[*1]

People v Klapper
2010 NY Slip Op 20150
Decided on April 28, 2010
Criminal Court Of The City Of New York, New York County
Whiten, J.
Published by New York State Law Reporting Bureau pursuant to Judiciary Law § 431.
This opinion is uncorrected and subject to revision before publication in the printed Official Reports.

Decided on April 28, 2010

Criminal Court of the City of New York, New York County

The People of the State of New York, Plaintiff,

against

Andrew Klapper, Defendant.

2009NY032282

For the People:

New York County District Attorney's Office

ADA Gregory LeDonne

One Hogan Place

New York, NY 10013

For the Defense:

Law Office of Robert E Brown, Esq.

Robert E. Brown, Esq

44 Wall Street, 12th Floor

New York, NY 10005

Marc J. Whiten, J.

In this day of wide dissemination of thoughts and messages through transmissions which are vulnerable to interception and readable by unintended parties, armed with software, spyware, viruses and cookies spreading capacity; the concept of internet privacy is a fallacy upon which no one should rely.

It is today's reality that a reasonable expectation of internet privacy is lost, upon your affirmative keystroke. Compound that reality with an employee's use of his or her employer's computer for the transmittal of non-business related messages, and the technological reality meets the legal roadway, which equals the exit of any reasonable expectation of, or right to, privacy in such communications.

In the case at bar, the defendant, Andrew Klapper, is charged with Unauthorized use of a Computer under Penal Law (PL) 156.05. By omnibus motion, the defendant moves to dismiss the charge as facially insufficient and for various other reliefs. **For the following reasons, defendant's motion to dismiss for facial insufficiency is GRANTED**.

[*2]Facial Sufficiency

In order to be facially sufficient, an information must substantially conform to the formal requirements of CPL 100.15. Additionally, the factual portion and any accompanying depositions must provide reasonable cause to believe the defendant committed the offense charged, as well as nonhearsay factual allegations of an evidentiary character which, if true, establish every element of the offense charged and defendant's commission thereof (CPL 100.15[3] and 100.40[1]; *see People v Dumas*, 68 NY2d 729 [1986]; *see also People v Alejandro*, 70 NY2d 133 [1987]).

The requirement of nonhearsay allegations has been described as a "much more

demanding standard" than a showing of reasonable cause alone (*People v Alejandro*, 70 NY2d at 138, *quoting* 1968 Report of Temp Comm on Rev of Penal Law and Crim Code, Intro Comments); however, it is nevertheless a much lower threshold than the burden of proof beyond a reasonable doubt *(People v Henderson*, 92 NY2d 677, 680 [1999]; *People v Hyde*, 302 AD2d 101, [1st Dept 2003]). Thus, "[t]he law does not require that the information contain the most precise words or phrases most clearly expressing the charge, only that the crime and the factual basis therefor be sufficiently alleged" (*People v Sylla*, 7 Misc 3d 8, 10 [2d Dept 2005]). Finally, where the factual allegations contained in an information "give an accused sufficient notice to prepare a defense and are adequately detailed to prevent a defendant from being tried twice for the same offense, they should be given a fair and not overly restrictive or technical reading" (*People v Casey*, 95 NY2d 354, 390 [2000]; *see also People v Konieczny*, 2 NY3d 569 [2004]; *People v Jacoby*, 304 NY 33, 38-40 [1952]; *People v Knapp*, 152 Misc 368, 370 [1934], *affd* 242 App Div 811; *People v Allen*, 92 NY2d 378, 385 [1998]; *People v Miles*, 64 NY2d 731, 732-733 [1984]; *People v Shea*, 68 Misc 2d 271, 272 [1971]; *People v Scott*, 2005 NY Slip Op 25179 [Crim Ct, NY County [2005]).

The factual portion of the accusatory instrument alleges, in pertinent parts, that:

[D]eponent is informed by a first individual known to the District Attorney's Office that the defendant installed software on a computer at the defendant's office that recorded the keystrokes entered by the users of said computer.

Deponent further states that deponent is further informed by a second individual known to the District Attorney's Office that said second individual was an employee at the defendant's office and was instructed by the defendant to use only the above mentioned computer. Deponent further states that deponent is further informed by said second individual that said second individual then used the above-mentioned computer for work-related purposes, including to access and use a personal e-mail account.

Deponent further states that deponent is further informed by the first individual that the software installed by the defendant on the above-mentioned computer recorded the password for the e-mail account of the second individual. Deponent further states that deponent is further informed by the first individual that said first individual observed the defendant access the second individual's e-mail account and print copies of computer data and

computer material contained within the second [*3]individual's e-mail account.

Deponent further states that deponent is further informed by the second individual that the defendant e-mailed said second individual an electronic document that contained portions of e-mails generated from said second individual's e-mail account. Deponent further states that deponent is further informed by said second individual that the defendant had no permission or authority to access said second individual's personal e-mail account or to take or use any computer data, computer material, or other electronic information stored in said second individual's personal e-mail account.

A person is guilty of unauthorized use of a computer when he or she knowingly uses, causes to be used, or accesses a computer, computer service, or computer network without authorization. PL 156.05. A computer is defined as "a device or group of devices which, by manipulation of electronic, magnetic, optical or electrochemical impulses, pursuant to a computer program, can automatically perform arithmetic, logical, storage or retrieval operations with or on computer data, and includes any connected or directly related device, equipment or facility which enables such computer to store, retrieve or communicate to or from a person, another computer or another device the results of computer operations, computer programs or computer data." PL 156.00[1]. A computer service includes "any and all services provided by or through the facilities of any computer communication system allowing the input, output, examination, or transfer, of computer data or computer programs from one computer to another. PL 156.00[4]. Under the statute, to access a computer, computer service or computer network means "to instruct, communicate with, store data in, retrieve from, or otherwise make use of any resources of a computer, physically, directly or by electronic means." PL 156.00[7].

Therefore, in sum, to support the charge the allegations must allege facts of an evidentiary nature to establish that defendant (1) knowingly used or accessed a computer or services; (2) without authorization.

At issue before this court is whether the above allegations are sufficiently plead to support the charge of unauthorized computer use. Specifically, the element of "without authorization".

Defendant contends that the accusatory instrument fails to allege facts sufficient to establish a *prima facie* case to support the charge of unauthorized use of a computer. Specifically, defendant argues that the factual allegations fail to identify with specificity the email account allegedly accessed or any other facts to support that the alleged access was unauthorized, inasmuch as the complaint fails to state whether the email account was complainant's personal-work email account or a "private personal" email account. Moreover, defendant argues the allegations are devoid of facts to support that complainant had an expectation of privacy with regard to email use at work since defendant owned the computer and complainant was defendant's employee.

The People oppose defendant's motion and contend that the factual allegations are sufficiently plead to support the charge. First, the People contend that the allegations that defendant was (1) observed by another employee installing keystroke-tracking software on a computer, (2) that he instructed complainant to use said computer, (3) that complainant did use said computer "for work-related purposes, including to access and use a personal email account", [*4]and (4) that defendant was later observed accessing said email are sufficient to support the charge, as the allegations provide defendant with the conduct and crime that he is alleged to have committed. Second, the People contend that the question of whether the defendant as an employer had the authority to access the email account is an issue of fact for trial, as the complainant's use of the computer for work-related purposes goes to the weight, not the sufficiency of the charges. This court disagrees with the People and finds that under the circumstances herein the factual allegations fail to establish the element of "without authorization", as such the accusatory instrument is jurisdictionally defective.

Penal Law 156.00[8] defines "without authorization" to mean the use or access of "a computer, computer service or computer network without the permission of the owner...where such person" (1) knew that access was without permission or (2) had actual notice that he or she did not have permission from the owner of the computer or computer service, or (3) by proof that the user knowingly circumvented a security measure installed or used by the owner of the computer or computer service. PL 156.00[8].

The allegations viewed in the light most favorable to the People (*see People v. Danielson*, 9 NY3d 342, 349 [2007]); *see also, Matter of David H.*, 69 NY2d 792, 793 [1989]), that defendant installed keystroke-tracking software and viewed email are legally

sufficient to establish that defendant knowingly used or accessed a computer. However, based on the circumstances, herein, the allegations are insufficient to establish that defendant acted without authorization.

It is not contested that defendant owned the computer, as the allegations clearly state that the keystroke tracking software was installed "on a computer at the defendant's office." The allegations further state that the complainant was "an employee at the defendant's office" and that complainant used said "computer for work-related purposes, including to access and use a personal e-mail account." However, the allegations do not allege that defendant, the computer owner, had notice of any limited access to the computer or the email account. The allegations further fail to allegation that complainant had installed a security device to prevent unauthorized access or use. Conversely, the allegations state that defendant sent an email to complainant containing documents from her email account, which supports an inference that defendant did not have notice or at minimum had a reasonable belief that his access was not prohibited or limited.

Review of the case law establishes that where a defendant, like the one herein, has some authority over the computer or computer services, to sufficiently establish the element of "without authorization" the factual allegations must clearly set forth facts to support that defendant had knowledge or actual notice that the particular access was prohibited or that defendant circumvented some security device or measure installed by the user. *(see; People v. Katakam*, 172 Misc 2d 943 [Sup Ct, NY County 1997] and *People v. Esposito*, 144 Misc 2d 919 [Sup Ct, NY County 1989]). Accordingly, contrary to the People's argument, based on the unique facts before this court, the fact that defendant as the computer owner and employer had some authority over the computer and possibly the email account is of import to the issue of sufficiency.

For example, in *People v. Katakam*, 172 Misc 2d 943 [Sup Ct, NY County 1997], the defendant a computer consultant, prior to leaving his employ, made copies of company applications and programs, which he later forwarded to himself. Defendant was charged with five counts of unlawful duplication (PL 156.30), one count of criminal possession of computer [*5]related materials (PL 156.35) and two counts of computer trespass (PL 156.10). The Supreme Court, New York County, dismissed the computer trespass charge, holding that defendant as an employee was authorized to access and use the files, as such,

even though defendant had notice that the computers and files were for business use, there was no culpability for computer trespass (PL 156.10), since there was no proof that defendant used the computers without authorization.

Similarly, in *People v. Esposito*, 144 Misc 2d 919 [Sup Ct, NY County 1989], the defendant was charged under PL 156.05 for using his employee computer access to conduct non-work related criminal history searches using the NYPD computer services. The court dismissed the charge of PL 156.05 as insufficient to support the indictment, since the allegations failed to establish that defendant had notice that his acts were prohibited or that the computer or computer service was password protected or in some other way prevented unauthorized use.

Whereas, some may view emails as tantamount to a postal letter which is afforded some level of privacy, this court finds, in general, emails are more akin to a postcard, as they are less secure and can easily be viewed by a passerby. Moreover, emails are easily intercepted, since the technology of receiving an email message from the sender, requires travel through a network, firewall, and service provider before reaching its final destination, which may have its own network, service provider and firewall. An employee who sends an email, be it personal or work related, from a work computer sends an email that will travel through an employer's central computer, which is commonly stored on the employer's server even after it is received and read. Once stored on the server, an employer can easily scan or read all stored emails or data. The same holds true once the email reaches its destination, as it travels through the internet via an internet service provider. Accordingly, this process diminishes an individual's expectation of privacy in email communications. (*See, Scott v Beth Israel Medical Ctr*, 17 Misc 3d 934 [Sup Ct, New York County 2007][Court, in a civil matter, held that an employer's "no personal use" email policy, combined with the employer's stated policy allowing for email monitoring, diminished any reasonable expectation of privacy an employee may have regarding computer services.]; *see also Smyth v. Pillsbury Co.* 914 F.Supp 97, 100-01 [ED Pa 1996][finding no expectation of privacy in email communications voluntarily made by an employee over the company email system]).

By the same accord, in enacting PL 156.05, the Legislative intent was to criminalize computer intrusions where the owner of the computer or service had sufficiently set forth protections or policies to avoid unauthorized access. (See*; People v. Angeles*, 180 Misc 2d

146, 148 [Crim Ct, NY County 1999] *citing* Mem of Attorney-General in support of L 1986, ch 514, 1986 NY Legis Ann, at 233, and *People v. Esposito*, at 923]["The Legislature. . .put computer owners on notice that in order to receive the protection of the criminal statute, they must equip their computers with some kind of protective mechanism, such as a password requirement or a lock."]). As such, Penal Law 156.05 was not intended to criminalize "mere use or access," but rather to protect against knowing intrusions. (See, *People v. Angeles*, 180 Misc 2d 146, 149 [Crim Ct, New York County 1999][Court dismissed PL 156.05 charge as facially insufficient, opining that in enacting PL 156.05 the legislature wanted to criminalize acts beyond mere use or access of a computer.]).

The allegations, herein, as in *Esposito and Katakam*, fail to allege facts establishing that defendant's access to the computer and email exceeded his authorized access as the computer owner and employer, since the allegations are devoid of facts to support that defendant had [*6]notice of any prohibition or limitation regarding access. Furthermore, the allegations also fail to state whether the complainant gave notice to the defendant or that defendant was aware of any limited access. (See, *Esposito, supra*). Although, the allegations state the defendant installed keystroke-tracking software and was seen accessing an email account, they fail to sufficiently support the claim that defendant's access was without authorization, inasmuch as (1) defendant owned the computer and (2) the email ownership is unstated. Accordingly, this court finds the allegations, herein, fail to support that defendant's access was unauthorized or that defendant was on notice that access was unauthorized.

The allegations also fail to set forth sufficient facts to establish that defendant circumvented a security device or password or that complainant had installed any security protections to prevent the defendant's authorization or access to the computer or email account. *(see; People v. Goss*, 3/15/2005 NYLJ p 17, col 2 [Dist Ct. Suffolk County 2005][Finding that although information alleged defendant typed in the user's screen name knowing he did not have permission, the allegations were insufficient to support the charge since they failed to allege that the computer was equipped with a safety device to avoid unauthorized access or use.]; *see also*, *People v. Angeles*, 180 Misc 2d 146, 149 [Crim Ct, NY County 1999][Court dismissed as insufficient the count charging PL 156.05 for failing to allege facts to support, even circumstantially, that there existed a device or coding system to prevent unauthorized use]).

Therefore, for the reasons set forth, defendant's motion to dismiss the accusatory instrument as facially insufficient is GRANTED. Given the dismissal of the accusatory instrument, defendant's remaining motions are also dismissed as moot.

This constitutes the decision and order of the court.

Dated: April 28, 2010_____

New York, New YorkMarc J. Whiten, JCC

Return to Decision List