such search processes create illegitimate proxies for an individual profile based on snippets, musings, third party innuendos, and private exchanges of an individual to develop a predictive profile of the individual's employment candidacy. The law has yet to respond to this imprecise and flawed subjective assessment based on intrusive privacy violations and unbridled data mining in which employers continue to engage.

As cyber-vetting continues to place privacy and speech at loggerheads with the attenuation of privacy we can see the right to expression is beginning to eviscerate. For example, an individual, staying within the permissible bounds of social norms and legal framework, can engage in producing an explicit sex video tape with another consenting adult individual. While the objective is mediated by individual preference, the social contract theory posits that the product of such act is not for public consumption, and therefore, the public should not be privy to such viewing of the recorded tape. In the social media-enabled societal landscape, such an individual can restrict the distribution of a product among a set of people belonging to a restricted set of digital communities.[143] Yet, unscrupulous on-line searches by an employer,

---

[142] The asymmetry between the technological sophistication of an employer's surveillance and the targeted applicant's awareness of such technology can be compared with the asymmetry that exists between the technological sophistication of the United States' drone operation in Afghanistan and Yemen and the targets' awareness of such monitoring. *See Drones: What Are They and How Do They Work?* BBC NEWS, http://www.bbc.co.uk/news/world-south-asia-10713898 (last updated Jan 31, 2012) (describing drones' ability to gather intelligence and deliver precision strikes "without the need for more intrusive military action"). Like the suspected terrorists targeted by drones, most applicants have very little idea about the sophisticated tracking ability of potential employers' digital surveillance methodologies and mechanisms. *See* Rachel Zupek, *How Social Media Can Hurt Your Career*, CNN, http://www.cnn.com/2009/LIVING/worklife/08/24/cb.job.social.medial.pitfalls/ (last updated Aug. 24, 2009) (describing how software company monitored and responded to potential hire's negative tweets and explaining how employees often post negative tweets about their jobs without realizing that their employers have an increasingly high presence in social media). Currently, a variety of employer surveillance software use sophisticated mechanisms to follow employees' digital footprints. Brittany Petersen, *Employee Monitoring: It's Not Paranoia—You Really Are Being Watched!*, PCMAG.COM (May 26, 2008, 10:40 AM), http://www.pcmag.com/article2/0,2817,2308363,00.asp. It must be recognized that the search of an individual's personal space, regardless of whether it is a physical dwelling or a virtual community, is against traditional constitutional protection. This view follows the main doctrinal trajectory of Justice Harlan's two-part test. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The limits to the surveillance power of a supervisory entity can be reasonably identified by evaluating the scope of an individual's expectation of her own privacy. Therefore, the broader idea is that a threshold for search and seizure within the context of an individual's private space can be developed by keeping the basic constitutional premises of privacy and liberty viable against an onslaught of technological advancement.

[143] *See* Alex Wawro, *12 Simple Steps to Safer Social Networking*, PC WORLD (Mar. 22, 2013, 3:02 AM), http://www.pcworld.com/article/2031456/12-simple-steps-to-safer-social-networking.html. The right to privacy must equally extend to both the interior of the physical space called home and within the confines of the home-like community of connected individuals—be it within the Twitter community, the Facebook community, the MySpace community, or any other online community. This is because these are self-selected communities that individuals have identified based on

working with the benefit of a lack of legal precedents, can access such prohibited material and develop a flawed assessment of an individual for the predictive analytic purpose of determining such individual's suitability for a particular employment. Not only is such a search into an individual's secluded zone of private affairs against social contract theory, it also violates both the First Amendment right to freedom of expression and the Fourth Amendment right to be secure within one's private surroundings. In the absence of settled law, robust legislation, and precedent judicial determination, using cyber-vetting and employment screening to find the suitable candidate has become an unbridled exercise in developing unfair inferences. This certainly puts privacy and anti-discrimination on a collision course, while implicating the basic fundamental constitutional rights of free speech. This has also attenuated both the right to employment and the right to privacy by pitting the right to employment against the right to expression.[144] Clearly, social media searches of an individual have distorted the fundamental paradigm of signaling in the employment marketplace, where a robust conceptual apparatus for appropriate information transfer is either missing or severely flawed.

IV. A PATH FORWARD—ALLOWABLE CONTOURS OF SEARCHES

Fundamentally, online searches of a candidate's social media activities have the potential to generate subjective and flawed inferences. Therefore, the law must impose a reasonableness or probable cause standard for intrusion against a potential employee's private seclusion. At its core, the purpose of cyber-vetting is to ensure an employer's legitimate business interest.[145] In the absence of objective indicia, an employer is looking to ensure that potential employees are trustworthy and conduct themselves in a manner consistent with societal standards. In essence, through cyber-vetting, an employer is trying to develop a predictable and suitable employee profile by relying on an individual's observable characteristics as manifested in online activities. If, however, an employer is settled on developing a cyber-vetting program, the process must be implemented within the framework of law, taking into consideration both existing and emerging regulatory schemes. More importantly, a search of an individual's digital footprint has the potential to both uncover anomalies[146] and surprises.[147] Employers must be prepared to deal with the legal consequences of such unexpected knowledge.

---

commonalities of interest or shared values. Namsu Park, et al., *Being Immersed In Social Networking Environment: Facebook Groups, Uses, and Gratifications, and Social Outcomes*, 12 CYBERPSYCHOL. & BEHAV. 729, 729 (2009). The increased amount of information available and ease with which it can be accessed should not prevent these individuals from exercising their right to be left alone. *See* Walter, *supra* note 80.

[144] Sprague, *supra* note 48, at 7 (describing balance between individual's right to privacy and employer's interest in uncovering information about potential hires).

[145] Del Riego et al., *supra* note 18, at 17. A slew of litigation in the last decade reveals a potential Achilles' heel for employers.

[146] *See* Zupek, *supra* note 142 (describing termination that occurred after an employer discovered comments an employee had made on Facebook, in which the employee stated that she found her job boring).

This can be illustrated with several examples. First, in the event of a conflict, the employer must carefully recognize that, while information provided on a resume or job application is likely verifiable and deterministic, the information gleaned from an online search could be imprecise or incomplete. Therefore, the danger of false positives may occur, such as basing adverse employment decisions on online information that is applicable to another person or that was falsely manufactured to harm the person under review.[148]

Second, if an online search reveals an individual's audio or video post, even if such digital post may be contrary to an employer's societal mores or behavioral expectation, the employer must find a legitimate linkage between such post and the potential employee's unsuitability for the job. This may thrust the employer into a legal liability based on personality-based discrimination, by placing privacy and anti-discrimination concerns at odds with each other.

Third, even if an online search of an individual's digital activities reveals that the individual may have been engaged in hate, criminal, or terrorist organizations, the First Amendment speech implications must be carefully analyzed prior to making a final determination of the individual's future job status. Thus, employers' legal liability based on violations of the First Amendment is a real concern that employers must recognize.

Fourth, an employer may be in danger of acquiring certain types of information that may bring in heightened legal liability in an attempt to develop efficient and appropriate personnel practices by revealing information related to protected classes.[149]

Therefore, when implementing a cyber-vetting policy, an employer must take into consideration a number of factors. These factors can present as allowable contour of scope and context of search procedure the employer may engage in. The list could be exhaustive, but can be categorized under a set of broader themes. Each theme can be further illuminated by exploring a set of relevant questions.

1. Temporal Aspect and Scope of Cyber-vetting

The questions that must animate the framework are as follows: At what stage during the hiring process should cyber-vetting occur? What should constitute cyber-vetting? What happens when the personnel involved in privileged information are related to a protected status? At what stages during employment should cyber-vetting occur? Should notice of cyber-vetting be given to those being vetted?

---

[147] *Id.* (describing termination that occured when an a young intern told his supervisor that he was unavaialbe due to a family emergency, but co-workers later discovered pictures on Facebook showing the intern attending a Halloween party dressed as a fairy).

[148] *See* John R. Grasso & Brandon Fontaine, *Criminal Consequences of Sending False Information on Social Media*, R.I. B.J., NOV.–DEC. 2011, at 5 (discussing the general unreliability of social media and the potential consequences of using it to publish false information).

[149] Ashley Kasarjian, *The Social Media Checklist for Companies: What Your Clients Should Do, Know and Learn*, ARIZ. ATT'Y, Mar. 2013, at 16, 20.

2. The Issue of Consent and Allowable Trajectory of Cyber-vetting

The following questions should address the issue of cyber-vetting without consent discussed earlier: Is consent required? What are the requirements for personnel conducting Internet searches? What personal information will be used to facilitate a complete and accurate cyber investigation? Is consent required for searching specific social media profiles? Should consent be required from every individual whose profile may become exposed in such searches?

3. The Appropriate Methodology

What are appropriate cyber-vetting methods? How will the cyber-vetting results be authenticated? How should decision makers adjudicate cyber-vetting results? How will the cyber-vetting results be protected from unauthorized disclosure? What recourse does an unsuccessful applicant have in challenging the cyber-vetting results?

To immunize itself from legal liabilities arising out of exposure to privileged or protected class related information, an employer may explore all areas identified above in detail. If an employer's current procedures are not compatible with the framework presented above, the employer must address the gaps and attempt to close the gaps or discontinue cyber-vetting until a robust framework can be implemented.

CONCLUSION

Contemporary society is confronted with a new paradox. In the limitless possibilities of the hyper-technological era, pervasive digital immersion of individuals has created a struggle between social norms and fundamental rights. The ease, access, and sophistication of technology have developed a newer mode of social media driven communication. Yet, exuberance in social media has resulted in a spectacular degradation of privacy. This is manifested in technology-fuelled surveillance delving deeper into an individual's private space, in the name of identifying the most suitable behavioral profile for a particular position. Thus, the fundamental right to privacy has been subsumed into the right to seek meaningful employment.

Individual privacy rights are under violent assault from ever expanding corporate rights. In the absence of robust laws supervising the scope and context of employer behavior in cyber-vetting, retaining individual privacy has become increasingly difficult in recent years. Because employers have an unprecedented arsenal of surveillance mechanisms with which to search the digital footprints individuals leave behind in cyberspace without sufficient legal protections to constrain such surveillance, the time is ripe for a new direction in employment law related to social media usage. This article is an effort in that direction. To evaluate the allowable contour of cyber-vetting, therefore, this work engages in a fundamental analysis of the linkage between individual behavior in social media and the expectation of privacy at the workplace and in an analysis of how employment law should address the growing disconnect in this area. The following observations

should formulate a robust trajectory of employer behavior related to the scope, context, and perimeter of searching an individual's online activities.

First, an employer should recognize that digital immersion with social media exuberance has given rise to pervasive online communication with strangers in cyberspace. In this context, there should be clear delineation between an applicant-employee relationship and an employee-employer relationship. Thus, when the privacy interest is transferred into an applicant-employee relationship, individual's behavioral profile in social media must not be conflated with the expected behavior as an employee within a professional setting. Conflation can result in flawed inferences, exposing the employer to a slew of legal liabilities.

Second, the scope of an employer's surveillance must be balanced with the targeted applicant's subjective expectation of privacy for which constitutional jurisprudence should provide the guiding principle. Revisiting Justice Harlan's two-prong test of privacy, this article contextualizes individual privacy as a function of society's technologically mediated behavior. Thus, the legality of an employer's surveillance should be analyzed as a function of both the employer's legitimate business interest and the affected applicant's expectation of privacy, as measured through the lens of the broader societal expectation.

Third, seamless communication across multiple platforms with multiple individuals with superior access and speed has lowered the threshold of individual privacy. However, individuals retain the ability to determine themselves how much information about them will be available on social media. This in turn must shape an individual's expectation of privacy in society, which can be used as an objective indicium of an individual's expectation of workplace privacy. Employer surveillance must not be able to jeopardize such an expectation. Yet, such an expectation must be objectively indexed based on the new reality of an über-connected social landscape.

Finally, driven by social media exuberance, an emerging behavioral norm is taking root within contemporary society. This norm must be recognized as a driver for shrinking contours of individual privacy. Employer surveillance must take due precaution in not shrinking individual privacy further. Destruction of an individual's right to privacy might aid in compromising an applicant's right of equity and anti-discrimination, which might invite sanctions and legal liabilities against the employer.