

GREGORY A. ABBOTT

Attorney-at-Law

GREGORY A. ABBOTT

P.O. Box 24453
Minneapolis, Minnesota 55424

gabbott@abbottlaw.us

(612) 217-2440

FAX (952) 400-5910

DECEMBER 13, 2009

Mitzi Rambling, Esq.
Assistant General Counsel
MINNESOTA PUBLIC RADIO
480 Cedar Street
St. Paul, MN 55101

Via fax (651-290-1243)

RE: **Lookout Services, Inc.**

<http://minnesota.publicradio.org/display/web/2009/12/11/security-breach/>

Dear Ms. Rambling:

I have been retained to represent Lookout Services, Inc., a Texas corporation, in connection with your news story about my client, which published on your website and broadcast on the radio Friday afternoon. See "<http://minnesota.publicradio.org/display/web/2009/12/11/security-breach/>". Specifically I am concerned about willful breaches of security conducted by your reporter, actions which violate a number of criminal statutes.

As you must know, Minnesota Public Radio ("MPR") knowingly and without authorization breached Lookout Services' computer network as part of its investigation. I quote from your story as posted on your website:

This week, Minnesota Public Radio was able to access state employee data on Lookout Services' Web site without using a password or encryption software. Employee names, birth dates, Social Security numbers and hire dates were visible on the Web site for every state agency using the service.

My clients inform me that hacking attempts are continuing even today, and that many of these attempts are coming from IP addresses associated with MPR.

Unauthorized breach of computer security is a serious crime under state and federal statutes. Attached to this letter are relevant excerpts from the federal and state computer crime statutes, specifically 18 U.S.C. 1030(a)(2); Minn. Stat. § 609.891, and Texas Penal Code § 33.02. MPR's actions in breaching security are straightforward violations of these criminal statutes. **A civil action for damages is created when these statutes are violated.** *See, e.g.,* 18 U.S.C. § 1030(g) and 1030(a)(5)(B)(i).

Your reporter's actions have caused and are continuing to cause substantial economic harm to Lookout Services. In the process of hacking into my client's network, your reporter looked at the data of five of Lookout Service's customers - one of which we know was the State of Minnesota. In conversations with my client, your reporter refused to disclose the identity of these four other companies whose data was reviewed. Not knowing the identity of these four other companies transforms a small security breach into a significantly more complex, time-consuming and expensive problem.

MPR has a duty to mitigate the damage caused by its reporter's security breach. There is no justification for continuing to withhold illegally obtained confidential data, given the ongoing damage to Lookout Services and its clients.

It is therefore imperative that MPR immediately disclose the identity of the other four Lookout Services customers whose confidential data was reviewed by your reporter.

Therefore, on behalf of my clients, **I demand that MPR immediately do the following:**

- 1. Identify all customers of Lookout Services whose confidential data was viewed, accessed, or downloaded by MPR employees, agents, or anyone acting on MPR's behalf;**
- 2. Cease its illegal efforts to breach the security of Lookout Services' computer network, which are continuing;**
- 3. Provide a copy to Lookout Services of any all confidential data MPR has obtained from Lookout Services' computer network (whether from its own activities or obtained from the unauthorized access of a third party - taking appropriate steps to preserve the confidentiality of any retained data); and**

Mitzi Rambling, Esq.

December 13, 2009

Page 3

4. Identify to Lookout Services the specific means or mechanism by which MPR has been able to breach Lookout Services' network security.

Compliance with these demands is necessary for Lookout Services to diagnose and remediate the current security breach, and prevent future security breaches.

Should MPR fail to respond to these demands, Lookout Services will pursue all available legal remedies including, but not limited to: filing a criminal complaint with federal and state authorities; seeking a temporary restraining order and/or injunction compelling MPR to comply with these demands; and pursuing a claim for damages arising from MPR's willful and illegal breach of Lookout Service's confidential data.

Unless MPR has confirmed it will comply with these demands by 5 p.m., Monday, December 14, 2009, in writing delivered to my office, Lookout Services has authorized me to initiate litigation against MPR and to seek a temporary restraining order and injunction compelling MPR to meet these demands.

This is a time-sensitive demand. Please take action accordingly. My e-mail address is: gabbott@abbottlaw.us My telephone number (612) 217-2440 - this number will ring both my office and mobile phones.

Sincerely,

/s

Gregory A. Abbott

c: Elaine Morley

FEDERAL AND STATE COMPUTER CRIME STATUTES:

18 U.S.C. § 1030(a)(2):

Whoever . . .

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

. . .

(C) information from any protected computer if the conduct involved an interstate or foreign communication; . . .

shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030(c) (emphasis added):

(c) The punishment for an offense under subsection (a) or (b) of this section is—

. . .

(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this sub-paragraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds \$5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this

section, or an attempt to commit an offense punishable under this subparagraph;

Minn. Stat. § 609.891 (emphasis added):

609.891 UNAUTHORIZED COMPUTER ACCESS.

Subdivision 1. **Crime. A person is guilty of unauthorized computer access if the person intentionally and without authorization attempts to or does penetrate a computer security system.**

Subd. 2. **Felony.** (a) A person who violates subdivision 1 in a manner that creates a grave risk of causing the death of a person is guilty of a felony and may be sentenced to imprisonment for not more than ten years or to payment of a fine of not more than \$20,000, or both.

(b) A person who is convicted of a second or subsequent gross misdemeanor violation of subdivision 1 is guilty of a felony and may be sentenced under paragraph (a).

Subd. 3. **Gross misdemeanor.** (a) A person who violates subdivision 1 in a manner that creates a risk to public health and safety is guilty of a gross misdemeanor and may be sentenced to imprisonment for a term of not more than one year or to payment of a fine of not more than \$3,000, or both.

(b) A person who violates subdivision 1 in a manner that compromises the security of data that are protected under section [609.52, subdivision 2](#), clause (8), or are not public data as defined in section [13.02, subdivision 8a](#), is guilty of a gross misdemeanor and may be sentenced under paragraph (a).

(c) A person who violates subdivision 1 and gains access to personal data is guilty of a gross misdemeanor and may be sentenced under paragraph (a).

(d) A person who is convicted of a second or subsequent misdemeanor violation of subdivision 1 within five years is guilty of a gross misdemeanor and may be sentenced under paragraph (a).

Subd. 4. **Misdemeanor.** A person who violates subdivision 1 is guilty of a misdemeanor and may be sentenced to imprisonment for a term of not more than 90 days or to payment of a fine of not more than \$1,000, or both.

Texas Penal Code § 33.02 (emphasis added):

Sec. 33.02. BREACH OF COMPUTER SECURITY.

(a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

(b) An offense under this section is a Class B misdemeanor unless in committing the offense the actor knowingly obtains a benefit, defrauds or harms another, or alters, damages, or deletes property, in which event the offense is:

(1) a Class A misdemeanor if the aggregate amount involved is less than \$1,500;

(2) a state jail felony if:

(A) the aggregate amount involved is \$1,500 or more but less than \$20,000; or

(B) the aggregate amount involved is less than \$1,500 and the defendant has been previously convicted two or more times of an offense under this chapter;

(3) a felony of the third degree if the aggregate amount involved is \$20,000 or more but less than \$100,000;

(4) a felony of the second degree if the aggregate amount involved is \$100,000 or more but less than \$200,000; or

(5) a felony of the first degree if the aggregate amount involved is \$200,000 or more.

(c) When benefits are obtained, a victim is defrauded or harmed, or property is altered, damaged, or deleted in violation of this section, whether or not in a single incident, the conduct may be considered as one offense and the value of the benefits obtained and of the losses incurred because of the fraud, harm, or alteration, damage, or deletion of property may be aggregated in determining the grade of the offense.

(d) A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.