ELECTRONIC COMMUNICATION PRIVACY

PART II – CIVIL AND CRIMINAL CAUSES OF ACTION FOR UNAUTHORIZED ACCESS TO ELECTRONIC COMMUNICATIONS

By Victoria M. Brown, Esq,
342 Grand Ave, Englewood, NJ 07631
201 567 6144

FEDERAL PROTECTIONS

1) ECPA – ELECTRONIC COMMUNICATIONS PRIVACY ACT
   a. Title I – Interceptions
   b. Title II – SCA – Stored Communications Act
   c. Title III- Pen Registers, Beepers, GPS

2) COMPUTER FRAUD AND ABUSE ACT

- **TITLE I** – OF THE "ECPA "-**INTERCEPTION**
  ELECTRONIC COMMUNICATIONS PRIVACY ACT

18 U.S.C. §2510-22 – a Subsection of Title 18, "Crimes and Criminal Procedure" amending the Federal Wiretap Act

A person is guilty of violating this statute if they
a. intentionally
b. ***intercept*** or endeavor to intercept or procure another person to intercept
c. the contents of
d. an electronic communication
e. using a device

,

- REQUIREMENT OF INTERCEPTION
- "IN TRANSMISSION"

- * it's when the communication is occurring
- Once it reaches its final destination it is in storage (e.g.. your email box in Yahoo)

"Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of the [Wiretap Act] is virtually impossible".
In re Pharmatrak, Inc 329 F3d 9 (1st Cir, 2003)

- EMAILS TRAVEL IN **PACKETS**
- Sometimes one email is broken down in to several pieces (packets) transmitted along different lines, stopping sometimes along the way, and then continuing, before being reassembled and put back together at its destination
- That is why the internet is so fast
- Issue – if a packet stops along the way, is it in "storage"? Majority of courts say no.

See U.S. v Councilman, 418 F3d 67 (Fed 1st Cir, 2005 – packets are in "storage"

- Governmental Use of Title I ECPA (Wiretap Act) for Warrantless interception
  - No warrant required if self-described "emergency"
  - Can force internet service providers, landlords and others to allow physical access to their facility

"Emergency" – danger of death, physical injury, national security interest threatened, organized crime

Public is blocked from seeing Orders issued

Thousands of records turned over each day

DAMAGES UNDER TITLE I

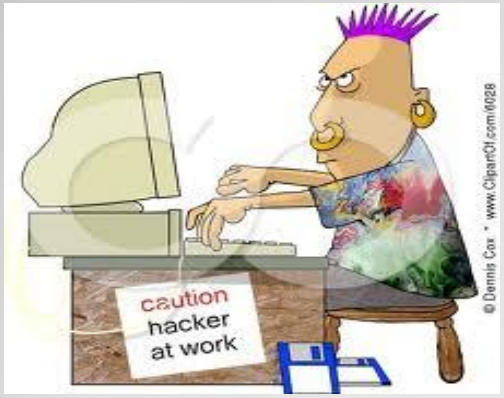
- Criminal: fine and imprisonment up to 5 years
- Civil: actual damages or profits or the greater of $100/day or $10,000, attorney's fees and possible punitive damages (18 USC §2520). Injunctive relief available.
- Only remedies are as provided in this statute except for constitutional violations

WIRETAP ACT – FOR INTERCEPTION

STORED COMMUNICATIONS ACT – TITLE II

OF THE ECPA –

18 U.S.C. §2701 et.seq.



"SCA"

A. Intentional or knowing
B. Access
C. Without Authorization
D. Or exceeds authorization
E. A facility through which an electronic communication service is provided
F. And thereby obtains, alter or prevent access to an electronic communication
G. While it is in electronic storage

Question: Are EMAILS covered by Title II?
Emails are “electronic communications”

Answer: Title II applies *only if emails are in remote electronic storage in a facility of an electronic communications service for storage purposes (see United States v Moriarty, 962 F Supp 217 (D. Mass 1997) like Yahoo or Gmail*

Not applicable if stored on your computer hard drive or a company network backup

(See *White vs. White*, 950 A2d 904, 195 NJ 517 (N.J. 2008)

“facility” whose facility? Eg.Yahoo!

"**electronic storage**" 18 USC 2510 (17)

- - temporary, intermediate storage .. Incidental to ..electronic transmission , and
- Any storage by an "electronic communication service" for the purpose of "backup"

- See *Theofel v Farey-Joney*, 359F3d 1066 (9th Cir, 2003) An email can be opened and still be in "backup". Cloud computing not back up because it has to be the backup of an "electronic communications service"

"knowing" "Intentional"

- One intends to do the act, regardless of the motive (*In re Pharmatrak*, 329 F.3d 9 (1st Cir.2003))
- One acts not upon mistake or negligence but in "bad faith" conscious of a wrong (*Theofel v Farey-Jones*, 359 F3d 1066 (9th Cir, 2003))

"unauthorized"

- Apply the common law principle of "trespass"
- Subjective and objective standard "If he ought to have known in the exercise of reasonable care" that the access was exploiting a known mistake, no authorization(see Theofel, supra)

"Exceeding authorization"

- A subscriber is authorized to access only their part of the facility of an electronic communications service – and if they check the emails of others, they have exceeded their authorized access

Facility of an Electronic Communication Service

This is not a company computer network facility, a school or library computer facility – because they are not electronic communication services. **This is also not just back up for retrieval in "cloud computing" because "not all remote comptering services are "electronic communication services". (See *Thoefel*, supra)**

DAMAGES -Title II

- Criminal: when the access is for a) commercial advantage, b) malicious destruction or criminal or tortious interference, 1st offense up to 5 years

- Civil: Actual damages, injunctive relief, attorney's fees and costs and profits but no less than $1,000, with possibility of punitive damages

SCA – Stored Communications Act

Pen Registers	• Track phone numbers • Not private – no warrant- only agency application – ex parte "relevant to an on-going criminal investigation"
Beepers	• Radio transmitter & receiver • No warrant if kept to public places • Time limits must be reasonable
GPS	• Global-Positioning-System • *U.S. v Jones*, 132 S.Ct. 935 (2012) warrant required under 4th Amendment

TITLE III of the ECPA – TRACKING 18 USC §3121

DEFENSES TO THE ECPA

STATUTE OF LIMITATIONS

GOOD FAITH

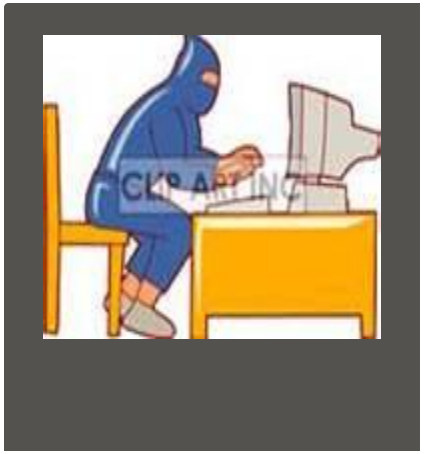
CONSENT

MISTAKE OR INADVERTANCE

CONSENT - AUTHORIZATION

- Consent may be implicit or implied but it must be actual consent rather than constructive consent (*Williams v Poulos*, 11 F3d 271 (1st Cir 1993)
- No consent "if not in line with the reasonable expectations of the party granting permission and not related to the systems intended function
- Apply common law of trespass standards
- See Theofel v Farey-Jones 359F3d1066(9th Cir 2003)
- Burden is on party asserting the defense (see In re Pharmatrak, Inc., 329 F3d9 (1st Cir, 2003)

COMPUTER FRAUD AND ABUSE ACT – "CFA"



PROTECTS HARD DRIVES ON COMPUTERS and Offline backup storage or back up storage with other than an "electronic communications service"

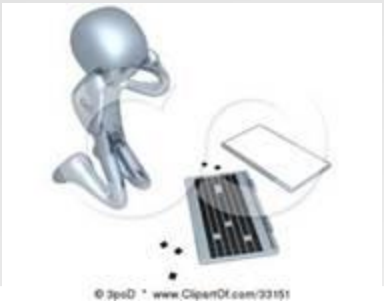
18 USC 1030a

a. "knowingly"
b. Accessed
c. A computer
d. Without authorization
e. Obtained information that is i) confidential to the government or ii) exceeds $5000 for 1yr.

Or,
iii) traffics in passwords or iv) causes damage to a protected computer

COMPUTER HARD DRIVE INVASION

- Under the CFA, there is no requirement as under ECPA Title I & II for the access to be via the internet
- The invasion is to the hard drive of a computer or storage facility of a company



If seeking DAMAGES

- Damage must be $5,000 or more in any one year
- Damages is defined ((e)(8) as “any impairment to the integrity or availability of data, a program, a system or information” and “loss” in (e)(11) as “any reasonable cost to any victim, including cost of responding, restoring, lost revenue and consequential damages due to interruption

FEDERAL PREEMPTION OVER STATE

–

Regarding the ECPA (and one will infer the CFA as well), “it is apparent to this Court ‘that Congress left no room for supplementary state regulation” *Bunnell v Motion Picture Ass’n of America*, 567 F. Supp2d 1148 (C.D. Cal, 2007)

NEW JERSEY STATE STATUTES

NJ Wiretap and Surveillance Act – NJSA 2A:156A 1-34
Equivalent to Title I of the ECPA – re: interception of an electronic communication while in transmission
NJ requires a warrant – strict interpretation

Unlawful access to Stored Communications (NJ "SCA") – NJSA 2A:156A-27
Equivalent to Title II of the ECPA –re: accessing electronic communications through an electronic communications service or exceeds authorization to access that facility and obtains an electronic communication while that communication is in electronic storage

Pen Registers, Tracking and Tracing – NJSA 24:2-2 (beepers)

New Jersey Computer Fraud & Abuse Act – NJSA 2A:38A-1 – need actual damages but no threshold of $5000 in any one year, compensatory and punitive damages caused to business for invasion of hard drive

New Jersey privacy rights of action under the common law

Four categories:

1. Intrusion upon seclusion – 2 yr. SOL
2. Public disclosure of private facts - 1 yr. SOL
3. Placing the Plaintiff in a false light – 1 yr SOL
4. Appropriation of Plaintiff's name or likeness for commercial benefit – 6 yr SOL

CASE STUDIES – APPLICATION OF PRINCIPLES IN THESE STATUTES

Home – *White vs White* – 344 NJ Super 211, 781 A.2d 85 (NJ Super Ch 2001)

BUSINESS –

Title I – *In re Pharmatrak, Inc* 329 F3d 9 (1st Cir 2003)

Title II - *Stengart v. Loving Care Agency*, 201 NJ 300 (2010)

Beepers- text messages – *Quon* case, 130 S. Ct. 2619 (2010)