

COMPUTER INVASION OF PRIVACY UNDER THE VIRGINIA COMPUTER CRIMES ACT

January 2001

By Raymond L. Hogge, Jr.
Payne, Gates, Farthing & Radd, P.C.
Attorneys and Counsellors at Law
Dominion Tower, Suite 1515
999 Waterside Drive
Norfolk, Virginia 23510-3309
(757) 640-1500
RHogge@PayneGates.com
www.VirginiaLaborLaw.com

**This article is intended solely for educational purposes,
and does not constitute or contain legal advice.**

Introduction

Common law claims for invasion of privacy are well established under the laws of some states. *See, e.g., Weeks v. Union Camp Corp.*, No. 98-2814, 2000 U.S. App. Lexis 12549 (4th Cir. 6/7/00) (unpub.) (invasion of privacy under South Carolina law). Such claims, however, have yet to be generally recognized under Virginia law. Under some circumstances, however, at least one Virginia court has recognized a “computer invasion of privacy” claim based on the Virginia Computer Crimes Act. Virginia employers need to be aware of this possible cause of action, in order to ensure that their employees do not take actions exposing the company to liability.

The Virginia Computer Crimes Act

The Virginia Computer Crimes Act, Va. Code 18.2-152.1 *et seq.*, provides criminal penalties for certain computer-related activities. One of its provision, Va. Code 18.2-152.5, prohibits “computer invasion of privacy.” *See, e.g., Plasters v. Commonwealth*, No. 1870-99-3, 2000 Va. App. Lexis 473 (Va. Ct. App. 6/27/00) (criminal conviction for computer invasion of privacy). Specifically, it provides:

A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person. "Examination" under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.

In addition to making such conduct a Class 3 misdemeanor, the Act provides for civil relief and damages:

A. Any person whose property or person is injured by reason of a violation of any provision of this article may sue therefor and recover for any damages sustained and the costs of suit. Without limiting the generality of the term, "damages" shall include loss of profits.

B. If the injury arises from the transmission of unsolicited bulk electronic mail, the injured person, other than an electronic mail service provider, may also recover attorneys' fees and costs, and may elect, in lieu of actual damages, to recover the lesser of ten dollars for each and every unsolicited bulk electronic mail message transmitted in violation of this article, or \$25,000 per day. The injured person shall not have a cause of action against the electronic mail service provider which merely transmits the unsolicited bulk electronic mail over its computer network.

C. If the injury arises from the transmission of unsolicited bulk electronic mail, an injured electronic mail service provider may also recover attorneys' fees and costs, and may elect, in lieu of actual damages, to recover the greater of ten dollars for each and every unsolicited bulk electronic mail message transmitted in violation of this article, or \$25,000 per day.

D. At the request of any party to an action brought pursuant to this section, the court may, in its discretion, conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer program and computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party.

E. The provisions of this article shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

F. A civil action under this section must be commenced before expiration of the time period prescribed in § 8.01-40.1. In actions alleging injury arising from the transmission of unsolicited bulk electronic mail, personal jurisdiction may be exercised pursuant to § 8.01-328.1.

Va. Code 18.2-152.12.

S.R. v. Inova Healthcare Services

The first reported case addressing a claim for “computer invasion of privacy” under this statute was *S.R. v. Inova Healthcare Services*, 49 Va. Cir. 119, 1999 Va. Cir. Lexis 287 (Fairfax County Cir. Ct. 6/1/99). In that case, the plaintiff was a health care professional employed at Fairfax Hospital. She sought psychiatric treatment at Alexandria Hospital, so her co-workers would not be aware of it. She claimed that certain employees of Inova disclosed the fact of her treatment, in violation of Virginia Code Section 18.2-152.5.

The court, in a case of first impression, ruled that “the cause of action for Computer Invasion of Privacy consists of the following four elements: (1) the use of a computer or computer network by the offender; (2) with the intent to examine another's records; (3) in an unauthorized context when the offender knew or should have known that he was without

authority to examine the records; and (4) the records so examined contain employment, financial, or personal information of the pleader.”

The defendants argued that the plaintiff’s motion for judgment failed to adequately allege that the defendants used a computer to access any of her personal information. The court rejected that argument, finding that the plaintiff sufficiently pleaded that the defendants used the computer system to obtain her medical information.

The defendants next argued that the claim “rested on the incorrect assumption that a hospital is without authority to view the records of its patients.” The court, however, rejected that argument as well. It explained, “the defendants misapprehend both the import of this statutory cause of action and Plaintiff’s allegations in support thereof. A plain meaning analysis of this statute reveals that its enactment was not aimed at preventing hospitals or other enterprises from accessing confidential information necessary to effectively conduct business. Rather, the statute is aimed at preventing the unauthorized examination of personal information. The amended motion for judgment amply alleges that the defendants acted without authority in accessing and examining her medical records via the [computer] system at a time when review of these records was not reasonably related to the rendering of health care services.”

Next, the defendants argued that the plaintiff had not sufficiently alleged that the defendants knew or should have known that they were without authority in undertaking the alleged wrongful examination of the plaintiff’s medical records. The court rejected this argument as well. It explained, “A violation of § 18.2-152.5(A) requires the offender to continue to view the information after he knew or should have known that he was without authority to view the information displayed. Plaintiff has alleged that while she was an in-patient at Alexandria Hospital’s psychiatric unit, Lippolt, Brendel, and others currently unknown conspired to and did learn of her whereabouts and admitting medical condition. Moreover, she alleges that the [computer] system was used to access at least some of this information and that the Defendant Hospitals (Alexandria and INOVA-Fairfax) knew or should have known that abuses in the [computer] system could occur and have occurred in the past. At this stage of the proceedings, taking all allegations and reasonable inferences therefrom in the light most favorable to the Plaintiff, the Court finds there to be sufficient allegations that Defendants knew or should have known that their examination of Plaintiff’s medical records was unauthorized.”

Finally, the defendants argued that the plaintiff’s allegations that the information allegedly examined was personal are insufficient to sustain this cause of action. Rejecting this argument, the court explained, “In her Amended Motion for Judgment, Plaintiff alleges that Defendants Dorothy Lippolt and Joyce Brendel and others currently unknown learned of the whereabouts and admitting medical condition of the Plaintiff into Alexandria Hospital. Additionally, she alleges that Defendants Dorothy Lippolt and Joyce Brendel secured and published confidential, sensitive, and privileged medical information related to Plaintiff. Section 18.2-153.5 proscribed unauthorized examination of salary, credit or any other financial or personal information relating to any other person.” At least one scholar has concluded that the information contained in medical history files is clearly within the contemplated scope of the personal information protected by § 18.2-152.5. *See* Robin K. Kutz, *Computer Crime in Virginia: A Critical Examination of the Criminal Offenses in the Virginia Computer Crimes Act*,

27 William and Mary L. Rev. 783, 826 (1986). This Court agrees and therefore holds that the information allegedly accessed by the Defendants falls squarely within the ambit of § 18.2-152.5.”

Significance for Virginia Employers

It is now clear that Virginia employers may face liability for computer invasion of privacy committed by their employees. Moreover, although *S.R. v. Inova Healthcare Services* involved medical information, the cause of action does not require that medical information be involved. To the contrary, a computer invasion of privacy claim probably can be based on “any employment, salary, credit or any other financial or personal information relating to any other person.” Va. Code 18.2-152.5. Accordingly, examination of a broad range of other types of information, such as information regarding evaluations, discipline, and payroll, conceivable could support this type of claim.

To address this concern, Virginia employers should consider adopting policies regulating access to personal information. Electronic access should be prohibited, but non-electronic access also should be governed by the same rules. To avoid confusion, it may be best to draft the policy without limitation to any particular means of access. As with all policies, it should be in writing, should be distributed to all employees, and should be consistently enforced.