NM Bar Student Essay Contest

Micaela de la Rosa

Centennial High School

Mr. Joel Hutchinson

(1499)

Background

Bill was hired for a summer job with the expectation that he would be hired for a part-time job when he started college. All went as planned, and he was offered the desired position at the end of the summer. During the interview, Bill was asked to identify any social media sites to which he belonged, as well as provide usernames and passwords for each. The company required military clearances for those working on large government contracts, and though Bill was involved with none of them, he was still required to provide access to private online accounts.

A much-disputed topic in current news is the question of employee privacy rights; namely, whether it is constitutional for employers to require employees to provide usernames and passwords to all their online social media accounts. The practice of demanding such access to secure social media sites is fast-becoming a common one, and it has sparked a debate as to whether these actions are prohibited by law. Current investigations into federal and state laws dealing with the violation of an employee's online privacy have turned up inconclusive results. The popular opinion in regards to whether or not employers are violating an employee's constitutional right to privacy by asking for usernames and passwords are strongly

against the practice, believing it to be an unlawful intrusion upon the latter's private and personal lives.

Is it constitutional for employers to gather passwords to social media accounts such as Facebook and Twitter, as part of a background check for a job?

Brief Legal History

Several cases dealing with the legality of demanding personal information from employees have caught public attention. One of these, *Pietrylo v. Hillstone Restaurant Group,* addresses the issue of online privacy. Brian Pietrylo and Doreen Marino sued the owners of their place of employment, Houston's restaurant, after managers logged onto a private site the pair had created where employees made negative comments and jokes about the restaurant. Managers asked employee Karen St. Jean for her username and password to the forum, the comments were viewed, and Pietrylo and Marino were fired. They sued, claiming their managers had violated their constitutional privacy. St. Jean's testimony that she "thought [she] would get in trouble" was instrumental in persuading the Court to rule in favor of the ex-employees. The Stored Communications Act, according to legal columnist Anita Ramasastry, "prohibit[s] intentional access to electronic information without authorization". Since St. Jean had been coerced into giving up the information, the managers had no legal authorization to visit the site. The Court ruled that the managers had intentionally violated the privacy of their employees.

Putting aside the fact that these two individuals were current employees of the establishment and Bill is still in the potential-employee stage, this case provides a valid legal base for the argument that Bill's employers would be violating his privacy by demanding that he turn over access to personal social media accounts. Bill would be coerced into giving the information for fear of being denied the desired position if he did not.

In a similar case, *Konop v. Hawaiian Airlines, Inc.*, employee Robert Konop sued the agency for viewing a secure website he created, through the use of the names of two employees. Konop claimed that company vice president James Davis had been in violation of the federal Wiretap Act and the Stored Communications Act, among others. The Court ruled that the website fit the Wiretap Act's definition of protected material ("any [intercepted] wire, oral, or electronic communication"). Since the website falls under the category of stored "electronic communication", and only "wire communication" can be intercepted, the agency was not in violation of the Wiretap Act. The Shared Communications Act provided even less legal protection to stored electronic information.

Overlooking the fact that Konop was a current employee and Bill is not, it can be predicted that Bill would be similarly protected (or similarly unprotected) by the Wiretap Act. If Konop's private, secure website conversations do not fall under the category of "intercepted" material, Bill's postings on a public social media site will be even less likely to fall under the Act's protection.

Recent questions about employee privacy rights are not limited to unwelcome online involvement. In *NASA v. Nelson*, twenty-eight engineers and

scientists from Caltech's Jet Propulsion Laboratory sued the Department of Commerce, Caltech, and NASA, claiming that their required background checks violated constitutional privacy. The checks were instituted after the 9/11 attacks, and applied to all contract government employees. They included questions about drug treatment and counseling, and were mandatory for the employees in question to retain their jobs. Acting based on precedents set by previous cases, (*Whalen v. Roe* and *Nixon v. Administrator of General Services*) the court ruled that although employees do have a right to privacy, the background checks were not violating it.

Again ignoring the fact that Bill is not yet an employee, it can be deduced that, like the NASA employees, Bill would not have his constitutional privacy legally violated by the demand for personal information. The argument has been made that viewing a potential employee's social media account could be both part of, and similar to, running a background check on the person. If the former is not illegal, then it can be deduced that the latter is not either (regardless of how unpopular both practices may be).

Present Legal Situation

The legal situation surrounding employee privacy rights is admittedly murky. The US Constitution states that "Congress shall make no law…abridging the freedom of speech" (1st Amendment) and "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches…shall not be violated" (4th Amendment). Private sites fall under the protected category of "freedom of speech", and asking an employee for access to their personal social

media accounts constitutes as an "unreasonable search". The 1st Amendment applies to Congress however, not directly to employers, and the term "unreasonable" is relative and subject to interpretation. The Washington Post states that "it is neither an invasion of privacy nor a violation of constitutional rights" for employers to demand the usernames and passwords to the social media sites to which their employees belong. Facebook itself has taken a stand against such actions, considering them a security risk and threatening privacy violators with legal action.

The line gets even more blurred when the employee in question is still a potential-employee (like Bill) involved in the interview process. Current employees enjoy greater rights than individuals still going through the hiring process. Ramasastry argues that "since prospective employees…do not have an established work relationship with the employer and have not used company computers to make postings…requiring them to give over their [social media] passwords is a violation of the SCA". Since would-be-employees (like Bill) are at the disadvantage in the interview process, it could be considered coercion for interviewers to demand they hand over access to such personal information. She also makes the case that since "employers are prohibited from asking certain questions in an interview", they should likewise "be prohibited from using Facebook to run around those ends'. Another argument against the practice, as presented by journalist Nicholas F. Casolaro, is one of "liability based on federal and state anti-discrimination laws", which prohibit employers from taking a candidate's "national origin, religious views, disabilities, age, marital status, or other classifications [including appearance]" into

consideration during the hiring process. If an employer logged onto a potential employee's social media account, (for example, Bill's) and that person happened to belong to a social or religious organization, the employer could be at risk for a lawsuit if he decided not to hire that person, especially if the cause was something they found while logged into the account.

Senators Richard Blumenthal (CT) and Charles E. Sumner (NY) have pushed for legislation to restrict employer demands of usernames and passwords during the job interview process. According to the New York Times, "[t]he senators said they were writing a bill to fill any gaps not covered by current laws." (Such gaps would most likely include those in the SCA and the Wiretap Act that would fail to protect potential-employees like Bill.) State legislatures also agree that this practice is unconstitutional, whether or not it has been made illegal. According to Casolaro, "[a]t least seven states – Maryland, Illinois, California, Massachusetts, New Jersey, Washington, and Minnesota – have already introduced legislation that would prohibit employers from asking for usernames and passwords to social media Web sites". These measures would prevent employers' intrusions of both current and would-be employees, effectively sheltering individuals like Bill from having to hand over such personal information.

Many individuals from a variety of occupations have found themselves in Bill's position, required to hand over personal usernames and passwords, providing access to secure sites that hold information not meant for unrestricted public consumption. Although current law may not explicitly prohibit the practice, public

and legislative opinions have recognized it for what it is: an unconstitutional intrusion upon the personal privacy of an individual.

Ruaidhrí (Rory) Crofton

West Las Vegas High School

Ms. Carmen Baca

Word Count: 1,326

I. Introduction

Bill was very excited that he had just been hired for a summer job that promised him a part-time position when he began college if he performed to expectations. Bill was well liked by his supervisor and coworkers, and at the end of the summer he was told that he would be hired for the part time position. The company Bill worked for, however, had a few large government military contracts with some that required special military clearances. As a result, Bill was asked to consent to a criminal background check, drug test, and provide the company with the most recent copy of his credit history as part of the hiring process. Additionally, Bill was asked for a list of all the social media sites he was a member of and to provide the usernames and passwords for each one.

II. Is it constitutional for employers to gather this type of information, including passwords to social media accounts such as Facebook and Twitter, as part of a background check for a job?

No other invention in the twenty-first century has affected our lives more than the creation of social media. Through online sites such as Facebook, Twitter, and YouTube, information in the form of messages, photographs, and videos can be quickly and easily shared by a single person to millions of others around the globe. Depending on the nature of the post and how the poster feels about its content, this information can be made more or less public; allowing only a select group of friends and family access to

more personal information. More and more often in today's society, however, part of an application process for a job may include providing a prospective employer with the username and password to social media sites we use. This in turn allows them to view information we may consider personal and confidential as part of a background check. Although no laws currently exist that would label this practice as "illegal" many view it as a violation of their rights set forth by the Constitution of the United States and wish to see its use discontinued.

Ratified in 1791, the Fourth Amendment of the US Constitution states that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Although no specific mention of information shared or stored on social media sites is made in this amendment due to the time in which it was drafted, it does guarantee citizens of the United States the right to have their personal belongings and papers protected from search and seizure without probable cause and a warrant -- two things often not considered or used by employers requesting the information. Court cases, such as *NASA vs. Nelson, 131 S. Ct. 746, 562 US __, 178 L. Ed. 2d 667, No. 09-530 (2011)* have pursued the conviction of companies for violating this constitutional right to informational privacy; in this case, twenty-eight scientists and engineers suing NASA, Caltech, and the Department of Commerce. While it could be argued that personal property becomes public once posted online and that this right in turn does not apply to "personal" property once posted on the internet, a place where anyone has access to it,

the practice of prospective employers viewing an applicant's social media pages should theoretically be prevented by the Bill of Rights as personal houses, papers, or effects under the Fourth Amendment.

In addition to the right to privacy and the prevention of unreasonable searches and seizures set forth in Amendment IV, other amendments and articles throughout the United States Constitution also make it unconstitutional for anyone, including employers, to discriminate against potential employees based on their gender, age, ethnicity, disability, religion, or beliefs. Probably the most well-known example of such amendments is Amendment I, which states "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." By requesting the passwords to social media sites as part of a background check, employers are in violation of these rights by accessing personal information that may pertain to a person's religious, social, political, or other beliefs. Whether deliberately or not, having learned this information may affect an employer's views of an applicant which could in turn lead to discrimination based on an employer's or company's own set of beliefs.

As set forth in the Ninth Amendment to the United States Constitution, failure of the Constitution to mention a specific right within its articles or amendments does not necessarily mean the right can be abridged, but rather that it must be covered by a separate law or act as determined by the United States Congress. As a result of the Constitution's failure to specifically mention anything about internet informational privacy, several acts have been passed to address this issue instead. The Stored

Communications Act: 18 U.S.C. Chapter 121 §§ 2701-2712 prohibits intentional access to electronic information without authorization or intentionally exceeding that authorization. The Computer Fraud and Abuse Act: 18 U.S.C. § 1030 also prohibits intentional access to a computer without authorization to obtain information. Whilst these laws prevent violations of prospective employee's personal information online, they are still relatively vague and apply to the internet as a whole, as opposed to social media specifically. Several lawsuits have since been filed under both the Computer Fraud and Abuse and the Stored Communications Act since their ratification. Such cases include *Konop vs. Hawaiian Airlines, Inc., 320 F.3d 868 (9th Cir. 2002)* and *Pietrylo vs. Hillstone Restaurant Group, 2008 WL 6085437 (D.N.J., July 25, 2008.* Both cases involved employees of either Hawaiian Airlines or Hillstone Restaurant Group who claimed that their employers had viewed their private and secure social media accounts without their prior permission. However, only the Pietrylo vs. Hillstone case was successful.

Finally, according to Amendment X of the US Constitution, " The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people." In turn, many states, such as Maryland and Illinois, have used the power given to them under this amendment to enact laws banning employers for asking for their current or perspective employees' social media passwords. These laws, whilst not a part of the Constitution itself, do much more to prevent this unconstitutional practice from occurring as they specifically mention personal information online that is posted on social media sites. Other laws, acts, and

amendments, however, mention this issue in a vaguer manner, specifying only personal papers and property or information posted on the general web.

III. Conclusion

In today's society, it is becoming more and more common for prospective employers to ask applicants for access to their personal social media accounts as part of a background security check. Although no specific mention of social media or internet privacy is made within the articles or amendments of the Constitution of the United States, an in depth analysis of the first and fourth amendments does suggest that this practice is in violation of a citizen's right to freedom of speech and religion, and freedom from unreasonable search and seizure of private property and papers. Although many court cases have been fought and multiple laws and acts have been passed by the national and state governments in an attempt to outlaw such practices, they continue none the less. However, there is no doubt that the practice of employers requesting social media passwords from their employees is indeed in violation of the rights of every citizen as stated in our national Constitution.

Works Cited

Anita, Ramasastry. "Can Employers Legally Ask You for Your Facebook Password When You Apply for a Job?." N.p., 12 Mar 2013. Web. Web. 22 Feb. 2013. <http://bit.ly/H8wjFc>.

United States. Congress. *Stored Communications Act*. Print.

United States. Congress. *Computer Fraud and Abuse Act*. Print.

"US Constitution." United States Senate, n. d. Web. Web. 22 Feb. 2013. <http://1.usa.gov/krfjhI>.

Ronald Davis III
Onate High School
Dr. Anne Foltz
Word Count: 1460

Introduction

Bill has been hired for a summer job with hopes that it will become his part-time job when he enters college. Bill's salary from the part-time position would cover his tuitions with $2,000 to spare. The hiring company had some large government military contracts, requiring special military clearance for some jobs. Even though Bill was not allowed to work on any of the special jobs, he enjoyed being around people who may have the clearance. He proved satisfactory and obtained the part-time job. In addition to a criminal background check, a drug test, and a recent copy of his credit history, Bill was required to identify all social media to which he was currently affiliated as well as the username and password for each. What must be determined is if the company can ask for his social media information, and to what extent they can use or view it.

Law Interpretation

The Computer Fraud and Abuse Act states that whoever accesses unauthorized or exceeds authorized access on a computer is subject to punishment. To "exceed authorized access" is to alter or obtain information that one is not entitled to alter or obtain. This act only allows the employing company to access information that Bill authorizes or entitles them to access.

The purpose of the Stored Communications Act is to protect the privacy of stored electronic communications. According to this act, intentionally accessing "a facility through which an electronic communication service is provided" without proper authorization or intentionally exceeding the authorization of the facility are punishable offenses. Exceeding the

authorization of a facility includes obtaining, altering, or preventing authorized access to the electronic communication service. The SCA restricts Bill's employer to view only authorized information and take authorized actions on Bill's social networking accounts.

The Wiretap Act has several provisions, but only three apply to Bill's scenario. It states that one may not intentionally intercept or attempt to intercept an oral, wire, or electronic communication neither directly nor through another person. Also, one cannot intentionally disclose the content of the electronic communications with knowledge that the information was intercepted in violation of the first provision of the Wiretap Act. Using the content of the communications in violation of this act for any purpose is also illicit. The Wiretap Act forbids Bill's employer from listening to his conversations, whether it is talking on the telephone or instant messaging on a social media site.

These acts explicitly restrict Bill's employers from obtaining any unauthorized information or eavesdropping on any of his communications. So as long as Bill agrees to authorize the information to his employers, everything complies with the constitution. The question remains: can the company constitutionally force Bill to provide information about his social media as a condition of his employment?

Court Cases

In the Pietrylo v. Hillstone Restaurant Group [06 Civ. 06-CV 5754 (FSH)] court case, the employer unconstitutionally accessed an electronic communication service in violation to the SCA. Pietrylo created a private group on his MySpace account dedicated to posting contempt against his employers. His managers became suspicious of the workers, so they "strong-armed and threatened a member of the private group so that this member was forced into providing them with the member's email address and password" to investigate the group. Hillstone was

found to be in violation of the SCA because the information was coerced out of the employee; the employee did not willingly give his/her consent. Bill must provide his social media information to the company, but he is not being forced or threatened to give up his information. He does not have to take the job, and he will not get into any trouble (unlike the Hillstone employee) if he doesn't provide his information. The choice is freely his to make. As long as Bill retains his listed constitutional rights, a private company can require that he provide the information.

In a similar circumstance, a pilot for Hawaiian Airlines Inc., Konop, hosted a website (the Air Line Pilots Association or ALPA) where he posted criticisms of his employer, officers, and certain unions. He provided usernames that allowed access to the bulletins to some fellow Hawaiian pilots while avoiding his employer and union representatives. James Davis, the vice president of the company, became suspicious of untruthful claims and used the username of Hawaiian pilot Gene Wong (with his permission) in order to make an account. In the process, Davis agreed that he was Wong and that he would not disclose any information. Konop discovered Davis's intrusion and sued him in the Konop v. Hawaiian Airlines Inc. [No. 99-55106, 236 F.3d 1035 (9th Cir., January 8, 2001), withdrawn, 262 F.3d 972 (9th Cir., August 28, 2001)] case. Finding in favor of Konop, the Supreme Court asserted that Davis violated the user agreement; hence, he did not have authorized access, infringing on the SCA. The Wiretap Act was also contravened, as he intercepted an electronic communication. The violation of the Wiretap Act in Konop's incident affirms the fact that Bill's employer cannot intercept or listen to ongoing conversations on the social media sites. This court case also led to the principle that the access to the electronic communication service must be direct and valid. In Bill's case, the employer would have legitimate, authorized access to his social media, most likely in a signed

contract. Bill must willingly give permission to his employer to access his social media accounts in order for the company to constitutionally access his electronic communication service.

The case of United States v. Turk [No. 90-5091-cr (2nd Cir. Nov. 30, 2010)] has also helped clarify the Wiretap Act. This case focused on whether listening to a recorded phone call without the authorization of its owner or a warrant was constitutional. The Supreme Court held that the actions of the police was constitutional and did not violate the Wiretap Act because they were not listening to a live, ongoing conversation; they were listening to a recorded audio tape. The Supreme Court's verdict made clear that the interception of the oral, wire, or electronic communication must occur at the same time the communications are made. This verdict asserted both a constitutional action and an unconstitutional action. With proper authorization one may view archived data, but may not view ongoing communications. Likewise, the company hiring Bill can read posts he *sent*, but not monitor current conversations.

Ethics

In addition to the constitutional interpretations of the law, determining if the actions are fair and responsible is also important. The company's request for Bill's username and password is fair because Bill is not being forced or coerced into giving his information to them. Bill simply must provide the information if he wants the job. A formal, written mutual agreement can avoid any charges between Bill and his employer.

Essentially, the job slot is the employer's, not Bill's. The employer should be able to require any information desired, as long as the information does not invade any constitutional rights. The choice to hire Bill solely belongs to the judgment of the company and the employer. Bill is in no position to argue about the requirement unless that requirement violates his constitutional rights, which this requirement clearly does not.

Most importantly, the job revolves around high clearance affairs. For this specific occasion, Bill's username and password for his social media especially should be available to the company. Special precautions should be taken for a job of this caliber where classified information is within Bill's reach. The ability to view information on Bill's social media may reveal aspects about him to the employer. The employer may find out that Bill plans to leak some information, engage in devious activity, or even conspire against the company.

Conclusion

Gathering information from social media accounts is constitutional because the CFAA, the SCA, and the Wiretap Act do not forbid such an action. These laws state what *cannot* be done and only restrict what the employer can do concerning Bill's electronic communication services. The Pietrylo v. Hillstone Restaurant Group [06 Civ. 06-CV 5754 (FSH)] and the Konop v. Hawaiian Airline Inc. [No. 99-55106, 236 F.3d 1035 (9th Cir., January 8, 2001), withdrawn, 262 F.3d 972 (9th Cir., August 28, 2001)] court cases help clarify the restrictions set by the laws and provide examples of improper access to electronic services. The United States v. Turk [No. 90-5091-cr (2nd Cir. Nov. 30, 2010)] case specified the provisions of the Wiretap Act.

If Bill's case when to court, then the court would most likely rule in favor of the employer because the information required does not violate Bill's constitutional rights. Further, the courts would likely rule in favor of the employer because Bill's presence may hinder national security without the proper precautions because he will work in a classified environment.