Law, Economics and Society; Vol. 1, No. 1; 2025
ISSN 3066-9340 E-ISSN 3066-9359
https://doi.org/10.30560/les.v1n1p169

An Exploratory Study of How Police Background Investigators Use Social Media Screening to Identify Extremism Among Applicants

Steven Matthew O'Quinn[1]

[1] Capitol Technology University, Laurel, Maryland, United States of America

Correspondence: Steven Matthew O'Quinn, Capitol Technology University, Laurel, MD, United States of America. Tel: 1-804-801-4004. E-mail: soquinn@captechu.edu

Received: April 2, 2025 Accepted: April 28, 2025 Online Published: May 19, 2025

Abstract

The institution of policing in the United States cannot function effectively unless the public has adequate confidence in the institution and trusts that officers are vetted for past criminal activity and extremism. Police background investigators thoroughly investigate each applicant's character, creditworthiness, social interactions, education, drug use, honesty, and integrity. Copies of credit scores are obtained, driving history records are examined, national and state criminal history checks are performed, and each applicant's personal history statement (PHS) is taken. Since the rise of social media, investigators have been challenged to gain access to and adequately screen applicant's social media posts to determine extremist memberships or tendencies, as well as past criminal activity. First Amendment protections for applicants in the United States can further hinder an investigator's access to private social media accounts. Past research focuses on ways social media posts can affect workplace hiring and screening of applicants in private industry and government agencies. This study seeks to fill the gap in research by focusing on the unique expectations of the public for law enforcement to screen their applicants at a higher level of scrutiny than private employers and the ethical and legal contexts in which they can accomplish this task effectively.

Keywords: police background investigations, social media screening, extremism, law enforcement recruitment

1. Police Use of Social Media to Screen Candidates

Police agencies also use social media to announce disasters, communicate emergencies to the public, and to attract and recruit the best candidates to help their organization succeed through job announcements (Ralph & Robinson, 2023). Once an applicant expresses interest in employment, the police begin to use social media screenings (SMS) as part of a comprehensive background investigation (Davison et al., 2011). Past criminal activity, extremist viewpoints, and other online interactions, most of which are publicly available for scrutiny, become a part of the background investigator's overall screening of a police recruit's suitability for employment.

5.24 billion people worldwide use at least one social media platform. Nearly seventy percent of the world's population creates digital footprints, and most posts, shares, memes, articles, and pictures are made public for potential employers to peruse and make hiring decisions (Statista, 2025). Employers use both the utilitarian and deontological approaches to conducting social media screenings. From a utilitarian approach, the agency may view that hiring the best overall candidate saves resources, which could be wasted if a poor candidate is selected. Deontologically speaking, police agencies see screening out bad applicants as their duty to save future embarrassment for their agency and exposure to civil litigation (A. F. Johnson et al., n.d.).

Police officers who engage in online speech, even speech that is not illegal and protected by the First Amendment, risk losing the confidence of the public if that speech is racist, sexist, xenophobic, or otherwise distasteful (Abel, 2022). Police departments recognize that it is not only their agency's reputation on the line. If these comments come to light, it could risk jury nullification, prosecutorial decisions not to file charges against their arrestees, or outright dismissal in court proceedings due to a lack of confidence in the officer's testimony.

Police departments intent on monitoring officers' free speech either before or after employment need to consider whether clear policies exist which expressly forbid public content. Police officers have the same speech rights as citizens. However, if an officer speaks on behalf of an agency, those speech rights may be limited (Pickering V. Board of Education, 391 U.S. 563 (1968), n.d.). Furthermore, the courts have affirmed that while police officer's speech is protected against criminal prosecution, the officer, or any government employee, may still be subjected to discipline from their agency (*Garcetti V. Ceballos, 547 U.S. 410 (2006)*, n.d.)

While it seems intuitive that all organizations should be critical of how their employees are seen and viewed by the public, it is essential for public safety agencies tasks with maintaining law and order in an increasingly polarized world (Cubitt, 2023). Realizing that even innocuous posts made or shared by police officers have the potential to diminish the department's reputation, many agencies look at past posts by police applicants to predict future actions by the officer if they are employed. The goal of the current research is to synthesize, through qualitative interviews, the current practices of background investigators concerning the social media accounts of police applicants. Police agencies routinely conduct background investigations to determine an applicant's suitability for employment. In many cases, and especially in smaller departments, routine criminal history checks and driving transcripts are obtained to determine past criminal history. However, this minimalist background check only reveals convictions or, at best, prior arrests.

Formal data retrieval from the National Criminal Intelligence Center (NCIC) is a necessary step in the background process and, in many cases, is required by law in various states before an officer can be hired and commissioned. However, these official data do not uncover criminal tendencies or activity, only arrests and convictions. As such, many departments engage in more informal vetting of candidates, including drug screening, polygraph examinations, credit checks, drug tests, psychological evaluations, and interviews with neighbors and spouses, former teachers, clergy, and associates.

The challenge facing the investigators since the rise of social media is that more and more of these interactions now occur online, may be conducted using aliases by the user, and are difficult to obtain during the investigation. One technique used to uncover social media posts and memberships is to ask the applicant to show the investigator their accounts so they may be inspected in the presence of the investigator. However, these accounts may be deleted or scrubbed prior to the viewing by the applicant who wishes to make their social media pages more presentable by eliminating any online persona they may have created.

To maintain social order, it is imperative that police agencies, and by proxy, their officers, conduct themselves in a way that enhances police legitimacy in the eyes of the public they serve. Research by Lee et al. (2022) concluded that police legitimacy among the public is necessary for preventing violence. Without legitimacy, the public will be less cooperative during investigations, hesitant to report certain crimes, and more likely to resist arrest or disobey a lawful command made by an officer. Public trust and legitimacy are, in this sense, safety issues for the officer, not to mention the citizens themselves. Improving the image of a department is at the forefront of many police executive’s minds if they desire to have an effective agency.

While some may argue that examining old social media posts infringes upon the privacy of individuals, others contend it is necessary in positions requiring public trust and confidence (Abel, 2022). School teachers who may have posted in child molestation forums, candidates for political office who have made anti-patriotic statements, bus drivers with several driving under the influence convictions, and nursing home staff previously accused of endangering the elderly are all examples of why investigating the past of individuals who apply for positions is important. The past does not always predict the future, but agencies and organizations are increasingly expected to do their due diligence in uncovering issues of importance.

With the rise of social media in the United States, many agencies have struggled to abandon old ways of screening applicants and adopt new methods around the current pool of applicants. Policing, in particular, has historically been guided by a set of disqualifying issues that resulted in an immediate denial of employment from a candidate, including prior arrest, criminal history, drug use, and adverse driving history. Research by Morison (2017) contends that police leaders and recruitment managers are constantly reevaluating their screen out criteria as the applicant pool has diminished for prospective police officer positions.

Human Resources personnel and hiring managers routinely use applicant’s social networking sites (SNS) to determine if the person is a good fit for an organization. The onboarding costs associated with hiring new personnel and the investment many organizations make in training lead many organizations to look for signs that an employee is a good fit for the organization before making this investment. Research by Hoek et al. (2016) points to two methods employers use. First, the employer might screen social media accounts before formally offering a position to an applicant. This method usually involves a written policy, a checklist of items to be viewed, and a consent form to obtain the applicant's consent before viewing. Another method involves covertly looking at social media profiles created by the applicant without their knowledge. While exposing the organization to possible litigation, the latter method may prevent applicants from scrubbing their accounts and removing embarrassing past posts before being hired.

Since social media became widespread, organizations have used social media platforms to recruit individuals. Most organizations use social media to recruit, but as of 2024, as few as 20 percent use it as part of the screening

procedure for new applicants (SHRM, 2024). The social media screening process is not always used to find negative posts. Employers may discover good writing and communication skills that help candidates attain employment.

Another concern is the timing of the social media screening in the selection process. Many organizations have policies forbidding the use of specific demographic data to be collected early in the hiring phase. For instance, a mother of three small children might be viewed as someone who could need time off for doctor visits with her children and could need to be absent from work. Employers might view this negatively early in the process and screen out the applicant before they offer an interview or view her qualifications. These screenings may also reveal age, accessibility needs, sexuality, and other personal details irrelevant to a person's ability to do the job adequately. Therefore, organizations committed to a blind hiring procedure may have a written policy forbidding social media screening until just before the job offer is finalized (Sweeney, 2019).

A challenge for many background investigators conducting social media screenings is defining what constitutes extremism. Even if an agency has a policy detailing the protocol for conducting social media screenings, it is nearly impossible to have a database of all organizations, memes, articles, pictures, and jokes that an applicant could leave on a social platform. Therefore, background investigators have much discretion when interpreting what they consider disqualifying. Extremism may be ideological or psychological, yet never implemented (Malcolm, 2023). In other words, simply sharing a tweet or liking a post on Facebook does not make that person an extremist. Being an extremist, at least in the United States, is not a crime. Being a digital extremist who likes, shares, or otherwise promotes extremist ideologies on social media may not be illegal. However, it certainly gets the attention of background investigators for potential police recruits.

In an increasingly hyperpolarized media landscape, the definition of extremism has become blurred. Extremism is challenging to define in the United States since extremist ideologies are not criminalized. The public pronouncement of extremist ideologies, whether racial, religious, or misogynistic, while not illegal per se, risks a loss of public confidence when they originate from a police officer. Social media platforms continue to offer extremist organizations a way to communicate their ideologies and gain membership in their groups (Akram & Nasar, 2023). Therefore, exposure to hateful and extremist content is easier than ever, and the chances of encountering dangerous ideologies online have increased. Moreover, many extremist groups use humor as veiled ideological gateways to recruit like-minded people who might find a meme or photo funny and then like or share the content (Rea, 2022).

Traditional definitions of extremism define a radicalized ideology put into practice, which could lead to terrorist activity in the future if not stopped (Hassan et al., 2023). Since terrorism has replaced the word extremism in the public vernacular, many background investigators are in danger of making a mental leap by judging one or two hyperpolitical social media posts when someone was a teen as a potential terrorist in need of being removed from an applicant pool.

Some states prohibit off-duty conduct as a determinant of employment for most jobs (Vosen, 2021). Some exceptions exist, mainly when employment is important for public trust and confidence. Policing is one of those professions. Current background investigations are concerned with the applicant's drug use, criminal and traffic convictions, and creditworthiness. These actions are presumably off-duty and outside of an applicant's employment. Therefore, proponents of social media screenings argue that vetting candidates through past social media posts and interactions is no different and even more important than past driving records. However, with this practice comes the potential to introduce biases and unfair hiring practices, especially if the social media screening process comes too early (Becton et al., 2019). In other words, social media screenings may introduce political biases, ideological leanings, and personal biases into the minds of background investigators early in the process rather than become a screening technique used to eliminate poor candidates after a hiring decision is made.

Each state has a network of laws and administrative procedures that regulate social media screenings (Johnson & Woolridge, 2024). Some states expressly prohibit any employer, government or otherwise, from requiring applicants to provide passwords or usernames to investigators, add the employing agency to their list of contacts, or compel the prospective employee to open their accounts in the presence of investigators. However, no laws prohibit the agency representative from viewing profiles if the applicant consents. Moreover, even without consent by the applicant, investigators may view any publicly available information the applicant has posted on any platform that anyone can see. The Code of Virginia, for example, expressly forbids any adverse hiring decisions or advancement of an employee if they refuse to supply employers with passwords upon request (*§ 40.1-28.7:5. Social Media Accounts of Current and Prospective Employees*, n.d.)

Case law exists regarding balancing government employees' free speech rights and the agency's need to establish trust and thoroughly vetted employees. However, many of these cases deal with the rights of current employees, not potential employees, in public safety. The courts established the rights of government employees in Pickering v. Board of Education (1968), concluding that public employees do not forgo all constitutional rights just because they are government employees. The Pickering Rule, however, does not apply to potential applicants for government jobs (Wasserman & Connolly, 2017). While many agencies may be concerned with the exposure to litigation by accessing social media posts, others may be equally concerned about a failure to uncover criminal actions and extremist memberships before hiring.

Police misconduct has long been an issue of debate and media attention (Lee et al., 2022). After the video of Derick Chauvin kneeling on George Floyd's neck began circulating online and in the media, calls to defund the police, public demonstrations, and calls for reform dominated the narrative for months (Boudreau et al., 2022). While it has been a longstanding tradition to conduct screenings of who in our society is worthy of carrying a badge, increased scrutiny by the public is likely to lead to increased internal scrutiny by agencies concerning whom they hire and place on patrol.

The President's Commission on Law Enforcement and the Administration of Justice made the first formal recommendation to police agencies in the United States that proper vetting should occur before an agency entrusts an individual with a full-time police role (Katzenbach et al., 2005). Since then, numerous national and state accreditation organizations have ensured background investigations are conducted thoroughly, and written policies are in effect to govern how this is accomplished. However, becoming an accredited agency is typically optional and expensive for the departments (Abner, 2022).

One way the police examine the background of applicants is through cyber-vetting or social media screenings. Social media screening is standard in many workplace hiring protocols, and employers have played catch-up as social media platforms evolve and become more popular and widely used. With many Americans increasingly using social media as their preferred method of communication, background investigators must monitor past online activity to search for criminal and extremist patterns before offering employment (Sweeney, 2019). Agencies may decrease their exposure to negligent hiring lawsuits by thoroughly vetting applicants through social media posts. However, they may also risk the invasion of privacy accusations and the possible reluctance of applicants to apply if they feel a past social media post may be uncovered, especially posts made while the applicant was immature and in their teens.

Current research in social media screening focuses on factors influencing the decision to discipline or terminate current police officers over posts, while little research explores applicant's social media activity. As Cubitt (2023) notes, little research has been conducted on using any vetting procedure to determine whether to hire an officer in the first place. Quality studies are needed to determine whether online posts made before becoming an officer or after working in the field affect performance as an officer. To many police executives, it is the opinion of the public, not merely the officer's performance, that leads to the decision of whether the officer should remain employed or be hired as a recruit.

The current study seeks to uncover social media screening tactics investigators use to determine the suitability of police applicants. More specifically, whether social media screenings are used, and if so, what vetting criteria are used when conducting the screenings. Background investigators who research, investigate, and report on an applicant's criminal history can provide valuable insight into the problem. These investigators are often employed as sworn police officers within a specific department. However, it is common for police retirees and civilians with unique human resource backgrounds and training to conduct the investigations. The current study sought to fill a gap in the existing research on social media use and human resource hiring decisions by contextualizing the unique hiring aspects of sworn officers instead of civilian employees. The following research questions are explored:

R1: Are background investigators conducting social media screenings on applicants, and if so, what are the methodologies being used?

R2: How do investigators gain access to applicants' social media accounts?

R3: How are social media screening findings reported to upper-level management for hiring decisions?

2. Methodology

Qualitative interviews were conducted on a population of background investigators whose primary tasks were vetting police applicants for state, county, and municipal law enforcement agencies. These interviews occurred during March and April of 2025. The method used to identify interviewees was the snowball approach, initially interviewing two background investigators known by the researcher and then using referrals from the first two to

identify other investigators in police departments within the region. Since there are no certifications to provide the researcher with a list of background investigators, referrals from police officers currently working in the field were necessary to identify which officers within an agency routinely conduct the investigations. In some instance, these officers are detectives, although they may be ranking executives or uniformed patrol officers. As contact information was provided, fifteen individuals were ultimately identified at a response rate of 80% after twelve accepted the interview invitation. All interviewees were currently serving as sworn law enforcement officers at the time of the interview.

The interviewees' average years of law enforcement experience was 21.6 years. The average number of years the interviewees have conducted background investigations for their agency was 8.7 years. Of all interviewees, all but one were male (N=11), and one was female (N=1). The sample consisted of interviewees from Tennessee and Virginia. Four agencies represented were from cities or counties with more than fifty sworn officers, five were sheriff's departments, one was from a municipal town of less than 10 sworn officers, and two were from public safety departments at state universities (one from Virginia and one from Tennessee).

Each interviewee was interviewed one-on-one, most lasting less than 30 minutes. The researcher recorded all interview sessions and took notes. A guide was used to ensure all interviewees were asked the same questions throughout the interview. Follow-up probing questions were asked to some interviewees who did not note that social media screenings were a part of their investigative process. After probing questions were used to solicit responses from the interviewees, the researcher engaged in a content analysis of the conversations' records. Inductive coding was used to develop themes and identify patterns within the responses.

The initial research question sought whether background investigators conduct social media screenings (SMS) to determine candidate suitability. Once it was established that SMS screenings occur, probing questions to determine whether the agency had a formal social media policy or whether the investigators themselves determined what was extremist, criminal, or noteworthy were established through follow-up questions to elicit responses. The researcher first asked each interviewee to determine their investigation's top three areas of focus. While most responses were about the applicant's criminal history or driving history, only one interviewee mentioned social media postings at the top of their list. Of interest, most indicated that social media screenings were relatively common, although not required, as exemplified by Investigator 3, who stated, "…*We have to be careful because we do not want them to think it is a make or break for the hiring processes. We see what we can discover by looking at their social media without knowing them. We ask for social media accounts on the questionnaire, so we know upfront which accounts they have".*

Many interviewees indicated that their department does not have a social media policy for applicants. However, most said their agency has a policy for current officers that details what they can and cannot post once they are employed. In other words, none of the agencies have a policy that clearly defines what is permitted, what is tolerated, what could lead to exclusion as an applicant, or what is considered extremist. As investigator number 7 noted, "*We do not have a social media policy, but we have a general morals policy, so social media falls into that category."*

Out of seven interviewees, only one investigator mentioned social media screening unprompted. Once prompted by the interviewer, all investigators began to stress the importance of social media screenings. When asked by the interviewer why social media was not on the top of their list of importance for vetting, many investigators began to describe the private nature of social media, the applicant's rights to privacy, and the technical difficulties of gaining access to the applicant's accounts. Some investigators mentioned that they only consider social media sometimes and do not attempt to see an applicant's profile at other times. As investigator 6 mentioned, " *Sometimes we look at social media. Sometimes we do not. If we look, we just look at what is publicly available. When I do, I use my personal Facebook to browse".*

Notably, none of the respondents indicated a designated social media account set up by their department to research and conduct social media screenings. Most interviewees describe the process of viewing applicants' accounts through their personal social media accounts. Facebook was the most common of the accounts mentioned, followed by Instagram and LinkedIn. Investigator number 4 stated, *"We look at anything open and made public. We ask them if they are on social media. I enter them into an open-source AI database and see if they have ever attached the email address to a social media account. We also use the cell number they provide on their application. If that cell number has ever been linked to a social media account, I will know about it".*

The methods used during the background investigation to gain entry to the applicant's personal social media accounts were explored during the research. None of the interviewed investigators indicated their agency had a policy, nor advertised in the job announcement, detailing that applicants were required to permit the investigator

to access their social media accounts to look for extremist/criminal content. Three of the agencies surveyed gave the researcher a waiver form their agency uses. In these cases, applicants sign a form granting the investigator privileges to access educational records, credit history, driving records, and interviews of references. However, social media accounts were missing from missing on some of the forms provided, suggesting a need to update the forms for a more modern world where social media is omnipresent in the lives of most, if not all, applicants for law enforcement positions.

Interviewees who responded that social media was one of the methods they used in vetting candidates were asked to explain the process of gaining access. All respondents who indicated that they view social media indicated that they use their personal social media accounts rather than a designated departmental social media account in the process. None of the respondents indicated that the process is conducted in the applicant's presence. Interviewee number one explained, "*I do not ask them; we just go on it and troll it. We look at it without their knowledge".* Interviewee number two further explained, " *Typically, we just look for their name. We go to the platform and search their name. During the questionnaire process, we ask them which platform they use".*

Only one investigator expressed that using social media screenings was a high priority during their background process. While this investigator's agency did not have a formal policy about social media for applicants, artificial intelligence is used to search for social media accounts for each applicant. The investigator uses a nondisclosed AI platform to search for any social media accounts connected to the applicant's cell number or email address, both of which are supplied on the employment application. As the investigator explained, "*We ask them on the questionnaire which platforms they use. This database helps to determine whether they were truthful on their application".*

If extremist or criminal content is discovered during the hiring process, only one of the interviewees indicated their agency had a policy to determine whether the content should exclude the applicant from employment. Interviewee four explained, "*If I find something, I submit my report to the hiring captain. In those cases, we have a three-person panel who will review the findings and decide whether to continue the employment process".* Two interviewees said they would include their findings in their final background investigation report. In contrast, one interviewee said they would bring it to the applicant's attention and have further discussions about the post and explain to them that, if hired, the posts are inappropriate for officers in their department.

While none of the interviewees could provide a formal list of what their agency deems extremist or disqualifying, further questioning by the researcher led most investigators to provide their subjective definitions of what they think is inappropriate. The most typical responses were racism, misogynism, and hate speech (although, after probing, none could provide a definition of what hate speech is and what it is not).

None of the respondents mentioned online social media memberships in gangs, criminal organizations, or enterprises listed as a formal disqualifying determinate for employment. Most investigators contended that those memberships would eventually affect hiring, while their departments likely do not have formal policies listing those memberships as disqualifying. In the United States, gang membership is not, within itself, deemed to be criminal due to the First Amendment's freedom of assembly. Paradoxically, most investigator's relayed to the researcher many other protected speech acts that are overtly disqualifying as a matter of public safety according to their departmental policies using broad definitions such as acts of moral turpitude, disagreements with neighbors and family, and various failures to hold public trust.

3. Discussion

According to the Society for Human Resource Management (SHRM, 2024), employers should have a written policy for handling social media screenings. The policy should include a set of questions or a template that the investigator should follow to conduct the investigation in the same manner as each applicant. Additionally, investigators are encouraged to create employer-owned profiles to conduct the screening rather than use their social media profiles. Finally, attention to documenting the screening is paramount, with accompanying screenshots, photographs, and notes for future recollection, just as all other hiring materials are retained.

Standardization in the social media screening policies of police departments is lacking. Agencies should consider adopting a social media screening (SMS) policy detailing which positions require the screening. Investigators should be trained in methodology, reporting, and anti-bias training. Furthermore, identifying, as precisely as possible, the definition of a derogatory post, extremist organization membership, picture, blog, or article and what constitutes a violation. The Washington D.C. Metropolitan Police Department, for example, provides an applicant who had a post or membership flagged by a background investigator during the process the ability to respond in wiring and explain the meaning behind the post (Ashton et al., 2020).

A study by Leott (2019), found that most college students who either majored or minored in criminal justice were aware of the ramifications of social media activity. Furthermore, the students expected that background investigators would screen their social media profiles and indicated they were confident that offensive posts, articles, memes, and shares would not be discovered by the investigator. These findings were consistent with many other professions, including business majors. Thus, it is possible that many prospective applicants are engaging in self-censorship to avoid embarrassing discoveries during the background process.

One limitation of this study is that a particular focus of the research was on potential applicants and not on current employees. Once an applicant is vetted, hired, trained, and begins work in the field, increased training and randomized social media screenings by supervisors or human resources may be beneficial. Radicalization and embracing extremist ideologies may not develop until the officer is hired. Therefore, agencies with solid social media screening policies for applicants should consider a policy for current employees. False information posted, violating trademarks and copyrights, or any racial or biased postings could impeach a current officer's testimony if discovered by defense attorneys, thus rendering the officer's testimony useless in court (Law Enforcement Policy Center, 2019).

There are implications to social media screening procedures that pertain to the overall recruiting policies of police departments. The traditional methods to screen bad applicants include criminal history checks that reveal an arrest, convictions, poor character in the community, poor credit ratings, polygraph examinations, and psychological screenings (Terpstra et al., 2022). Police agencies can create policies to determine which convictions will result in a rejection from the applicant pool, and most requirements are located within the job advertisement. It is relatively straightforward to list that if an officer is convicted of a felony, they need not apply. However, it is a challenge to define what constitutes a racist social media post, a xenophobic meme, or which organizations or groups they should not be a member of on Facebook.

Potential risks and biases are associated with background investigators' more prevalent use of social media screenings during hiring. What might be seen as harmless humor by one background investigator may be seen as a highly offensive post by another. Standardizing what constitutes criminal, offensive, or disqualifying social media activity is necessary, yet remains a challenge. Since no agency represented in this study has a requirement that background investigators explore the social media accounts of applicants, it is up to the investigator to decide whether to explore this area of an applicant’s background. At a minimum, written policies defining clear red flags should be implemented, and the decisions should not be left to one background investigator.

In the absence of clearly defined policies on what is permissible and what is a violation of policies, the background investigators are subject to discriminatory lawsuits brought by applicants whom the agency excluded because of a post, particularly if they continue to use their private accounts to conduct screenings. Furthermore, in the event of a discriminatory hiring lawsuit, the investigator’s private accounts may become subject to scrutiny and discovery during court proceedings. Having designated departmental accounts to view applicant’s posts should be considered a best practice.

Police officer applicants, as well as the police who are presently employed, have First Amendment rights. Furthermore, it is assumed that, at least in the case of applicants not presently employed, the posts, shares, and other social media activity were made and posed on their own time while not at work. However, the same logic applies to creditworthiness, personal interaction with neighbors, driving history, and other events that have been deemed disqualifying for applicants for years. Police agencies, as a matter of public trust and departmental integrity, have always highly securitized the off-duty actions of current and potential employees. Social media activity is no exception.

Interviewee number nine indicated that, in the past, background investigators routinely asked applicants to open their social media accounts during the interview process. However, this practice is no longer permitted within that particular agency. The Code of Virginia prohibits prospective employers from penalizing applicants for failing to provide their passwords to access their social media accounts (§ 40.1-28.7:5. Social Media Accounts of Current and Prospective Employees, n.d.). However, there are numerous privacy laws, such as the right to financial privacy (Right to Financial Privacy Act, n.d.) and the Family Education and Privacy Rights (FERPA) (20 U.S. Code § 1232g - (Family Educational & Privacy Rights, n.d.), both of which are designed to protect the credit scores and educational records from government intrusion. Nevertheless, investigators routinely ask applicants to sign waivers during the background process to permit access to credit and educational records. Adding a social media access waiver alongside financial, personal, and educational records could document the applicant's consent to access these social media accounts, thereby protecting the officer and the agency and, in the long run, ensuring public confidence that agencies are hiring the best officers.

The challenges faced by police agencies concerning social media are shared by other non-police governmental agencies. The digital communication of applicants before hire appears to be a predictor of public employee behavior once they enter an agency. Constitutionally sound policies are necessary going forward which specifically detail permissible online activity, and standardized screening methods should be transparent and readily available to applicants and current employees. A policy that defines the time limits of the speech (i.e. at what age would a post be considered exclusionary for employment), the nature of the prohibited speech (i.e. memberships in foreign terrorist groups online), and a clear definition of what is considered racists, sexists, or extremist based upon the values of the agency is necessary. While it may be impossible to identify all social media content that is not acceptable, a written policy is a necessary first step in communicating the values of an agency with current and prospective employees.

4. Conclusion

While it may be cost-effective for agencies to use social media screenings to assess the fitness of potential employees, and in the case of law enforcement, a necessary screening tool to identify criminal and/or extremist content, the potential for abuse is high. Therefore, guidelines and policies must be in place to balance the agency's needs and the privacy of individuals in a free society. Research by Vosen (2021) suggests that written policies identifying who gets screened, the method it is carried out, and a detailed explanation of what constitutes extremist or criminal content will help shield the agency from litigation and protect the applicant from undue bias and hiring discrimination.

This study stresses the need for agencies to update formal screenings, ensure background investigators receive legal and ethical training in using SMS protocols, establish, at minimum, red flag posts and shares, and establish a protocol for when to elevate findings to upper management for decisions. Furthermore, while creditworthiness, criminal history, arrest records, and driving records are well-established hiring criteria, agencies might consider listing social media activity free from hate speech, criminality, and acceptable as an officer as part of the job requirements in the advertisement for employment. Career counselors, criminal justice college faculty, and recruiters might then be armed to stress the need for an acceptable social media presence to young students and job seekers hoping for a career in law enforcement.

This study examined the practice of background investigators' use of social media screening for hiring; however, research into the use of social media practices of those currently employed within a law enforcement agency and its impact on promotion and termination is lacking (Becton et al., 2019). Furthermore, the small sample size in this study was limited to two states, each having two distinct sets of employment laws and policies limiting the government's access to the social media accounts of prospective employers. In the absence of a centralized police force in the United States, each state must be researched individually to gain a better understanding of current practices. More research is needed in other states, which could contain samples of larger departments, state police department, and federal agencies.

Research is needed to determine the current practices of enforcing social media etiquette during the training phase and after employment is secured. While state government and local agency policies vary, a study of federal law enforcement agencies could provide some insight into how the federal workforce screens law enforcement applicants. In the case of the federal government, the officers are spread out over a vast geographic region, yet all function under the same human resource agency setting those specific social media policies. State police agencies and university system police departments provide future researchers another area of focus. Concerning universities, especially those systems governing many unique college campuses, research into whether traditional harbors of free speech (the campus) extend that same speech to its police officers warrants further attention and research.

References

§ 40.1-28.7:5. Social media accounts of current and prospective employees. (n.d.). Virginia Code. https://law.lis.virginia.gov/vacode/title40.1/chapter3/section40.1-28.7:5/

20 U.S. Code § 1232g - Family educational and privacy rights. (n.d.). Legal Information Institute. https://www.law.cornell.edu/uscode/text/20/1232g

Abel, J. (2022). CoP- "Like": The First Amendment, criminal procedure, and the regulation of police social media speech. *Stanford Law Review, 74*(6), 1199–1252. https://www.stanfordlawreview.org/print/article/cop-like/

Abner, G. (2022). Predictors of public support for police accreditation. *Policing: An International Journal, 45*(5), 828–845. https://doi.org/10.1108/PIJPSM-02-2022-0035

Akram, M., & Nasar, A. (2023). A bibliometric analysis of radicalization through social media. *Ege Akademik*

Bakis (Ege Academic Review), 23(1), 1–14. https://doi.org/10.21121/eab.1166627

Ashton, P., Kane, C. M., Strang, B., Tignor, J., Vorndran, K., & Tobin, M. G. (2020). *Personal use of social media*. Office of Police Complaints. https://policecomplaints.dc.gov/sites/default/files/dc/sites/office%20of%20police%20complaints/publication/attachments/PersonalUseofSocialMedia.FINAL_.pdf

Becton, J. B., Walker, H. J., Gilstrap, J. B., & Schwager, P. H. (2019). Social media snooping on job applicants. *Personnel Review, 48*(5), 1261–1280. https://doi.org/10.1108/PR-09-2017-0278

Black, S. L., Stone, D. L., & Johnson, A. F. (2014). Use of social networking websites affects applicants' privacy. *Employee Responsibilities and Rights Journal, 27*(2), 115–159. https://doi.org/10.1007/s10672-014-9245-2

Boudreau, C., MacKenzie, S. A., & Simmons, D. J. (2022). Police violence and public opinion after George Floyd: How the Black Lives Matter movement and endorsements affect support for reforms. *Political Research Quarterly, 75*(2), 497–511. https://doi.org/10.1177/10659129221081007

Cubitt, T. I. C. (2023). The value of criminal history and police intelligence in vetting and selection of police. *Crime Science, 12*(1), Article 2. https://doi.org/10.1186/s40163-023-00186-3

Davison, H. K., Maraist, C., & Bing, M. N. (2011). Friend or foe? The promise and pitfalls of using social networking sites for HR decisions. *Journal of Business and Psychology, 26*(2), 153–159. https://doi.org/10.1007/s10869-011-9215-8

Garcetti v. Ceballos, 547 U.S. 410 (2006). https://supreme.justia.com/cases/federal/us/547/410/

Hassan, H., Farine, L., Kinnish, N., Mejía, D., & Tindale, C. (2023). What is extremism? Advancing definition in political argumentation. *Topoi, 42*(2), 573–581. https://doi.org/10.1007/s11245-023-09895-5

Hoek, J., O'Kane, P., & McCracken, M. (2016). Publishing personal information online. *Personnel Review, 45*(1), 67–83. https://doi.org/10.1108/PR-05-2014-0099

Johnson, A. F., Roberto, K., & Myers, E. (n.d.). Using social media in the selection process: An ethical perspective for employers and applicants. *SAM Advanced Management Journal*, 42–48. https://doi.org/10.52770/CBTK6384

Johnson, A., & Woolridge, C. (2024). Selection protections in the social media landscape: More justice needed? *Journal of Managerial Issues, 36*(2), 112–126.

Katzenbach, N. D., Isidore, & Silver, I. S. (2005). *The challenge of crime in a free society*. Bureau of Justice Statistics. https://openlibrary.org/books/OL14365552M/The_challenge_of_crime_in_a_free_society

Law Enforcement Policy Center. (2019). *Social media: Considerations*. International Association of Chiefs of Police. https://www.theiacp.org/sites/default/files/2019-05/Social%20Media%20Considerations%20-%202019.pdf

Lee, S. U., Hamm, J., & Lee, Y. H. (2022). Instrumental and normative pathways to police legitimacy: Why do people cooperate with the police? *Policing: An International Journal, 45*(5), 812–827. https://doi.org/10.1108/PIJPSM-03-2022-0037

Leott, Y. M. (2019). #Screening out: Criminal justice students' awareness of social media usage in policing. *Cogent Social Sciences, 5*(1), Article 1573570. https://doi.org/10.1080/23311886.2019.1573570

Malcolm, F. (2023). Analysing extremism. *Ethical Theory and Moral Practice, 26*(2), 321–327. https://doi.org/10.1007/s10677-023-10370-8

Morison, K. P. (2017). *Hiring for the 21st century law enforcement officer: Challenges, opportunities, and strategies for success*. Office of Community Oriented Policing Services. https://cops.usdoj.gov/RIC/Publications/cops-w0838-pub.pdf

Pickering v. Board of Education, 391 U.S. 563 (1968). https://supreme.justia.com/cases/federal/us/391/563/

Ralph, L., & Robinson, P. (2023). Assessing police social media practices through a democratic policing lens. *International Journal of Police Science & Management, 25*(3), 237–249. https://doi.org/10.1177/14613557231169391

Rea, S. C. (2022). Teaching and confronting digital extremism: Contexts, challenges and opportunities. *Information and Learning Sciences, 123*(1/2), 7–25. https://doi.org/10.1108/ILS-08-2021-0065

Right to Financial Privacy Act. (n.d.). Federal Reserve. https://www.federalreserve.gov/boarddocs/supmanual/cch/priv.pdf

SHRM. (2024, January 26). *How to use social media for applicant screening*. Society for Human Resource Management. https://www.shrm.org/topics-tools/tools/how-to-guides/how-to-use-social-media-applicant-screening

Statista. (2025, February 13). *Worldwide digital population 2025*. https://www.statista.com/statistics/617136/digital-population-worldwide/

Sweeney, D. (2019). *Social media screening of homeland security job applicants and the implications on free speech rights*. Naval Postgraduate School. https://apps.dtic.mil/dtic/tr/fulltext/u2/1073680.pdf

Terpstra, B., White, M. D., & Fradella, H. F. (2022). Finding good cops: The foundations of a screen-in (not out) hiring process for police. *Policing: An International Journal, 45*(4), 676–692. https://doi.org/10.1108/PIJPSM-08-2021-0116

Vosen, E. (2021). Social media screening and procedural justice: Towards fairer use of social media in selection. *Employee Responsibilities and Rights Journal, 33*(4), 281–309. https://doi.org/10.1007/s10672-021-09372-4

Wasserman, L. M., & Connolly, J. P. (2017). The Garcetti effect and the erosion of free speech rights of K–12 public education employees: Trends and implications. *Teachers College Record, 119*(6), 1–28. https://doi.org/10.1177/016146811711900607

Appendix A

Survey Instrument

An Exploratory Study of How Police Background Investigators Use Social Media Screenings to Identify Extremism Among Applicants

Principle Investigator: Steven M. O'Quinn

Interview date:

Interview location:

1. How many years of law enforcement experience do you have total?
2. How long have you been conducting background investigations?
3. What are the top three focus areas of your investigation when determining whether a candidate is suitable for employment with your agency?
4. Do you view what a police applicant posts (or previously posted) on social media (pictures, memes, articles, posts) as something police background investigators should use as a part of the vetting process?

   Follow up: Does the age of the applicant at the time of the post make a difference?
5. Can you tell me about a time you conduct social media screenings (SMS) as part of the background process?
6. Does your agency have a written social media screening policy?
7. Can you walk me through the steps you take to view a candidate's social media accounts?

   Follow up: If the applicant refuses to grant you access, how do you handle the situation?
8. How do you identify extremist social media posts or content during the investigation process?
9. How do you determine if an applicant's casual interaction with extremist online content is a sign of extremist ideologies?
10. How are your findings reported to upper level management for hiring decisions?
11. I've asked you a lot of questions about what it was like to conduct background investigations and do social media screenings. I'm wondering if there is anything I've forgotten to ask, especially because I haven't had that experience myself?