

Testimony of Fran Freedman

Deputy Commissioner

NYC Department of Consumer Affairs

New York City Council Civil Service and Labor

Committee Hearing

September 25, 2013



Jonathan Mintz
Commissioner

Fran Freedman, LMSW
Deputy Commissioner for
External Affairs
FFreedman@dca.nyc.gov

42 Broadway
8th Floor
New York, NY 10004

+1 212 000 0000 tel
+1 212 000 0000 fax

nyc.gov/consumers

September 25, 2013

Council Member Michael Nelson
Chair, Committee on Civil Service and Labor
Hearing Room, 16th Floor, 250 Broadway
New York, NY 10007

Re: Intro 1106

Dear Chairman Nelson:

Thank you for your invitation to comment on Intro 1106, legislation which would prohibit employers, employment agencies and labor organizations from requiring access to online social networks and other personal accounts of employees and prospective employees in connection with the hiring process.

The Department of Consumer Affairs (DCA) has no testimony to offer on this subject, however, nor does it have an expertise that would be of use to the Council in its deliberations regarding this bill. Indeed, the subject matter of this bill, while proposed to be appended to the Department's chapter of the New York City Charter and Administrative Code, has no substantive connection to its mission, work and expertise.

For nearly 45 years, since its creation by the Council in 1969, the Department of Consumer Affairs mission has been to empower businesses and consumers to ensure a fair and vibrant marketplace. At its core, the Department's work is focused on protecting consumers in the commercial retail arena by licensing businesses (now more than 81,000 in 55 different industries); regulating industries which have the potential to harm consumers but which it does not license; enforcing Council's comprehensive Consumer Protection Law and other related business laws in all retail business in the City; mediating and resolving consumer complaints against businesses; and adjudicating consumer claims and violations against retail businesses. DCA's expertise lies in dealing with every aspect of the complex and multilayered transactional relationships between consumers and businesses. Beginning In 2006, with the launching of DCA's Office of Financial Empowerment, the Department developed expertise, services and programming for consumers with low incomes in the financial marketplace as well.

If you have further questions or concerns about the Department or its mission, please don't hesitate to contact me at 212 436 0179 or by email at ffreedman@dca.nyc.gov

Sincerely,

A handwritten signature in black ink, appearing to read "Fran Freedman". The signature is written in a cursive style and is positioned above the printed name and title.

Fran Freedman, LMSW
Deputy Commissioner for External Affairs



NYCLU

NEW YORK CIVIL LIBERTIES UNION

125 Broad Street
New York, NY 10004
212.607.3300
212.607.3318
www.nyclu.org

Testimony of the New York Civil Liberties Union
before
The New York City Council
Committee on Civil Service and Labor
Regarding Introduction 1106-2013, Relating to Online Social Media and other Personal
Online Accounts and Employment
September 25, 2013

My name is Nate Vogel, and I am a legislative counsel with the New York Civil Liberties Union, on whose behalf I respectfully submit this testimony. I would like to thank the committee on Civil Service and Labor for inviting the NYCLU to provide testimony on Intro 1106. The NYCLU is a not-for-profit, non-partisan organization with almost 50,000 supporters around the state, including nearly 26,000 in New York City. The NYCLU is the foremost defender of civil rights and civil liberties in New York State.

We support Intro 1106. The bill would prohibit employers from requiring job applicants or employees to give the employer access to their private, personal online accounts. It has never been acceptable for an employer to go to an employee's home, read his or her mail, peruse a personal diary, or listen to the employee's home phone calls. The same consideration should apply to all our private communications.

As more and more of our lives are lived online, employers here in New York and across the country are increasingly turning to social media to assist them in making decisions about hiring, promotion and retention. For many years, employers have searched for publicly available information about job candidates and existing employees on sites like LinkedIn and Facebook. A 2011 study found that 89% of employers use social media in their recruiting.¹ A separate study in 2013 reported that 43% of hiring managers who use social media to research applicants had

¹American Bar Association, *Social Media in Recruitment and Hiring* (Sept. 2012), available at http://www.americanbar.org/newsletter/groups/labor_ll_flash/1209_aball_flash/lel_flash_9-2012tech.html.

decided not to hire someone based on what they found online.²

A recent trend has emerged and employers are now seeking access to information about employees and applicants that is maintained in social media fora but not publicly accessible because the employee or applicant has restricted his or her audience. Employers do this by requiring employees and applicants to grant them access to private accounts.

Last year, the AP reported the story of Justin Bassett. Mr. Bassett, a New York City-based statistician, applied for a new job.³ After searching for Bassett's Facebook page and finding it restricted, his prospective employer asked for his log-in information. Mr. Bassett refused to give it, and he withdrew his job application.

But not everyone can afford to refuse an employer's request. In 2010, Robert Collins testified before the Maryland state legislature about his application to be reinstated after a leave of absence as an employee of the Maryland Division of Corrections.⁴ When his interviewer asked for his social media account passwords, he felt like he could not say no without losing a job he needed. He turned over his Facebook password and the interviewer proceeded to log in and read through his private messages and posts.

The practice is not limited to employers asking for information from specific employees. After hearing Robert Collins' story, the ACLU of Maryland learned that the Division of Corrections had a blanket policy of requiring login and password information from *all* job applicants.⁵

An employer who demands account passwords from a job applicant or an employee intrudes deeply into the worker's privacy. Social media messages and email may include intimate conversations between romantic partners. Searching through a Google account, an employer could scrutinize an employee's web search history, learning about her political or religious affiliations. An Amazon.com account can reveal a person's shopping history, disclosing anything from her taste in movies to her medical purchases. Combing through an applicant's online accounts, an employer might be able to discern information upon which it would be unlawful to base a hiring decision, such as religious beliefs, citizenship status, pregnancy or sexual

² CareerBuilder.com, *More employers finding reasons not to hire candidates on social media, finds CareerBuilder Surver* (June 27, 2013), available at <http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=6%2F26%2F2013&id=pr766&ed=12%2F31%2F2013>.

³ Manuel Valdes, *Job seekers getting asked for Facebook passwords*, Associated Press (March 20, 2012), available at <http://finance.yahoo.com/news/job-seekers-getting-asked-facebook-080920368.html#>.

⁴ Testimony of Robert Collins before the Maryland State House Economic Matters Committee, Feb. 15, 2012, available at http://www.aclu-md.org/uploaded_files/0000/0176/collins_testimony.pdf.

⁵ ACLU of Maryland, Press Release, *ACLU says Division of Corrections revised social media policy remains coercive and violates 'friends' privacy rights* (Apr. 18, 2011), available at http://www.aclu-md.org/press_room/30.

orientation.⁶

Employers who sift through private messages on personal accounts also intrude on the privacy of the individuals who sent those messages to the applicant or employee. These third parties--who might be family members, friends, or a doctor setting up an appointment--expected their conversations to remain private. They have no ability to refuse the employer's demands for access to those conversations.

When employers condition a job on access to deeply personal information, employees and job seekers face a difficult choice: Do I defend my privacy and the privacy of those who communicate with me? Or do I keep my job?

Protecting the privacy of online accounts is a vital reform, and one that is gaining momentum. Legislatures around the country are recognizing the need for reform. Just last month, New Jersey Gov. Christie signed a bill to protect workers' online privacy.⁷ In all, ten states have passed bills protecting the online privacy of applicants and employees.⁸ And legislation has been introduced in at least thirty-six states, including New York.⁹ The NYCLU hopes that New York City joins the list of jurisdictions that have taken action to protect employee privacy.

Intro 1106 provides strong privacy protections for New York City workers. It will prohibit employers from requiring both employees and job applicants to provide access to online accounts, including social media fora like Facebook and Twitter, personal e-mail accounts, and online shopping accounts.

The bill bans actions that employers could use to circumvent the prohibition on demanding direct access. Specifically, it bars employers from requiring applicants to log into their personal accounts while an interviewer watches over the applicants' shoulder. Intro 1106 also prohibits employers from requiring employees add them as friends or change their privacy settings.

Intro 1106 defines limitations that will ensure the bill does not interfere with legitimate supervision and investigation by employers. The legislation would permit employers to seek out and use information about an employee that is publicly available, and ensures that employers

⁶ See, e.g. New York City Administrative Code § 8-107 (prohibiting discriminatory practices in hiring in New York City); New York Executive Law § 296 (prohibiting discriminatory practices in hiring in New York State); 42 U.S.C. §§ 2000e et seq. (prohibiting discriminatory practices in hiring the United States).

⁷ A2878/S1915, signed by Governor Christie August 28, 2013 (bill text available at <http://www.njleg.state.nj.us/bills/BillView.asp?BillNumber=A2878>).

⁸ Specifically, Arkansas, Colorado, Illinois, Nevada, New Jersey, New Mexico, Oregon, Utah, Vermont, and Washington. See National Conference of State Legislatures, *Employer Access to Social Media Usernames and Passwords 2013*, available at <http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx>.

⁹ See A443-A (Dinowitz)/S2434-B (Klein), available at <http://assembly.state.ny.us/leg/?bn=A00443&term=2013>.

may access accounts to investigate unlawful actions by their employees. These provisions demonstrate that employees' privacy does not need to be sacrificed to protect employers' legitimate interests.

Intro 1106 is a positive step towards ensuring all New Yorkers can engage in the kinds of private communications and activities online that are critical for personal liberty and a free, democratic society. The NYCLU urges the Council Members to approve the bill.



THE CITY OF NEW YORK
OFFICE OF THE MAYOR
NEW YORK, N.Y. 10007

WILLIAM M. HEINZEN
DEPUTY COUNSELOR TO THE MAYOR

September 25, 2013

Hon. Michael Nelson
Chair, Committee on Civil Service and Labor
New York City Council
250 Broadway
New York, NY 10007

Re: Introduction No. 1106

Dear Chairman Nelson:

Thank you for your invitation to the Department of Consumer Affairs (DCA) to comment on Introduction No. 1106, which would prohibit employers, employment agencies and labor organizations from requiring access to online social networks and other personal accounts of employees and prospective employees in connection with the hiring process.

The Department of Consumer Affairs has asked that we respectfully submit that it lacks the expertise that would be of use to the Council in its deliberations regarding this bill. Indeed, the subject matter of this bill, while proposed to be appended to the Department's chapter of the New York City Charter and Administrative Code, has no substantive connection to its mission, work and expertise.

For nearly 45 years, since its creation by the Council in 1969, DCA's mission has been to empower businesses and consumers to ensure a fair and vibrant marketplace. At its core, the Department's work is focused on protecting consumers in the commercial retail arena by licensing businesses (now more than 81,000 in 55 different industries); regulating industries which have the potential to harm consumers but which it does not license; enforcing Council's comprehensive Consumer Protection Law and other related business laws in all retail business in the City; mediating and resolving consumer complaints against businesses; and adjudicating consumer claims and violations against retail businesses. DCA's expertise lies in dealing with every aspect of the complex and multilayered transactional relationships between consumers and businesses. Beginning In 2006, with the launching of DCA's Office of Financial Empowerment, the Department developed expertise, services and programming for consumers with low incomes in the financial marketplace as well.

The Mayor's Office would also point out that, because there is no City agency with jurisdiction over employer-employee relations outside of the City's Commission on Human Rights, which has jurisdiction over allegations of discrimination with respect to employment, among other things, we believe that the subject matter is more appropriate for state legislation and enforcement. We would also caution that there may be a legitimate need for information about the online activities of employees and prospective employees of certain public safety agencies.

Thank you again for the opportunity to comment on Introductory No. 1106.

Sincerely,

A handwritten signature in blue ink, appearing to read 'William Heinzen', with a long horizontal flourish extending to the right.

William Heinzen
Deputy Counselor to the Mayor

STATEMENT OF
SECURITIES INDUSTRY AND FINANCIAL MARKETS ASSOCIATION
BEFORE THE
NEW YORK CITY COMMITTEE ON CIVIL SERVICE AND LABOR
HEARING ON
INT. NO. 1106 - IN RELATION TO ONLINE SOCIAL MEDIA AND OTHER
PERSONAL ONLINE ACCOUNTS AND EMPLOYMENT
September 25, 2013

The Securities Industry and Financial Markets Association¹ (SIFMA) respectfully requests your consideration of changes to the most recent version of legislation barring employers from requesting access to employees' social media and other personal online accounts (Int. No. 1106).

The securities industry has no interest in accessing employee accounts that are used exclusively for personal use. The problem, however, is that many people use the same account for both personal and business activity. According to a 2012 American Century Investments study, nearly nine out of ten financial services professionals have a social media profile or account. Fifty-eight percent of these professionals use social media for business at least several times per week; twenty-seven percent use it for business on a daily basis.² Business use includes, among other things, reading and posting commentary, monitoring and sharing relevant news, business promotion and brand building, sharing best practices, and obtaining customer feedback. A "personal" account that is used for business purposes must be treated as a business account.

While this legislation is well-intentioned, they conflict with the duty of broker-dealers to supervise, record, and maintain business-related communications as required by federal law, the Financial Industry Regulatory Authority ("FINRA") rules, and by state law. Section 17 and Rule 17a-4(b)(4) of the Securities Exchange Act of 1934 require that broker-dealers retain written and electronic communications related to the broker-dealer business for a minimum of three years. "Communications" has been broadly interpreted to include postings on social media sites.

FINRA is the largest independent regulator for all securities firms doing business in the United

¹ The Securities Industry and Financial Markets Association (SIFMA) brings together the shared interests of hundreds of securities firms, banks and asset managers. SIFMA's mission is to support a strong financial industry, investor opportunity, capital formation, job creation and economic growth, while building trust and confidence in the financial markets. SIFMA has offices in New York and in Washington, D.C. For more information, visit <http://www.sifma.org>.

²https://www.americancentury.com/pdf/Financial_Professionals_Social_Media_Adoption_Study.2012/pdf

States and is considered a self-regulatory organization under federal securities laws. To protect investors, FINRA requires, among other things, that securities firms supervise, record and maintain their employees' business communications – including those disseminated on social media sites. This is spelled out in several different FINRA rules and regulatory notices, including:

- Securities firms must establish procedures for the review of registered representatives' written and electronic business correspondence. (NASD Rule 3010(d))
- “Firms must adopt policies and procedures reasonably designed to ensure that their associated persons who participate in social media sites for business purposes are appropriately supervised” (FINRA Regulatory Notice 10-6)
- “The content provisions of FINRA’s communications rules apply to interactive electronic communications that the firm or its personnel send through a social media site.” (FINRA Regulatory Notice 10-6)
- A firm’s procedures “must be reasonably designed to ensure that interactive electronic communications do not violate FINRA or SEC rules, including the content requirements of NASD Rule 2210, such as the prohibition on misleading statements or claims and the requirement that communications be fair and balanced.” (Regulatory Notice 11-39)

State securities laws and regulations similarly require broker-dealers and broker-dealer agents to maintain books and records relating to the firm’s business. This can include business communications made or transmitted using social media. Denying broker-dealers access to social media accounts where business is being conducted directly conflicts with FINRA regulations and state law. The North American Securities Administration Association made these arguments in their recent letter³ to the National Council of State Legislators.

Prohibiting broker-dealers from supervising business communications on social media accounts also puts customers at risk. Without appropriate monitoring, it will be much harder for firms to detect serious problems. Such problems could include: (1) misleading claims by an employee, such as the promise of an unrealistically high rate of return on investment; (2) fraudulent activity, including insider trading and Ponzi schemes; and (3) inappropriate conduct such as the selling of investment products that are not approved by the firm.

SIFMA therefore respectfully requests that you consider a narrow exemption to these bills so that securities firms can continue to comply with state requirements and FINRA regulations. Exemption language from New York State legislation and Michigan’s social media law (Public Act No. 478)⁴ which states in Section 5(2), “This act does not prohibit or restrict an employer from complying with a duty to screen employees or applicants prior to hiring or to monitor or retain employee communications that is established under federal law or by a self regulatory organization, as defined in section 3(a) (26) of the securities and exchange act of 1934, 15 USC 78c(a)(26).” This language also works, although we would suggest replacing “federal law” with “state or federal law or

³ <http://www.nasaa.org/wp-content/uploads/2011/07/NASAA-letter-to-NCSL-Regarding-Social-Media-Privacy-Legislation-FINAL-2-14-2013.pdf>

⁴ <http://www.legislature.mi.gov/documents/2011-2012/publicact/pdf/2012-PA-0478.pdf>

regulation” to recognize state requirements in this area. Or as alternative, New Jersey’s new law ⁵ (A. 2878) which in Section 6 which reads, "Nothing in this act shall be construed to prevent an employer from complying with the requirements of state or federal statutes, rules or regulations, case law or rules of self-regulatory organizations." Also, Section 1 defines “personal account” does not include “business related” communications.

We would encourage you to amend your bills to include similar language. Thank you for your consideration of our views.

⁵ http://www.njleg.state.nj.us/2012/Bills/PL13/155_.PDF

Int. No. 1106

By Council Members Palma, Williams, Rose, Mark-Viverito, Foster, Nelson, Rivera, Koslowitz, Mendez, Rodriguez, Koppell, King, Dromm, Van Bramer, Lander, Brewer, Weprin and Halloran

A LOCAL LAW

To amend the administrative code of the city of New York, in relation to online social media and other personal online accounts and employment.

Be it enacted by the Council as follows:

§ 2. Section 2203 of the New York city charter is hereby amended by adding a new subdivision e, relettering current subdivisions e through g as subdivisions f through h, and amending relettered subdivisions f and h to read as follows:

(e) The commissioner shall have all powers as set forth in chapter 8 of title 20 of the administrative code relating to the receipt, investigation, and resolution of complaints thereunder regarding confidentiality of personal online accounts.

~~[(e)]~~ (f) The commissioner, in the performance of said functions, including those functions pursuant to subdivision e of this section, shall be authorized to hold public and private hearings, administer oaths, take testimony, serve subpoenas, receive evidence, and to receive, administer, pay over and distribute monies collected in and as a result of actions brought for violations of laws relating to deceptive or unconscionable trade practices, or of related laws, and to promulgate, amend and modify rules and regulations necessary to carry out the powers and duties of the department.

~~[(f)]~~ (g) The commissioner shall exercise the powers of a commissioner of public markets under the agriculture and markets law with respect to open air markets.

~~[(g)]~~ (h) (1) Notwithstanding any inconsistent provision of law, the department shall be authorized, upon due notice and hearing, to impose civil penalties for the violation of any laws or

rules the enforcement of which is within the jurisdiction of the department pursuant to this charter, the administrative code or any other general, special or local law. The department shall have the power to render decisions and orders and to impose civil penalties for all such violations, and to order equitable relief for and payment of monetary damages in connection with enforcement of chapter 8 of title 20 of the administrative code. Except to the extent that dollar limits are otherwise specifically provided, such civil penalties shall not exceed five hundred dollars for each violation. All proceedings authorized pursuant to this subdivision shall be conducted in accordance with rules promulgated by the commissioner. The remedies and penalties provided for in this subdivision shall be in addition to any other remedies or penalties provided for the enforcement of such provisions under any other law including, but not limited to, civil or criminal actions or proceedings.

§ 2. Title 20 of the administrative code of the city of New York is amended by adding a new chapter 8 to read as follows:

Chapter 8

Right of employees and prospective employees to confidentiality of personal online accounts.

§ 20-911 Definitions. For purposes of this chapter, the following terms shall be defined as follows:

a. “Employee” shall mean any person who is employed by any employer in return for the payment of direct or indirect monetary wages or profit, or any person who volunteers his or her services to such employer for no monetary compensation.

b. “Employment agency” shall mean any person undertaking to procure employees or opportunities to work.

c. “Employer” shall mean any person, partnership, association, corporation or non-profit entity which employs one or more persons, including agencies of the city of New York, as defined in section 1-112 of the code, and the council of the city of New York.

d. “Labor organization” shall mean any organization which exists and is constituted for the purpose, in whole or in part, of collective bargaining or of dealing with employers concerning grievances, terms and conditions of employment, or of other mutual aid or protection in connection with employment.

e. ~~“Personal Online social and networking media account” shall mean any online account that is used by an employee primarily or exclusively for personal communications internet based service that allows individuals to: construct a public or semi-public profile within a bounded system, created by such service; create a list of other users with whom such individuals share a connection within the system; and view and navigate such individuals’ list of connections and those made by others within the system the content of which may include, but is not limited to, videos, still photographs, instant messages, text messages and email, to which access is restricted by a password or other unique means of identification.~~¹

f. ~~“Other personal online account” shall mean any internet based service that allows individuals to create a personal account within a bounded system, created by such service, for purposes including, but not limited to, email, dating, employment, banking, blogging, video blogging, podcasting, making online purchases, selling items online, paying for purchases from third parties, receiving payments for online sales to third parties, tracking shipments, maintaining~~

¹ This provides a clear definition for the term “personal online account.” similar to ones used in other states. All references to “online social and networking media account” have been changed to “personal online account” throughout the bill text.

² The term “other personal online account” is no longer necessary given the definition of “personal online account” above. Additionally no other social media privacy bill or law contains such a definition.

~~records of past purchases or sales, or otherwise containing private information, to which access is restricted by a password or other unique means of identification.~~

§ 20-912 Prohibition against employers requesting or requiring access to ~~online social networking and other personal online~~ accounts. a. No employer, labor organization, employment agency or employee or agent thereof, shall request, or require an employee, or a prospective employee in connection with the interview or hiring process, to:

(1) provide a password or other ~~authentication~~³ information in order to gain access to such employee or prospective employee's ~~online social and networking media accounts or other personal online accounts;~~

(2) access such employee or prospective employee's ~~online social and networking media accounts or other~~ personal online accounts in the presence of the employer or prospective employer ~~in a manner that enables the employer or prospective employer to observe the contents of such accounts~~⁴; or

~~(3) add any person, including the employer, prospective employer or any agent of the employer, to the list of contacts associated with the employee or prospective employee's social and networking media accounts or other personal online accounts; or~~⁵

~~(4)~~ (3) alter the ~~privacy~~ settings on the employee or prospective employee's ~~social and networking media accounts or other~~ personal online accounts that would allow the employer,

³ "Other information" is very unclear and fails to provide employers with guidance about what they cannot request. The "authentication" language is important here to avoid triggering liability if an employer simply "friends" an employee on Facebook, when the employee is free not to accept.

⁴ This clarifying language focuses on the contents of the personal online accounts and has been used in other states with balanced social media privacy laws.

⁵ The language as drafted in the original Section (a)(3) would ban employers from asking job applicants for their LinkedIn job information. We suggest a narrower version of this prohibition based upon similar laws in Washington State and Oregon in a new subsection (b).

prospective employer, or employee or agent of the employer, to view the content of such accounts.

b. No employer, labor organization, employment agency or employee or agent thereof, shall, in connection with the interview or hiring process, coerce or require an employee or a prospective employee to add any person, including the employer, prospective employer or any agent of the employer, to the list of contacts associated with the employee or prospective employee's personal online accounts.⁶

cb. No employer, labor organization, employment agency or employee or agent thereof shall discharge, discipline, threaten to discharge or discipline, or otherwise retaliate against an employee or applicant solely for not complying with a request or demand by the employer that violates this section. However, this section does not prohibit an employer from terminating or otherwise taking an adverse action against an employee or applicant if otherwise permitted by law.

§ 20-913 Application of chapter. a. Nothing in this chapter shall prohibit an employer, labor organization, employment agency, or employee or agent thereof, from obtaining information about a prospective employee that is publicly available.

b. Nothing in this chapter shall affect an employer's existing rights and obligations to request that an employee provide access to ~~online social and networking media accounts or other~~ personal online accounts reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations, or as otherwise required by law, provided that access to such accounts is used solely for purposes of that investigation or a related proceeding. ~~An employer investigation, as specified in this section,~~

⁶ This change is necessary to avoid violating a First Amendment free speech violation by chilling friendly, totally non-coercive invitations to "friend" colleagues on Facebook in situations where an employee is totally free to decline the request.

includes requiring the employee's cooperation to share the content that has been reported in order to make a factual determination.⁷

c. Nothing in this chapter shall preclude an employer from requiring, or requesting an employee to disclose, a username, password, or other authentication means for accessing:

(1) ~~online social and networking media accounts or other~~ personal online accounts that were created and maintained for or on behalf of the employer; or

(2) electronic communications devices supplied or paid for by the employer.⁸

d. ~~If through the use of an electronic device or program that monitors an employer's network or the use of employer provided devices, an employer inadvertently receives an employee's password, or other authentication information, the employer is not liable for having this information, but may not use this information to access an employee's personal online accounts~~⁹~~Nothing in this chapter shall preclude an employer from lawful monitoring of employees' use of employer owned computers, networks or servers, including any use of online social and networking media accounts or other personal online accounts on such computers, networks or servers.~~

⁷ This language clarifies that the employer can review the specific content of the account, but does NOT say that the employer can actually obtain the user name and password. This would remain prohibited.

⁸ This change is helpful to avoid dis-incentivizing employers from offering "bring your own device programs" where employees can select, pay and be reimbursed for their own smart phones and other personal devices, instead of using an employer-issued device. If the device is used for work purposes and is paid for in part by the employer, it should be searchable like a work computer.

⁹ This is a narrower version of the employer monitoring exception that has been supported by the National ACLU and enacted in other states, such as Washington and Oregon.

e. Nothing in this chapter shall preclude an employer from complying with the requirements of state or federal statutes, rules or regulations, case law, or rules of self-regulatory organizations.¹⁰

§ 20-914 **Enforcement.** a. The department shall enforce the provisions of this chapter. In effectuating such enforcement, the department shall establish a system utilizing multiple means of communication to receive complaints regarding non-compliance with this chapter and investigate complaints received by the department in a timely manner.

b. Any person alleging a violation of this chapter shall have the right to file a complaint with the department within 180 days of the date such person knew or should have known of the alleged violation. The department shall maintain confidential the identity of any complainant unless disclosure of such complainant's identity is necessary for resolution of the investigation or otherwise required by law. The department shall, to the extent practicable, notify such complainant that the department will be disclosing his or her identity prior to such disclosure.

c. Any person claiming to be aggrieved by an act that violates section 912 of this chapter may make, sign and file with the department a verified complaint in writing and proceed with such complaint, or commence a civil action and proceed with such action. Upon receiving a complaint alleging a violation of this chapter, the department shall investigate such complaint. The department shall keep complainants reasonably notified regarding the status of their complaint and any resultant investigation. If the department believes that a violation has occurred, it shall issue to the offending person or entity a notice of violation. The commissioner shall prescribe the form and wording of such notices of violation. The notice of violation shall be returnable to the administrative tribunal authorized to adjudicate violations of this chapter.

¹⁰ Certain employers, such as those in the financial services industry, have legal obligations under federal law and other rules/regulations to check employees' personal online accounts. This clarifies that such employers are permitted to comply with these mandates.

d. The department may also itself make, sign and file a verified complaint alleging that an employer, labor organization, employment agency, or employee or agent thereof, has violated section 912 of this chapter and proceed with such complaint pursuant to the provisions of chapter one of this title.

~~e. In addition to the aforementioned provisions of this section, any person claiming to be aggrieved by a violation of this chapter shall have a cause of action in any court of competent jurisdiction for compensatory damages, injunctive and declaratory relief, attorney's fees and costs, and such other relief as such court deems appropriate. Submitting a complaint to the department shall be neither a prerequisite nor a bar to bringing a private action.~~

f. A person must file a complaint with the department or a court of competent jurisdiction within one year of when that person knew or should have known of an alleged violation of this chapter.

~~§ 20-915 Violations. Notwithstanding any inconsistent provision of law, if, in an action instituted pursuant to this chapter judgment is rendered in favor of complainant, the department shall have the power to impose penalties provided for in this chapter and to grant an employee, prospective employee or former employee all appropriate relief. Such relief shall include a civil penalty of not less than two hundred and fifty dollars but not more than two thousand dollars for each violation, and equitable relief, as appropriate, including, but not limited to, ordering an injunction prohibiting any acts tending to render ineffectual relief that could be ordered by the department after a hearing as provided by this chapter.~~

§ 3. This local law shall take effect one hundred and twenty days after its enactment into law.

Formatted: zzmptailerItem

LS# 3498, 3502, 3503 & 3517
MWC
6/21/13

Formatted: zmpTrailerItem

State Privacy and Security Coalition, Inc.

September 24, 2013

Council Member Annabel Palma
250 Broadway, Room 1781
New York, NY 10007

Re: NYC Council Social Media Privacy Bill

Dear Council Member Palma:

Thank you for addressing the issue of employer access to personal online accounts of employees and prospective employees. We agree that there is no valid reason for most employers in almost all sectors to request that prospective employees provide log-in credentials for personal online accounts. However, the proposed bill could create privacy concerns and could also make it difficult for people to engage in routine online speech protected by the First Amendment to the U.S. Constitution. For instance, as drafted, the measure could make it illegal to send an employee a “friend” request or follow them on Twitter. Moreover, this bill would ostensibly outlaw popular social networking sites designed for job seekers like LinkedIn.

In addition, any legislation in this area must create narrow exceptions for areas of legitimate employer interest, such as the use of work accounts or work equipment for job-related activity, allegations of illegal activity involving an employee account, or downloading confidential information from a work computer to a personal account. Likewise, social media privacy bills should not prevent employers from protecting and monitoring company networks or complying with legal requirements.

While the bill, as drafted, contains an exception for certain employer investigations in § 20-913(b), this should be broadened to allow employers to ask an employee – not a prospective employee – to share the contents of a personal online account – without obtaining the employee’s password to that account – in response to a specific allegation of work-related misconduct involving that personal online account. However, these exemptions would not cover asking the employee to divulge the employee’s log-in credentials to any such personal online account. Similar exceptions have been included in almost all state laws on this subject.

The economic impact of the failure to broaden these exceptions could be very significant. For instance, there have been federal prosecutions of foreign companies that bribe employees of U.S. companies to steal intellectual property/trade secret information. Failure to broaden exceptions for legitimate employer investigations would create a “safe zone” for employees who want to steal valuable IP assets of companies in your city and state by transferring them to the employee’s personal online account.

State Privacy and Security Coalition, Inc.

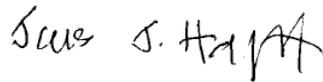
September 24, 2013
Page 2

Attached please find suggested amendments that we believe would accomplish the goals of this legislation while eliminating any unintended consequences. These amendments are in keeping with legislation passed in several other states and reflect a compromise we developed with the American Civil Liberties Union affiliates that was added to similar bills in other states.

Without these narrow and entirely reasonable exceptions; this very well intentioned bill could be used as a shield by employees to hide illegal conduct or undermine the security of company networks and devices. With them, the bill would address an important privacy issue in a thoughtful and balanced way.

For all these reasons, we respectfully urge you to amend this bill as per our attached amendments. Please feel free to contact us at the contact information below if you have any questions or would like to discuss our concerns in greater detail. Thank you for your time and consideration.

Sincerely,



James J. Halpert
General Counsel

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. 1106 Res. No. _____

in favor in opposition

Date: _____

(PLEASE PRINT)

Name: Sarah DeStefano

Address: 200 Schenmerhorn, Apt 310

I represent: _____

Address: _____

Please complete this card and return to the Sergeant-at-Arms

**THE COUNCIL
THE CITY OF NEW YORK**

Appearance Card

I intend to appear and speak on Int. No. 1106 Res. No. _____

in favor in opposition

Date: 9-25-23

(PLEASE PRINT)

Name: Nate Vogel

Address: 2201 Chestnut St. Phila, PA 19103

I represent: New York Civil Liberties Union

Address: 125 Broad St. NY NY

Please complete this card and return to the Sergeant-at-Arms