

TABLE OF CONTENTS

TABLE OF AUTHORITIES	v
----------------------	---

INDEX OF APPENDICES	xiii
---------------------	------

STATEMENT OF THE CASE	1
Nature of the Proceeding	1
Jurisdiction	1
Nature of the Judgment	2
Notice of Appeal	2
Questions Presented on Appeal	2
Summary of Argument	3
Statement of Facts	3

ASSIGNMENT OF ERROR NO. 1	12
---------------------------	----

The trial court erred when it denied defendant's Motions to Suppress as follows: The Court having heard the sworn testimony and duly considered the arguments of counsel, FINDS that: 1. The affidavit for the search warrant establishes probable cause and is not overbroad. 2. The police did not violate Oregon Revised Statute 133.575 3. Any omissions or inaccuracies in the search warrant affidavit are not material and there is no substantial basis to question the good faith, accuracy or truthfulness of the affiant. 12

ARGUMENT 12

I. Supplementary Motion to Suppress (Motion to Controvert)	12
A. Standard of Review	12
B. Findings and Conclusions	13
C. Inaccuracies and Untruths in Affidavit	13
D. Material Omissions from Affidavit	16
E. Trial Court's Decision	19
1. Requisite Analysis	19
2. Materiality	23
II. Motion to Suppress	25
A. Probable Cause in General	25
B. Overbreadth of Warrant	28
C. Article 1, §8 and First Amendment Implications.	33
D. Violation of ORS 133.575	34
E. Suppression Required	37

ASSIGNMENT OF ERROR NO. 2	37
---------------------------	----

The trial court erred when, during the hearing on defendant's Demurrer, it denied the defendant the opportunity to offer evidence as follows: MR. SUSSMAN: At this point I'd like to call Norman Kirth. MR. TINTERA: Your Honor, I'm going to object to taking any testimony. It's my understanding that a demurrer is purely a legal issue. It does not require the production of any facts * * * THE COURT: Sustain the objection. . 38

ARGUMENT 38

ASSIGNMENT OF ERROR NO. 3 39

The trial court erred when it denied defendant's Demurrer as follows: * * *

[T]his is not a first amendment issue . . . * * * In this particular case the two key words [in the statute] are alter and access. Access is defined in the statute, alter is not. Access, being defined by the statute has a very specific legal meaning. This meaning may be quite different from the average understanding of the word. In this particular case it's (sic) definition is directed specifically toward issues around computers and computer systems. Alter is not statutorily defined and therefore carries its usual and customary meaning. This meaning is different from the statutory definition of access. When read as a whole, this statute is sufficiently clear for any particular individual to determine if their behavior constitutes a crime. * * * This particular statutes (sic) describes at least two different ways of committing a crime. One is to access a computer system for the purpose of doing some other bad act. Another way is to knowingly alter or damage a computer system when the individual knew he had no authorization to take such action. * * * 40

I. VAGUENESS 40

A. Alter and Access 40

B. Authorization 44

II. DEFINITENESS AND CERTAINTY 48

ASSIGNMENT OF ERROR NO. 4 50

The trial court erred when it denied defendant's Motion for Judgment of Acquittal as follows: * * * The jury could find this is a high-tech version of taking a TV set and putting it in a dumpster with the idea of coming back later that night and taking it out. I know that's sort of a simple comparison, but factually, it's very close to what Mr. Tintera has attempted to prove here. 7/19/95 Tr. 51 ll. 16-21. * * * * I do believe the evidence that has been produced here on all three counts is sufficient for the case to go forward and I'm denying the motion on all three counts 50

ARGUMENT 50

ASSIGNMENT OF ERROR NO. 5 52

The trial court erred when it ordered restitution as follows: There are special damages that could be recovered and I am going to order that restitution to Intel for those expenses, after deduction of the amounts that we've talked about for Mr. Stites, they now total \$59,692 will be recovered and they are the amounts of restitution. * * * *

* * * Those amounts leave \$8,779.45 for the expense of the Miller, Nash firm in advising Intel in this rather complex matter and the total of those two amounts, the direct expenses incurred by Intel plus the outside counsel expense total \$68,471.45, if my math is correct.

And I find that those are pecuniary losses suffered by Intel as a result

of the actions of the defendant. His actions directly caused that expenditure of money and that is a pecuniary loss that may be recovered by them and I find that that amount actually has been incurred as damages by the Intel Corporation. 53

ARGUMENT 53

I. Attorneys Fees 54

II. Non-Recoverable Salaries and Expenses 55

III. Employee Benefits 56

IV. Failure to Meet Burden of Proof 57

ASSIGNMENT OF ERROR NO. 6 58

The trial court erred by denying the defense Motion to merge Counts 2 and 3 as follows: With regard to Counts 2 and 3, there is the issue of merger. I'm of the opinion different. One alleges and incident November 1st, 1993, and the other October 25th, 1993, so we have different acts, a little over a week apart, and they are separate crimes and although they do allege violations of the same statute, 164.377, Subsection 4, they are separate incidents and separate crimes and I'm going to sentence separately 58

ARGUMENT 58

CONCLUSION 60

CERTIFICATE OF SERVICE 60

APPENDICES 61

TABLE OF AUTHORITIES

Cases

<i>1000 Friends of Oregon v. Wasco Co.</i> ,	399 Or 344, 703 P2d 207 (1985)	40
<i>Andresen v. Maryland</i> ,	427 US 463, 480 (1976)	33
<i>Barber v. Gladden</i> ,	327 F2d 101 (9th Cir.),	<i>cert den</i> 377 US 971 (1964) 49
<i>Connally v. Georgia</i> ,	429 US 245 (1977)	36
<i>Galley v. Babb</i> ,	50 Or App 617, 624 P2d 616,	rev. den. 291 Or 117 (1981) 46, 50
<i>Giaccio v. Pennsylvania</i> ,	382 US 399 (1966)	46
<i>Grayned v. City of Rockford</i> ,	408 US 104 (1972)	46
<i>Johnson v. United States</i> ,	333 US 10, 68 SCt 367, 92 LEd2d 153 (1948)	36
<i>Lo-Ji Sales, Inc. v. New York</i> ,	442 US 319, 326 n.5 (1970)	33
<i>Payton v. New York</i> ,	445 US 573, 100 SCt 1371,	63 LEd2d 639 (1980) 26
<i>Portland General Elec. Co. v. Bureau of Labor and Industries</i> ,	317 Or 606, 610-11, 859 P2d 1143 (1993)	43
<i>Raymond v. Feldmann</i> ,	124 OrApp 543, 548-49, 863 P2d 1269 (1993)	54, 55
<i>Samuel v. Frohnmayer</i> ,	95 OrApp 561, 770 P2d 914,	rev'd on other grounds, 308 Or 362, 779 P2d 1028 (1989) 54
<i>Sizemore v. Swift</i> ,	79 OrApp 352, 358, 719 P2d 500 (1986)	54
<i>Stanford v. Texas</i> ,	379 US 476, 485 (1965)	34
<i>State ex rel Juv. Dept. v. Rogers</i> ,	314 Or 114, 836 P2d 127 (1992)	37
<i>State v. Anspach</i> ,	298 Or 375, 692 P2d 602 (1984)	23, 25, 28, 32
<i>State v. Atkinson</i> ,	98 OrApp 48, 777 P2d 1010 (1989)	59
<i>State v. Barkley</i> ,	315 Or 420, 435, 846 P2d 390 (1993)	57
<i>State v. Bates</i> ,	304 Or 519, 527-28, 747 P2d 991 (1987)	13
<i>State v. Blackburn/Barber</i> ,	266 Or 28, 34, 511 P2d 381 (1973)	29, 31, 33
<i>State v. Blair</i> ,	287 Or 519, 524, 601 P2d 766 (1979)	43
<i>State v. Buffington</i> ,	87 OrApp 559 743 P2d 738 (1987)	28
<i>State v. Bullock</i> ,	135 OrApp 303, 899 P2d 709 (1995)	55, 56
<i>State v. Carillo</i> ,	125 OrApp 52, 56, 865 P2d 379 (1993)	56
<i>State v. Carlile</i> ,	290 or 161, 165, 619 P2d 1280 (1980)	25
<i>State v. Carter</i> ,	316 Or 6, 13, 848 P2d 599 (1993)	21, 23-26, 32
<i>State v. Cooper</i> ,	78 OrApp 237, 239-40, 715 P2d 504 (1986)	48, 49
<i>State v. Corpus-Ruiz</i> ,	127 Or App 66, 874 P2d 90 (1994)	27
<i>State v. Crotsley</i> ,	308 Or 272, 278, 779 P2d 600 (1989)	59
<i>State v. Davis</i> ,	295 Or 227, 666 P2d 802 (1983)	37
<i>State v. Dillon</i> ,	292 Or 172, 181, 637 P2d 602 (1981)	53, 55
<i>State v. Dimeo</i> ,	304 Or 469, 478 n. 4, 747 P2d 353 (1987)	13
<i>State v. Evans</i> ,	119 Or App 44, 47, 849 P2d 539 (1993)	26, 27
<i>State v. Gates</i> ,	31 OrApp 353, 356, 570 P2d 670 (1977)	38
<i>State v. Gloster</i> ,	145 OrApp 555, 558, 932 P2d 68 (1997)	24
<i>State v. Goodman</i> ,	152 Or App 83, ___ P2d ___ (1998)	26
<i>State v. Graves</i> ,	299 Or 189, 700 P2d 244 (1985)	39, 41, 46
<i>State v. Green</i> ,	245 Or 319, 422 P2d 272 (1966)	48
<i>State v. Harp</i> ,	299 Or 1, 697 P2d 548 (1985)	19, 21

<i>State v. Hart,</i>	299 Or 128, 139, 699 P2d 1113 (1985)	53
<i>State v. Heath,</i>	75 OrApp 425, 706 P2d 598 (1985)	57
<i>State v. Heneghan,</i>	108 OrApp 637, 816 P2d 1175 (1991) rev. den	59
<i>State v. Henry,</i>	302 Or 510, 516, 732 P2d 9 (1987)	33
<i>State v. Hodges,</i>	254 Or 21, 27, 457 P2d 491 (1969)	40
<i>State v. Ingram,</i>	313 Or 139, 145, 831 P2d 674 (1992)	29-31, 33, 37
<i>State v. Jim/White,</i>	13 OrApp 201, 508 P2d 462 (1973)	49
<i>State v. Jones,</i>	103 Or App 316, 797 P2d 385 (1990)	33
<i>State v. Keeney,</i>	323 Or 309, 918 P2d 419 (1996)	20
<i>State v. Kincaid,</i>	78 OrApp 23, 714 P2d 624 (1986)	49
<i>State v. Kurtz,</i>	46 OrApp 617, 624, 612 P2d 749 (1980)	38
<i>State v. Lefthandbull,</i>	306 Or 330, 758 P2d 343 (1988)	53, 57
<i>State v. Lindsly,</i>	106 OrApp 459, 808 P2d 727 (1991)	55
<i>State v. Lyons,</i>	124 OrApp 598, 863 P2d 1303, 1312 (1993)	58
<i>State v. Mahoney,</i>	115 OrApp 440, 838 P2d 100 (1992)	54, 55
<i>State v. Matsen/Wilson,</i>	287 Or 581, 601 P2d 784 (1979)	26
<i>State v. Maxfield,</i>	133 Or App 371, 891 P2d 1342 (1995)	23
<i>State v. Miller,</i>	116 Or App 174, 179 (1992), (1993)	20, 22 aff'd as modified 119 Or App 102
<i>State v. Modrell-Lydall,</i>	128 Or App 372, 876 P2d 315 (1994)	20
<i>State v. Moeller,</i>	105 OrApp 434, 806 P2d 130 (1991) 815 P2d 701 (1991)	38, 40, 50 rev. dismissed, 312 Or. 76,
<i>State v. Nunn,</i>	110 OrApp 96, 821 P2d 431 (1991)	rev. den. 313 Or 211 (1992) 59
<i>State v. O'Brien,</i>	96 OrApp 498, 774 P2d 1109, (1989)	54 rev. den. 308 Or 466, 781 P2d 1214
<i>State v. Olson,</i>	287 Or 157, 598 P2d 670 (1979)	26
<i>State v. Peller,</i>	287 Or 255, 598 P2d 684 (1979)	26
<i>State v. Ray,</i>	302 Or 595, 733 P2d 28 (1987)	43
<i>State v. Reed,</i>	116 OrApp 58, 840 P2d 723 (1992)	38
<i>State v. Reid,</i>	319 Or 65, 872 P2d 416 (1994)	29, 30
<i>State v. Ritter,</i>	71 OrApp 282, 288, 692 P2d 158 (1984)	13
<i>State v. Robertson,</i>	293 Or 402, 408, 649 P2d 569 (1982)	50
<i>State v. Rodriguez,</i>	317 Or 27, 854 P2d 399 (1993)	37
<i>State v. Sanders,</i>	280 Or 685, 572 P2d 1307 (1977)	49
<i>State v. Sanderson,</i>	33 OrApp 173, 575 P2d 1027 (1977)	42
<i>State v. Spencer,</i>	289 Or 225, 611 P2d 1147 (1980)	43
<i>State v. Stockton,</i>	120 Or App 111, 852 P2d 227 (1993)	27
<i>State v. Sumerlin,</i>	139 OrApp 579, 584, 913 P2d 340 (1996)	59
<i>State v. Tidyman,</i>	54 OrApp 640, 643-44, 635 P2d 1355 (1981), 644 P2d 1131 (1982)	24, 42 rev den 292 Or 722,
<i>State v. Valentine,</i>	264 Or 54, 504 P2d 84 (1972)	36
<i>State v. Waldo,</i>	93 OrApp 613, 763 P2d 417 (1988)	38
<i>State v. Wallock/Hara,</i>	110 OrApp 109, 821 P2d 435 (1991), (1992)	59 rev. den. 313 Or 75
<i>State v. Wise,</i>	305 Or 78, 749 P2d 1179 (1988)	13
<i>State v. Yancey,</i>	32 OrApp 477, 574 P2d 358 (1977)	49
<i>State v. Zuniga-Ocegueada,</i>	111 OrApp 54, 824 P2d 427	rev. den. 313 Or 211 (1992)59

<i>Union Pacific R. Co. v. Bean</i> ,	167 Or 534, 119 P2d 575 (1942)	41
<i>United States v. Perez</i> ,	67 F3d 1371 (9th Cir 1995)	28
<i>Voss v. Bergsgaard</i> ,	774 F2d 402, 405 (10th Cir. 1985)	34
<i>Wong Sun v. United States</i> ,	371 US 471 (1963)	37

Constitutional Provisions

Oregon Constitution, Article I §9	29, 37
Oregon Constitution, Article 1 §833,	34
Oregon Constitution, Article I § 20	48
Oregon Constitution, Article I, §11	48
United States Constitution, Fourth Amendment	29, 36, 37
United States Constitution, First Amendment	33, 34
United States Constitution, Fourteenth Amendment	49

Statutes

ORS 131.505	59
ORS 133.015	48
ORS 133.535	32, 33
ORS 133.565	29, 30
ORS 133.683	37
ORS 133.693	12, 20, 22
ORS 135.630	38, 48
ORS 136.445	52
ORS 137.103	53, 54, 56, 57
ORS 137.106	53
ORS 138.040	1
ORS 138.222	1
ORS 161.025	40
ORS 161.062	59
ORS 161.067	58, 59
ORS 161.565	53
ORS 164.015	51
ORS 164.377	1, 12, 14, 24, 40, 41, 43, 44, 49, 51, 52, 60
ORS 174.010	40
ORS 133.575	12, 34, 36

Rules

OAR Chapter 253, Division 4, Appendix 4	38
---	----

Other

Black's Law Dictionary, 5th Edition 41, 44
The Merriam-Webster Dictionary 41

INDEX OF APPENDICES

Affidavit for Search Warrant, 11/3/93 App 1-5

Opinion Letter, 8/1/94 App 6-7

Findings and Order from Omnibus Hearing, 6/22/95 App 8

Excerpt from Transcript 7/19/95, pp. 52, l. 13 - 53, l. 24,
Court Colloquy App 9-10

Excerpt from Transcript 7/18/95, 7/18/95, pp. 99, l. 10 - 100, l. 22,
Herb Mayer Cross Examination App 11-12

Excerpt from Transcript 7/1/94, pp. 13, l. 21 - 15, l. 13,
Court Colloquy App 13-15

STATEMENT OF THE CASE**Nature of the Proceeding**

This is a criminal appeal in which the defendant seeks reversal of his conviction for three counts of computer crime. The defendant was charged by indictment.

The indictment is set forth as follows:

INDICTMENT - Secret**ORS 164.377 - Counts 1 thru 3**

The above named defendant(s) is/are accused by the Grand Jury of Washington County by this indictment of the crime(s) of computer crime (Class C Felony) in counts 1, 2 and 3 committed as follows:

That the above named defendant(s) on and between November 1, 1992, and November 1, 1993, in Washington County, Oregon, did unlawfully, knowingly and without authorization alter a computer and computer network consisting of Intel computers Mink and Brillig,

Count 2

That the above named defendant(s), on and between August 1, 1993, and November 1, 1993, in Washington County, Oregon, did unlawfully and knowingly access and use a computer and computer network for the purpose of committing theft of the Intel SSD's password file,

Count 3

That the above named defendant(s), on and between October 21, 1993, and October 25, 1993, in Washington County, Oregon, did unlawfully and knowingly access and use a computer and computer system for the purpose of committing theft of the Intel SSD individual user's passwords, contrary to the statutes in such cases made and provided and against the peace and dignity of the State of Oregon.

Dated: March 2, 1994.

Jurisdiction

Jurisdiction of the Court of Appeals is invoked pursuant to ORS 138.040 and ORS 138.222(4)(a) & (7).

///

Nature of the Judgment

The defendant was convicted by a jury on all three Counts and sentenced to 5 years probation on Count 1 (reduced to a misdemeanor) with special conditions including restitution, 18 months probation on each Counts 2 and 3 (felonies) with special conditions including restitution, all sentences to run concurrently. None of the counts was merged with any other count for the purpose of the imposition of sentence.

Notice of Appeal

Notice of Appeal was timely filed on February 1, 1996.

Questions Presented on Appeal

Was there probable cause to support the search of defendant's home?

May police officers executing a search warrant invite non-law enforcement personnel along at their discretion?

Is the computer crime statute unconstitutionally vague either on its face or as applied?

Does the copying of a password file from one Intel computer to another Intel computer, using Intel's network, and the execution of a password-guessing program on the password file also using an Intel computer, constitute theft of that password file?

Does the copying of a password file from one Intel computer to another Intel computer, using Intel's network, and the execution of a password-guessing program on the password file also using an Intel computer, constitute a separate theft of the individual user's passwords?

Did the trial court err by refusing to merge Counts 2 and 3 for sentencing purposes?

Did the trial court err by ordering restitution when the state failed to prove that defendant's activities were the actual cause of the restitution amounts claimed or that the amounts claimed as restitution were actually incurred or easily measurable? Could restitution be imposed for those amounts claimed which were not recoverable as pecuniary damages?

Summary of Argument

The warrant which authorized the search of defendant's home was based on an affidavit which was speculative in its entirety and rife with inaccuracy. Shorn of inaccuracy, the

affidavit was lacking in facts from which it could be inferred that any of the legitimate objects of search and seizure would probably be discovered in the places sought to be searched. Moreover, the warrant directed the seizures of items which seizures were not even justified by the speculation.

The statutory basis for the charges against defendant is unconstitutionally vague in that the terms "alter" and "authorization" are not defined and the term "alter" is not distinguished from the term "access." The statute criminalizes socially tolerable, and even completely innocuous, conduct. Finally, the statute lends itself to ex post facto application.

Neither copying a password file from one Intel computer to another Intel computer, using Intel's network, nor running a password guessing program on any password or all the passwords (also using Intel's computer), constituted theft. Nothing was taken from its original place. There was no evidence of intent to deprive the owner or rightful possessor of any value inherent in the password file or in the individual passwords.

The state did not offer adequate evidence that defendant's activities were the actual cause of the restitution amounts claimed by Intel or that the amounts claimed as restitution by Intel were actually incurred or easily measurable. Restitution could not be imposed for those amounts claimed which were not recoverable as pecuniary damages.

Statement of Facts¹

On October 28, 1993, an Intel system administrator² named Mark Morrissey discovered a password-cracking program running on one of the Intel computers administered by him.

App 1; 6/14/95 Tr. 178. He also found a file called "password.ssd"³ in the computer where

¹Many of the facts set out here are taken from the affidavit underlying the search warrant for Schwartz's home, which was executed on 11/1/93. See App-1 - App-5.

²A system administrator is a kind of computer programmer with special skills. It is his or her job at Intel to administer Intel's employees' (and contractors) access to Intel's information. 6/13/95 Tr. 77. Systems administrators keep the "systems" working. See 7/14/95 Tr. 205 l. 11 to Tr. 207 l. 16.

³"SSD" is the name given to the supercomputer division at Intel. App 1. Morrissey also found a file called "psswd.ora," which turned out to be the password file from Schwartz's book publisher's site.

the password-cracking program was stored. The file name indicated to him that the file contained a password file from the Intel Supercomputer Division. App 1; 7/14/95 Tr. 169. It was, in fact, **a copy** of the SSD password file. 7/14/95 Tr. 86 ll. 14-18.

Passwords are groups of computer characters, usually letters, digits and printable punctuation which, when used in conjunction with the applicable "username,"⁴ permit access to the information stored on a computer or group of computers. 7/13/95 Tr. 178, 181. They are "encrypted (7/13/95 Tr. 179)," using a mathematical formula known as an "algorithm," and kept in a file on the computer. Anyone with access to the computer can see the password file. 7/18/95 Tr. 95 ll. 19-24. To gain access to the computer and its files, a user must "login" with a username and the unencrypted counterpart to that specific user's password. 7/18/95 Tr. 7 ll.11-13. The computer, using the "algorithm," encrypts the password which is offered, and then compares it to the password listed for that user in the password file. If it matches, the user is given access to the computer and/or the system.

The password cracking program is freely available on the internet, 6/14/95 Tr. 188, and is used by system administrators to insure the effectiveness of password files. 7/13/95 Tr. 127; 7/14/95 Tr. 91; 212 ll. 17-19; 7/19/95 Tr. 63 ll. 5-18. It uses the algorithm to encrypt words and their derivations from a dictionary or dictionaries available to it. 6/14/95 Tr. 188; 7/14/95 Tr. 178. Then it compares the encrypted word to the encrypted passwords in the password file. 7/13/95 Tr. 179; 7/20/95 Tr. 140; Tr. 142 ll. 10-16. If it comes up with a match, the password is "cracked" and the system administrator notifies the user to change his or her password. 7/13/95 Tr. 105. Intruders,⁵ if they are able to gain access to the system,⁶ may also use such a program to "crack" one or more passwords and then use the cracked password(s) to gain access to the information to which that user has access. 7/13/95

⁴The name taken by an individual user. Schwartz's username at Intel was "Merlyn." 7/18/95 Tr. 11 l. 10.

⁵Outside intruders are known variously as "hackers" or, more contemporarily, as "crackers," which is a shorthand way of saying "criminal hackers." 7/21/95 Tr. 75 ll. 8-13; Tr. 134 l. 1.

⁶Intruder access is possible over the internet. 7/18/95 Tr. 17-19. Elaborate measures are taken to prevent such access, and it is one of the focal points of the statutory scheme prohibiting "computer crime."

Tr. 137.

Network security is a major concern for companies such as Intel (7/14/95 Tr. 98), because the engineers and scientists work on the network, and their work is considered a company secret. 7/13/95 Tr. 102-103. It is part of the job of a systems administrator to see to it that the systems which he/she administers are secure against such intrusions. 7/13/95 Tr. 102 ll. 15-22.

Morrissey knew that only a limited number of people at Intel are allowed to run password cracking programs on password files, and he knew that access to SSD files is limited, due to the fact that they contain data on state-of-the-art computer products which are very valuable and at least some of which are under export restrictions by the U.S. government. Morrissey suspected a violation of Intel security policy, and he notified Intel Security of his findings. App 1; 7/14/95 Tr. 169.

The password cracking program was running⁷ under the username and password assigned to Randal Schwartz⁸ (6/14/95 Tr. 187; 7/14/95 Tr. 168), who was an independent contractor at Intel with system administrator duties involving the operation of Intel's email systems. 7/13/95 Tr. 106-107; 7/21/95 Tr. 151 ll. 3-6.

After discussing the matter with Rich Cower, an Intel Network Security Specialist (9/9/94 Tr. 98 l. 17; 6/14/95 Tr. 192), Morrissey talked to John Kent, a systems administrator for the SSD Division, who said that Schwartz was not permitted to "conduct this activity," and that under SSD policy such "activity" is a firing offense. App 1. Morrissey told Kent that he had noticed a record of several instances of Schwartz connecting with a computer called "Brillig" in the SSD cluster (7/13/95 Tr. 179; 7/14/95 Tr. 36-37), and Kent expressed surprise (7/14/95 Tr. 170), as he thought that all of Schwartz's

⁷When a program is dormant on a disk, it is just a program. When it is actually running, or "executing," it is called a "process." 7/14/95 Tr. 176.

⁸UNIX systems are multi-user systems, and the system administrator can enter a command that tells him which user or users are running which process or processes. 7/14/95 Tr. 177. UNIX is an operating system, like DOS or WINDOWS, but much more complex. 7/13/95 Tr. 94-95.

"accounts"⁹ on SSD machines had been removed when his SSD contract expired the previous spring. This turned out not to have been accurate. 7/13/95 Tr. 181, 186; 7/14/95 Tr. 36-37. It also turned out that Kent was not the system administrator responsible for Brillig. 7/14/95 Tr. 106.

Morrissey advised Kent to look for a file called "gate" on "Brillig," because he was aware that Schwartz had used such a program in the past to gain access to Intel systems over the internet when he was off site. Kent did find such a program on "Brillig." 7/14/95 Tr. 75 (See Count 1). Morrissey rechecked files "owned" by Schwartz, who was a system administrator in his own right (7/13/95 Tr. 94 ll. 12-22; 7/14/95 Tr. 165 ll. 6-8), and discovered that many passwords for SSD employees had been "compromised."¹⁰ App 2; 6/13/95 Tr. 148. ///

He talked to Wilcox and Kirkwood,¹¹ who confirmed that running the crack program on the SSD password file was beyond the scope of Schwartz's contracts and done without permission. App 2.

Kent told Morrissey that the "compromised" passwords included those of Ed Masi, a VP of Intel Corporation, the President of the SSD Division and one of the supercomputer architects for SSD. App 2. Masi's password was "PRE\$IDEN."¹² 7/14/95 Tr. 14-15. Kent said that sensitive information was "likely" kept in files accessible under some of these passwords. App 2. Morrissey arranged to maintain the backup tapes for the computers he was administering so that "daily snapshots" of Schwartz's activities would be available.

⁹One who has an active password in the password file of a computer with a UNIX operating system and a home directory is said to have "an account" on that system. 7/13/95 Tr. 178; 7/18/95 Tr. 7 ll. 5-9.

¹⁰By "compromised," the affiant on the search warrant thought that only the "user" could look at his own password. 6/13/95 Tr. 148. In actuality, anyone with access to a machine can see the whole password file. 7/21/95 Tr. 151 ll. 18-20.

¹¹Wilcox and Kirkwood were the Intel employees to whom Schwartz was responsible under his contracts. 7/13/95 Tr. 93-94; Morrissey had been hired, originally, to assume some of Schwartz's system administrator duties. 7/13/95 Tr. 106.

¹²A password should not be a dictionary word or the easy derivative of a dictionary word (7/14/95 Tr. 14), because the password cracking program tries such words first. 7/13/95 Tr. 105.

7/13/95 Tr. 68; 7/14/95 Tr. 180. The examination of those backup tapes revealed **no trace** of any SSD passwords, files from SSD or data from any individual's SSD files. 7/14/95 Tr. 216 l. 20 to 217 l. 14.

Intel staff met on Friday, 11/29/93, to discuss the situation, and because Schwartz was out of town it was decided to do nothing until Monday. 6/13/95 Tr. 80-81; 7/14/95 Tr. 136. When a suggestion was made that it might be advantageous to simply ask Schwartz what was going on when he returned, the idea was vetoed by someone in authority who said that the decision to seek to prosecute Schwartz had already been made. 7/14/95 Tr. 225-226; 7/18/95 Tr. 148.

On the morning of Monday, 11/1/93, Cower, Morrissey, Kent, Intel security specialist Clyde Stites, in-house counsel Richard Pierce and paralegal Janice Baldwin met with Detectives Lilley and Lazenby of the Washington County Sheriff's office and DDA Thomas Tintera.

9/20/94 Tr. 77-78. An affidavit in support of a warrant to search Schwartz's home was prepared. Omnibus Hearing Exh. 2; App 1-5.

That affidavit stated, among other things, that Morrissey told Det. Lilley that Schwartz uses an Apple portable computer to do his work at Intel, and attaches it to the Intel network when he is there. Morrissey "expressed concern" that passwords had been transferred to that computer. Morrissey also said that Schwartz was identified, through his user identification and password,¹³ as the person running the password-cracking program,¹⁴ (6/15/95 Tr. 63 ll. 17-22), and that Schwartz was security conscious enough to use a password that would be difficult for anyone else to obtain and use. App 1. Morrissey also said that Schwartz was sophisticated enough to cover his tracks if that was what he intended (6/15/95 Tr. 63 ll. 8-13; 7-14-95 Tr. 204) and that Schwartz was running the password

¹³A system administrator has what is called "root access" to the operations of the computers in his system. That means that, among other things, he can determine who is doing what at any given time by executing a command or a series of commands. 6/14/95 Tr. 180, 188; 7/14/95 Tr. 210-211.

¹⁴6/14/95 Tr. 187.

cracking program in the open under his own user identification and password. 6/15/95 Tr. 63 l. 17 - Tr. 64 l. 6.

Det. Lilley swore that Cower volunteered that if Schwartz desired to avoid detection, he "would" transfer the files to his portable computer, and that this would be a "convenient" way to move them from Intel to his home or office without detection (App 2). By contrast, Cower denied that he volunteered this information and denied that he said anything to Det. Lilley about Schwartz taking anything home. 6/13/95 Tr. 89. According to that affidavit, Morrissey said that Schwartz often works out of his office or home (App 2). Morrissey, under oath, adamantly denied that he had said that. 6/14/95 Tr. 199 l. 13 to 200 l. 2.

Det. Lilley was told that Schwartz's activities were monitored all day on Monday, 11/1/93, that he had not logged onto the computer running the password cracking program, and that he had not logged onto that computer since that program began running on 10/21/93. 7/13/95 Tr. 68, 69. That was omitted from the affidavit.

According to Det. Lilley, Cower said that information can be stored on any computer that has: 1) floppy disc drives; 2) any kind of tape drive; 3) any kind of hard drive; 4) tapes and/or floppy discs. It can also be stored on: 5) printouts; 6) "computer related documentation;" 7) written information related to Intel Corp; 8) a personal digital assistant; 9) any "computer related contents" in personal and/or business vehicles. App 2-3.

Also according to Det. Lilley, Morrissey said that Dirk Brandewie, the system administrator responsible for "Mink" (7/18/95 Tr. 6; See Count 1), had told him that in March, 1993, Schwartz had bypassed Intel security systems ("blocks") which prevent outside access to Intel computers. Brandewie reportedly said that he told Schwartz to replace "the blocks," but in July of the same year had found that "the blocks" were back off. Schwartz had explained that he desired to gain access to Intel systems from the outside. App 3. When Morrissey testified about this, however, it turned out that he had personally examined the outside access program and that the outside access program had not been quite the open door that it had appeared to be from the affidavit. 7/14/95 Tr. 191-2; Tr. 195-6. Brandewie confirmed that. 7/18/95 Tr. 12 ll. 2-9. Brandewie did indicate, however,

that telnetting¹⁵ in from the internet, as opposed to telnetting out, was not permitted. 7/18/95 Tr. 9 l. 5 to Tr. 10 l. 13. According to Schwartz, the policy was that inbound telnet was "dangerous."¹⁶ 7/21/95 Tr. 81 ll. 1-2.

Det. Lilley swore that Morrissey said that the program used by Schwartz was "RUBY.ORA.COM," which belongs to the publisher of books written by Schwartz. According to the affidavit, Morrissey did not know how, or from what location, Schwartz was gaining access to "RUBY.ORA.COM." App-3. In fact, "RUBY.ORA.COM" is not a program, Morrissey did not say that it was (6/14/95 Tr. 216), and, consequently, the affiant either misunderstood or misrepresented what he heard.

Det. Lilley included the location of Schwartz' office and home, and a detailed description of his vehicle. Among the long list of items he requested permission to seize were all computers, discs and tapes, because, he alleged, it is not possible to know which of those (if any) contain "material sought by this affidavit" without examining them. See App-4 to 5. That was based on the assertion that Det. Lazenby "knows" that persons "involved in these activities" try to conceal the contents of the disks and tapes "Schwartz used" by mislabeling or not labeling their contents, and that an expert is needed to examine computer evidence in an environment where information will not be destroyed. App-4.

The affidavit also requested permission to search for, and seize "all telephones equipped with recording devices, automatic dialers or any other special equipment the examination of which can reveal information concerning the prior use of the equipment" and "any 'blue boxes' or 'black boxes' that being devices specifically constructed for the purposes of using telephone services while avoiding detection or payment for the services provided." App-4 to 5.

On 11/1/93, the search warrant was executed at Schwartz's residence. In addition to some uniform officers, the detectives in charge of the case invited Cower, Pierce, and Stites along to help execute the warrant (9/20/94 Tr. 80-81) without authorization from the

¹⁵A way of talking computer to computer. 7/20/95 Tr. 144 ll. 12-17; Tr. 145 ll. 12-19.

¹⁶Intel had policy manuals, but they were not generally circulated. 7/14/95 Tr. 183.

magistrate who issued the warrant, despite the fact that Cower, Pierce and Stites were involved in the preparation of the affidavit and the magistrate's permission could have been sought.

Schwartz's two laptop computers and two hard drives were seized and examined by one of the two Washington County Deputy Sheriffs trained in computer evidence analysis. 7/19/95 Tr. 96-97. The data stored on Schwartz's computers was examined using technology which makes a "mirror copy" of the data in those devices. 7/19/95 Tr. 98 ll. 5-12. This mirror copy preserves not only whole, active files but also bits and pieces of files that have been erased but not overwritten.¹⁷ 7/19/95 Tr. 98 ll. 13-17.

Then the data in the mirror image was searched using a program that looks for keywords.¹⁸ 7/19/95 Tr. 98-99. After that, the data was searched for anything of evidentiary value. 7/19/95 Tr. 99 ll. 18-22. This process was completed four times, one for each device. 7/19/95 Tr. 99 ll. 23-25. Nothing of an incriminating nature was found on either of the hard drives or on either of Schwartz's laptop computers. 6/15/95 Tr. 286 ll. 15-16; 7/14/95 Tr. 228 l. 1 to 230 l. 13; 7/19/95 Tr. 103 ll. 21-25.

During the execution of the warrant, Det. Lilley interviewed Schwartz for two hours. 6/15/95 Tr. 50 ll. 6-9. Lilley's understanding of computers was very limited. 7/13/95 Tr. 61, ll. 6-11. He did not understand much about what Schwartz had to say.¹⁹ 7/13/95 Tr. 45 ll. 6-9. Small portions²⁰ of the conversation were recorded in his notes and included in his police report. 6/15/95 Tr. 42-50. According to Det. Lilley, his report was "the summary of the essence of what was said." 7/13/95 Tr. 76 ll. 16-17.

¹⁷The mirror imaging technology does not work on laptops, so the data was copied from the laptops to another hard drive prior to the examination. 7/19/95 Tr. 104.

¹⁸The keywords were supplied by Intel. 7/19/95 Tr. 101 ll. 19-23. The printouts of the results of the keyword searches were presented to Intel. 7/19/95 Tr. 100 ll. 4-7.

¹⁹For example, Det. Lilley understood Schwartz to say that "root" is a program which is "the means for which he ran the Crack program." 7/13/95 Tr. 81, ll. 5-13; Tr. 83 ll. 3-11. "Root" is a term that designates a system administrator's privilege in a network of computers using the UNIX operating system, not a program. 6/14/95 Tr. 179 ll. 14-19; 7/13/95 Tr. 135 ll. 6-11. One with "root" access can do anything on that system. 7/13/95 Tr. 134-135.

²⁰Det. Lilley's testimonial rendition of his two-hour long conversation with Schwartz, including questions by the prosecutor, took 15 minutes. 7/13/95 Tr. 75 l. 23 to Tr. 76 l. 1.

///

Seeking suppression of his statements, defendant filed both a Motion to Suppress and a Supplementary Motion to Suppress (Motion to Controvert). Both Motions were denied. 7/13/95 Tr. 40-53.

Defendant demurred to the indictment on the grounds that: 1) The terms "alter" and "without authority" in ORS 164.377(3) are unconstitutionally vague; 2) that the statute underlying Count 1 was not sufficiently definite and certain in that it did not distinguish between a culpable mental state and an element; and 3) that the computer crime statute was unconstitutionally overbroad in several particulars. That demurrer was denied.

Schwartz was convicted on all counts by the jury and sentenced on all counts, over the objection that Counts 2 and 3 should merge. The court ordered \$68,471.45 in restitution to Intel as a condition of probation, over the objection that the state had not sufficiently proved the losses that Intel had claimed or demonstrated that they were suffered as a result of Schwartz's conduct.

ASSIGNMENT OF ERROR NO. 1

The trial court erred when it denied defendant's Motions to Suppress as follows:

The Court having heard the sworn testimony and duly considered the arguments of counsel, FINDS that:

1. The affidavit for the search warrant establishes probable cause and is not overbroad.
2. The police did not violate Oregon Revised Statute 133.575
3. Any omissions or inaccuracies in the search warrant affidavit are not material and there is no substantial basis to question the good faith, accuracy or truthfulness of the affiant. App-8.

ARGUMENT

I. Supplementary Motion to Suppress (Motion to Controvert)

A. Standard of Review

In a motion to controvert, the moving party is required to prove the affiant's lack of good faith, accuracy or truthfulness by a preponderance of the evidence. ORS 133.693(3). The Court of Appeals reviews a trial court's findings for supporting evidence in the record.

State v. Ritter, 71 OrApp 282, 288, 692 P2d 158 (1984).

B. Findings and Conclusions

The defense requested "Specific Findings of Fact and Conclusions of Law," both in the caption and the body of the Supplementary Motion to Suppress. The trial court simply found that "[A]ny omissions or inaccuracies" were not material. It did not find that there were no such omissions or inaccuracies. In fact, the trial court noted on the record that there were both inaccuracies in, and omissions from, the affidavit. 6/15/95 Tr. 285-6. Simply dismissing them as "immaterial" is not sufficient. The trial court was required, at a minimum, to provide this Court with a list the assertions in the search warrant affidavit that it deemed to be inaccurate. *State v. Wise*, 305 Or 78, 749 P2d 1179 (1988); *State v. Bates*, 304 Or 519, 527-28, 747 P2d 991 (1987); *State v. Dimeo*, 304 Or 469, 478 n. 4, 747 P2d 353 (1987).

C. Inaccuracies and Untruths in Affidavit

1. " * * * Mr. Rich Cower * * * told me that based upon his security experience in computer hacking (unauthorized access to computer information), in order to avoid detection in the workplace, Mr. Schwartz would transfer the information to his Apple portable computer in order to work with the information in the privacy of his own home." App 2

The truth, according to Cower, was that Cower had called the FBI and a computer crime investigator told him not to let Schwartz out of the building with his laptop, "because if he has any confidential information, it would be on the laptop." 6/13/95 Tr. 86, ll. 20-22. What Cower was told by the FBI indicated nothing, then, about Schwartz's home. The information Cower related to Det. Lilley was what he had learned from the FBI. 6/13/95 Tr. 89, ll. 11-19.

According to Det. Lilley, "the Intel people" brought that subject up, and Det. Lilley admitted that Cower did not relate any facts indicating that Schwartz was running the programs in question in a way calculated to "avoid detection in the workplace." 6/13/95 Tr. 153. In fact, Det. Lilley admitted that he was told that Schwartz was running the program under his own name and that the files upon which the program were running, the SSD

password files, were stored under Schwartz's own name and user identification. 6/13/95 Tr. 143; Morrissey confirmed that. 6/14/95 Tr. 187. Morrissey also told Det. Lilley that Schwartz is sufficiently knowledgeable that he could avoid systems security checks and also cover any traces of his activities if he chose to do so. 6/14/95 Tr. 200-201. Det. Lilley omitted that information from the affidavit, and apparently created the reference to Schwartz's home out of whole cloth.

2. "That on 11/1/93 I spoke with Mark Morrissey, Senior Engineer (15 year computer knowledge), an employee of Intel Corporation, who advised me that he had found evidence of violations of ORS 164.377 (Computer Crime) at Intel Corporation, 5200 N.E. Elam Young Parkway, Hillsboro, Washington County, Oregon." App 1.

Det. Lilley admitted that the "evidence of violations of ORS 164.377 (Computer Crime)" words were supplied "later," and had not been said by Morrissey. 6/13/95 Tr. 125. Morrissey confirmed that he had not said that. 6/14/95 Tr. 195.

3. "That Mr. Morrissey told me that he expressed concern to Mr. Kent that password information had been transferred to Mr. Schwartz's Apple portable computer." App 2.

Det. Lilley testified that the "concern was more for the potential rather than any actual transfer of information." 6/13/95 Tr. 151, ll. 24-25. Det. Lilley had been given no information to indicate that anything of an improper nature had been transferred to Schwartz's laptop computer. 6/13/95 Tr. 152. Morrissey testified that when Det. Lilley asked if it was possible that Schwartz could have transferred information to his laptop, Morrissey responded that it was "possible." 6/14/95 Tr. 209 l. 19.

Morrissey also testified that he told Det. Lilley that Schwartz had transferred information to his laptop before and that to do so was, indeed, the reason for bringing the laptop to Intel. 7/14/95 Tr. 209-210. He said that he did not know what information had been copied to Schwartz's laptop, that he would assume that Schwartz had done so in his capacity as a contractor for Intel,²¹ and that Det. Lilley did not ask what kind of information Schwartz might have copied to his laptop. 6/14/95 Tr. 211 ll. 4-6. According to Morrissey, Det. Lilley was expressly interested in whether it was **possible** that Schwartz had copied

²¹6/14/95 Tr. 210 l. 23.

information from Intel computers onto his laptop. 6/14/95 Tr. 210 ll. 15-17. This was reiterated by Morrissey on cross-examination - that Det. Lilley had asked him if it was **possible** that Schwartz had copied information from Intel's computers onto his laptop. 6/14/95 Tr. 231. However, that is not what the paragraph in the affidavit said, and it is not what the magistrate was led to believe. The magistrate was led to believe that the subject was raised by Morrissey and that there was some unspoken reason for his "concern."

4. "That further Mr. Morrissey told me that Mr. Schwartz has told him that he (Mr. Schwartz) often works out of his home and office." App 2.

Morrissey denied this most material allegation in its entirety. Not only did Schwartz not tell Morrissey where it was, off-site, that he worked, but Morrissey did not tell Det. Lilley that Schwartz had said anything about working "out of his home and office." Morrissey did not claim any knowledge about where Schwartz works when off the Intel campus. 6/14/95 Tr. 199 l. 13 to 200 l. 2.

Det. Lilley was less than definitive on this issue. The most he could say was that he "believed" that he recalled that "someone" from Intel told him that Schwartz worked on Intel business from home. 6/13/95 Tr. 135. This entire sentence should have been stricken from the affidavit. It and the statement about "avoiding detection in the workplace," which was attributed to Cower but which Cower repudiated and Det. Lilley at least partially recanted, were **the only** references in the affidavit which even mentioned Schwartz's home.

///

///

5. "That Mr. Morrissey told me that the reason he believed that Mr. Schwartz himself was running the [password cracking] program was because Schwartz is security conscious enough to use a secure password that would be extremely difficult for any other person to obtain and utilize." App 1.

What Det. Lilley did not say, in this connection, is that Morrissey also told him that Schwartz is sufficiently knowledgeable to not only avoid systems security checks but to cover any traces of his activities if he chose to do so. 6/14/95 Tr. 200-201. Had that information been included in the affidavit, it would have directly contradicted the inference

that Det. Lilley was creating²² that Schwartz had been involved in some kind of surreptitious activities.

D. Material Omissions from Affidavit

1. Det. Lilley was told that all of Schwartz's files on "Brillig" had been checked and that no stolen or illegal files had been found. He omitted this from the affidavit. 6/13/95 Tr. 141-2. Its omission was material and significant, given the fact that Det. Lilley included the following: "That Mr. Morrissey told me that he then rechecked files owned by Randal Schwartz using Mr. Morrissey's computer system and discovered that many passwords for SSD employees had been compromised."

Det. Lilley was also told that Schwartz had an authorized, working password on "Brillig,"²³ a computer in the SSD cluster, which he also omitted from the affidavit. This is significant because it is standard practice to remove a user's password from the password file on a machine when his authorized access is terminated. 6/14/95 Tr. 197-198. Schwartz's password on Brillig was legitimate. 7/13/95 Tr. 181-182.

///

///

2. Morrissey told Det. Lilley that there was no indication that Schwartz had removed the password cracking program or elicited any passwords from the output (i.e., from Morrissey's systems).²⁴ 6/14/95 Tr. 206, 207. That information was omitted from the affidavit.

3. "That Mr. Morrissey told me that Dirk Brandewie, Software Engineer, Intel Architecture Development Labs, told him: that in March of 1993, Mr. Brandewie had found evidence that Mr. Schwartz had bypassed the Intel security systems which prevented people from accessing the Intel computers from outside. That Mr. Brandewie had Mr. Schwartz put the blocks on preventing outside access and in July of 1993, while conducting an update check Mr. Brandewie had found the blocks were back off and in confronting

²²For instance, with the phrase "to avoid detection in the workplace," which he attributed to Cower but for which Cower declined to take credit.

²³6/14/95 Tr. 198.

²⁴Morrissey said that it was possible to alter the activity logs, but that there was no reason to believe that had been done and that he could tell if it had. 6/14/95 Tr. 205.

Mr. Schwartz, Mr. Schwartz said he did it to gain access to Intel systems from the outside." App 3.

Det. Lilley omitted the following known, relevant facts from the affidavit:

- a. The machine that Schwartz was "accessing" from the outside was specifically set up for the purpose of outside access from inside Intel. 6/14/95 Tr. 215-216. It was an "internet gateway host." 7/18/95 Tr. 8.
- b. Brandewie and Morrissey told Schwartz that it was a violation of Intel policy for him to run the access program **in that fashion**, and that access needed to be narrower. 7/14/95 Tr. 182 (Emphasis added). Morrissey informed Det. Lilley of that fact. 6/14/95 Tr. 221
- c. Schwartz had a valid, authorized account on the machine on which the program was running, and Det. Lilley knew that as well. 6/14/95 Tr. 222.
- d. Morrissey also told Det. Lilley that Schwartz said that he needed the outside access in order to do his Intel work and, among other things, read his Intel email. 6/14/95 Tr. 215.

The omission of this information left the magistrate with a completely false impression of what was actually happening.

4. "Mr. Brandewie told Mr. Morrissey who told me that the program being used by Mr. Schwartz to access Intel systems from the outside was identified as RUBY.ORA.COM. That Mr. Morrissey told me that RUBY.ORA.COM is a program that belongs to O'Rielly and Associates, which is the publisher of UNIX books and they are located on the East Coast of the United States. That Mr. Morrissey also told me that O'Rielly and Associates is a publisher that has published books written by Mr. Schwartz. Mr. Morrissey also told me that he does not know how or where Mr. Schwartz is accessing the RUBY program from." App 3.

This paragraph actually embodies a rich mixture of inaccuracies and false impressions conveyed through the use of material omissions. RUBY.ORA.COM is a computer, not a program, and Morrissey did not tell Det. Lilley that RUBY.ORA.COM **was** a program. He told Det. Lilley that it was a computer. 6/14/95 Tr. 216. Schwartz had an email address at this computer, which is owned by his book publisher. 6/14/95 Tr. 216, ll. 21-26; 7/19/95 Tr. 60 ll. 5-7; Tr. 60 l. 23- Tr. 61 l. 3. He used his perfectly legitimate access to that

computer to read his email at Intel. 7/13/95 Tr. 69 l. 24-Tr. 70 l. 7; 7/14/95 Tr. 182; 7/18/95 Tr. 140 ll. 8-13.

When the gate program was first discovered running on Mink, Schwartz told Brandewie exactly that. 7/18/95 Tr. 34 ll. 20-22. Schwartz travelled out of town during his tenure at Intel (7/13/95 Tr. 117), and it was within his contract terms to do so. 7/13/95 Tr. 117. The problem with the gate program was that Morrissey and Brandewie did not believe that the access gained by means of that program was narrow enough. See 6/14/95 Tr. 221-223; 7/14/95 Tr. 182. The affiant's inaccuracies in and omissions from this paragraph created an impression which was entirely at odds with the truth. It was written to suggest that Schwartz gained illicit access to a program owned by his publisher that he was using to access Intel machines for nefarious purposes.

5. "That Detective Lazenby of the Washington County Sheriff's Office has told me that through his experience and training he knows that persons who are involved in these activities often will try to conceal the contents of the disks and tapes **Mr. Schwartz used** by mislabeling or not labeling their contents, therefore, it is respectfully requested that the authorization for seizure of any and all computer disks and tapes be ordered to enable review of the necessary computer storage disks and tapes." Emphasis added.

No one told Det. Lilley that Schwartz had used any disks or tapes. He admitted that he did not know whether he was told that Schwartz used disks or tapes. 6/13/95 Tr. 151. Morrissey certainly did not tell him that. 6/14/95 Tr. 225. Det. Lazenby testified that he had no information indicating that Schwartz used disks or tapes. 6/13/95 Tr. 64-65.

Moreover, Det. Lazenby had **no** experience in the investigation of computer crimes. 9/20/94 Tr. 131 ll. 3-5. His experience consisted of four or five drug cases and a homicide case where computers were seized. 6/13/95 Tr. 70. He was not trained to examine data. 6/13/95 Tr. 70. Det. Lazenby's training consisted of a two week course in the investigation of computer crimes. 6/13/95 Tr. 63. He was basically taught how to seize computers and tag all the parts. 6/13/95 Tr. 69. Det. Lilley was aware of Det. Lazenby's "training and experience." 6/14/95 Tr. 159. When he referred to "these activities," Det. Lazenby was referring to cases where "somebody goes into a computer and takes stuff that's not theirs."

6/13/95 Tr. 65. No one had any information, at the time that Det. Lilley filed this affidavit, indicating that Schwartz had "taken" anything. 6/13/95 Tr. 92-93, 104. In fact, he had not. 6/15/95 Tr. 286.

The inclusion of this paragraph, with these two misstatements, was materially misleading and was a significant factor in the issuance of a warrant that authorized the seizure of such things as keyboards and monitors (App 4), upon which no data can be stored.

E. Trial Court's Decision

1. Requisite Analysis

State v. Harp, 299 Or 1, 697 P2d 548 (1985) requires that once inaccuracies appear in the affidavit, the Judge hearing the motion to suppress must begin to perform surgery. His job "is a procedure of subtraction, not addition." 299 Or at page 9. Also, once a substantial basis for questioning the good faith, accuracy or truthfulness of the affiant has been shown, there is no occasion for according the decision of the magistrate the deference that it ordinarily deserves. 299 Or at page 10.

After the untrue and inaccurate information is excised from the affidavit, the affidavit must be reevaluated for probable cause in light of the controverting information. *State v. Miller*, 116 Or App 174, 179 (1992), aff'd as modified 119 Or App 102 (1993) (requiring that officer's subjective belief that something subject to seizure is in the place to be searched be objectively reasonable and holding that officer's good faith will not save warrant if excision of untrue or inaccurate statements nullifies probable cause); *State v. Keeney*, 323 Or 309, 918 P2d 419 (1996).

That is not what happened here. First, even though the trial court acknowledged that the affiant misreported, to the magistrate, the information he had received, the trial court "denied" the Motion to Controvert. 6/15/95 Tr. 286 ll. 7-8. Nothing was excised from the affidavit. Apparently, that denial was based on the trial court's view that the inaccuracies and omissions proved did not constitute a "substantial basis" for questioning the good faith, truthfulness or accuracy of the affiant. 6/15/95 Tr. 286 ll. 3-7. The cases do not support

that view.

In *State v. Modrell-Lydall*, 128 Or App 372, 876 P2d 315 (1994), the Court of Appeals ruled that a statement from someone who claimed to be one of the CRI's to the effect that some of the information contained in the affidavit was "wrong."²⁵ The error was that the affiant had asserted the personal knowledge of the informant, whereas the informant had told the affiant that she knew the information by hearsay. The mere assertion of this inaccuracy established a "substantial basis" under ORS 133.693 for questioning the good faith, truthfulness and accuracy of the affiant.

The trial court here noted that the affiant knew things at the time of the submission of the application for the search warrant that were "relevant," but that the affiant did not see as "all that relevant" at the time. 6/15/95 Tr. 285. This remark suggests that the trial court believed that "relevant" was not equivalent to "material."

Omissions which affect the probable cause are significant when evaluating search warrant affidavits. The omitted information may not be included for purposes of analyzing what is left of that pattern after the inaccurate or untrue allegations are removed. *State v. Harp*, supra, 299 Or at 9. However, what was omitted from the affidavit may significantly alter or limit the inferences which may be drawn from the remaining, accurate information. *State v. Carter*, 316 Or 6, 13, 848 P2d 599 (1993), citing *State v. Harp*, supra.

An example of this is the affiant's assertion that Schwartz would take information home on his laptop computer in order "to avoid detection in the workplace." Ignoring for argument's sake the fact that Cower did not say anything of the kind, the affiant learned that Schwartz was running the password cracking program on the SSD password file on a machine readily accessible by others, that he was running it using his own user identification (6/13/95 Tr. 137, 143) and that he was running it using his own password. 6/13/95 Tr. 138. The affiant admitted that he "may" have been told that Schwartz was

²⁵The trial court here remarked that even though there were inaccuracies and "relevant" omissions, there was no basis for questioning the good faith, truthfulness or accuracy of the affiant. 6/15, Tr. 286.

sophisticated enough to cover his own tracks if he desired to do so. 6/13/95 Tr. 137.

The affiant completely altered the tenor of this information by omitting those facts. The affiant replaced that information with the following:

* * * "That Mr. Morrissey told me that he then conducted a check on who was running this program and learned that it was Randal Schwartz . . . * * * That Mr. Morrissey told me that he was able to identify Mr. Schwartz as the owner of the program and data files by Mr. Schwartz's user identification. That Mr. Morrissey told me that the reason he believed that Mr. Schwartz himself was running the program was because Mr. Schwartz is security conscious enough to use a secure password that would be extremely difficult for any other person to obtain and utilize." App 1.

Considered in light of the whole of what the affiant was told, the statement about "avoiding detection in the workplace" was deceptive to say the least, and the statement about why Morrissey believed Schwartz was running the program was an outright fabrication. As such, this entire passage was grossly misleading when presented to the magistrate.

Another example of information tailoring was the statement that Morrissey said that he had expressed "concern" to Kent that password information had been transferred to Schwartz's laptop computer. App 2. Lilley testified that the concern was more for the "potential" transfer of information than the actual transfer (6/13/95 Tr. 151). He omitted that fact from the affidavit. In addition, he omitted the facts that: 1) He had been given no reason to believe that Schwartz had improperly transferred password information to the laptop (6/13/95 Tr. 152); 2) Morrissey had told him that transferring information to the laptop was, indeed, the reason for bringing the laptop on site (7/14/95 Tr. 209-210); 3) Morrissey told the affiant that he would assume that, if Schwartz had done so, he had done so in his capacity as a contractor for Intel (6/14/95 Tr. 210 l. 23); and 5) the whole subject came up in response to the affiant's question about whether it would have been **possible** for Schwartz to transfer password information to the laptop, not, as implied by the statement's context in the affidavit, as part of an earlier conversation between Morrissey and Kent.

These omissions, together with the careful, abridged way the included information was

presented, created a completely false impression of the information that the affiant had been given, and permitted, if not compelled, the drawing of false and unwarranted inferences. ORS 133.693 "requires a court to suppress evidence if it finds that an officer acted in other than good faith in making an affidavit, as for example, by purposefully excluding material information that would go against a finding of probable cause for a search or seizure." *State v. Miller*, supra, 116 Or App at 178.

///

///

2. Materiality

The trial court's decision that the omissions and inaccuracies in the affidavit were not material is not supported by the evidence in the record. The only two references to the place sought to be searched - the home of Schwartz - were recanted or debunked.

In an unbroken line of cases beginning with *State v. Anspach*, 298 Or 375, 692 P2d 602 (1984), the Oregon Supreme Court and the Oregon Court of Appeals have required that a search warrant affidavit state sufficient facts to permit a reasonable person to infer that seizable items are in the place to be searched. A suspicion that the evidence may be there is not enough. *State v. Anspach*, supra, 298 Or at 381; *State v. Carter*, supra, 316 Or at 12.

The first reference in the affidavit to Schwartz's home was attributed to Cower. However, neither Cower nor the affiant confirmed that Cower had made any reference to Schwartz's home. The context in which the statement appeared in the affidavit was utterly contradicted by overwhelming evidence. The affiant put a spin on this that was completely unsupported by what he had learned.

The second reference to Schwartz's home, to the effect that Schwartz often works at his home, allegedly came from Morrissey. It was that reference upon which the prosecutor relied to distinguish the instant case from *State v. Maxfield*, 133 Or App 371, 891 P2d 1342 (1995). 6/13/95 Tr. 19. During arguments on the Motion to Suppress, the trial judge specifically called that reference to the attention of both counsel, in answer to defense counsel's assertion that the affidavit contained no facts indicating that any evidence would

be found in Schwartz's home. 6/13/95 Tr. 18.

As noted above, Morrissey clearly and without reservation disavowed the statement attributed to him by the affiant, testifying that Schwartz had never discussed, with him, where Schwartz worked when he was not present at Intel. 6/14/95 Tr. 199. He said that all he told the affiant was that Schwartz had said that Schwartz did work off site. 6/14/95 Tr. 199 ll. 22-23. Det. Lilley could only recall that he "believed" someone from Intel had told him that Schwartz worked at home. 6/13/95 Tr. 135.

Had the statement in the affidavit merely been attributed to "someone at Intel," it would have constituted an anonymous tip which adds nothing to the probable cause. *State v. Carter*, supra 316 Or at 11. But it was attributed to Morrissey, who did not say it. The trial court made it clear in his questions during the argument on the Motion to Suppress that he believed that Morrissey's information should be credited. 6/13/95 Tr. 21. For the trial court to hold, then, that these references to Schwartz's home were not "material" to the probable cause is simply unfathomable. It was Schwartz's home that was the principal target of the search warrant.

An affidavit supporting a search warrant must set forth some factual nexus between the objects of the search and the place to be searched. *State v. Gloster*, 145 OrApp 555, 558, 932 P2d 68 (1997) citing *State v. Tidyman*, 54 OrApp 640, 643-44, 635 P2d 1355 (1981), rev den 292 Or 722, 644 P2d 1131 (1982). In this case there was no true factual nexus between the objects sought and the place to be searched, and the affiant sought to cure that fatal flaw by making some up. He recognized that references in the affidavit to Schwartz's home would be very significant. The Motion to Controvert should have been granted and these references to the home of Schwartz should have been stricken.

Likewise, the trial court should have stricken the sentence indicating that Morrissey said he had discovered evidence of violations of ORS 164.377 (Computer Crime), the report that Morrissey said he had expressed "concern" about the transfer of password information to Schwartz's laptop, the whole paragraph about Schwartz using a machine called RUBY.ORA.COM to bypass Intel security systems to access Intel computers from outside,

the references to "persons involved in these activities" and "the disks and tapes Mr. Schwartz used" in the paragraph outlining Det. Lazenby's contribution, and the sentence indicating that Morrissey "believed" that Schwartz was running the password cracking program. In fact, he **knew** it; it was obvious, and the way the sentence is crafted permits an unwarranted inference to be drawn.

All these inaccuracies, together with the material omissions noted, combined to give a false picture to the magistrate.

II. Motion to Suppress

A. Probable Cause in General

In reviewing an affidavit to determine whether it alleges particular facts that would lead a "reasonable person to believe that seizable things will be found," *State v. Anspach*, supra, 298 Or at 381, mere suspicions, conjectures or conclusions, entertained without the presence of particular facts to support them, do not establish probable cause to search and cannot support a search warrant. *State v. Carter*, supra, 316 Or at 12.

Most of the information in the affidavit comes from named informants, who are entitled to a presumption of veracity. *State v. Carlile*, 290 Or 161, 165, 619 P2d 1280 (1980). Yet, leaving aside for a moment the substantial controversion outlined above, the only basis in this affidavit for thinking that any of Intel's information left the Intel campus with Schwartz was Cower's alleged statement, later denied, about how it would be done **if it had been done** and Morrissey's "concern" (expressed to Kent, apparently, and not the affiant) that password information had been transferred to Schwartz's computer. The affidavit did not contain any facts to indicate that password information actually had been transferred, only that Morrissey told Kent that he was **concerned** that it had.

Morrissey's expression of "**concern**" constitutes no more than conjecture under these circumstances. There are no facts upon which the magistrate could infer that Schwartz **had** transferred password information from Intel computers to his laptop. And, while Cower's beliefs about how hackers transfer information and can store data were instructive, they did not establish that there was a probability that this particular computer user had done so.

Extraneous knowledge and conclusions, even those attributed to trained and experienced police officers, are insufficient to support such a finding. In *State v. Evans*, 119 Or App 44, 47, 849 P2d 539 (1993), the Court said: "[S]tanding alone, the officer's intuition or professed knowledge of the common practices of people who grow, distribute and sell marijuana is not an additional fact supporting probable cause that this particular residence contained any particular evidence." This rule was reaffirmed in *State v. Goodman*, 152 Or App 83, ___ P2d ___ (1998).

In *State v. Carter*, supra, 316 Or at 13, the Supreme Court stated:

A fact that merely supports an inference that some other fact is possible - as one among the range of many other and different possibilities - does not support an inference that any specific one of the possible facts is itself probable. Probable cause is necessary to support a warrant, not merely one possibility, among many.

The failure of the affidavit to establish more than a mere possibility that Schwartz had transferred information to a portable computer is particularly important because the applicant for this warrant sought to search Schwartz's **home**. The home is the place where, traditionally, there is the highest legitimate expectation of privacy. *Payton v. New York*, 445 US 573, 100 SCt 1371, 63 LEd2d 639 (1980). If the conclusions, speculations and conjectures of software engineers (Morrissey) and Network Security Specialists (Cower) are insufficient to support a probability that Schwartz had transferred password information to his laptop computer, they can hardly support the entry, seizure²⁶ and search of his home for that computer. The affidavit at issue here is lacking in specific articulable facts to support an inference that any criminal activity occurred at or near the Schwartz's home, office or vehicle. Evidence concerning those events reported by the various Intel employees, who are the sole sources of information contained in the affidavit, is inferentially available, if anywhere, solely in the electronic memories of the machines at

²⁶A seizure of any premises constitutes seizure of everything in the premises, which must be supported by probable cause. *State v. Matsen/Wilson*, 287 Or 581, 601 P2d 784 (1979); *State v. Olson*, 287 Or 157, 598 P2d 670 (1979); *State v. Peller*, 287 Or 255, 598 P2d 684 (1979).

Intel.²⁷ That is clear from a common sense, non-technical reading of the four corners of the affidavit.

Where there is an insufficient factual nexus between suspected criminal activity and the suspect's home, there is no probable cause to search that home. *State v. Stockton*, 120 Or App 111, 852 P2d 227 (1993); *State v. Evans*, supra.

In *State v. Corpus-Ruiz*, 127 Or App 66, 874 P2d 90 (1994), the affiant had noted three events connecting the place to be searched with drug activity: A known drug offender under surveillance (Michael) had been seen entering the defendant's house; another subject was seen leaving the defendant's house under the influence of heroin some six months previous to the warrant; and Michael's car had been seen parked in front of the defendant's house. The person leaving the defendant's house under the influence supported the inference that he had obtained the heroin there, but the Court of Appeals held that a single, remote incident did not support the inference that any heroin would still be there. 127 Or App at 669-670. In so holding, the Court stated:

The reference to Michael's car stopping at defendant's house is vague in this context. We cannot tell whether Michael's car parked in front of defendant's house because that parking spot was near Gomer's house, or if the occupant of the car visited defendant's house. The vagueness of the car stopping in this context forces a magistrate to make two consecutive inferential leaps: first, that Michael met with someone at defendant's house and second, that the meeting was drug-related. In context, the reference to the car stopping was too vague to be relevant.

The facts recited by the affidavit in this case would not lead a reasonable magistrate to believe that evidence of drug distribution would probably be found at defendant's house. *State v. Anspach*, [supra], 298 Or at 380-81. The court erred by denying the motion to suppress. 127 Or App at 670.

In the present case, at least three inferential leaps were required to arrive at even a suspicion that there was any connection between what happened at Intel and any of the contents of the Schwartz residence. The first, that Schwartz was doing anything inimical to Intel's interest, is unsupported by specific facts, particularly given the circumstances

²⁷For example, the existence of the "gate" program was revealed in an examination of the data at Intel, not by looking somewhere else.

surrounding what actually happened. Any basis for the second, that he took anything belonging to Intel that he was not authorized to take, is totally speculative. The third, that he took that something home, is pure conjecture. Speculation and conjecture do not equal probable cause. *State v. Buffington*, 87 OrApp 559 743 P2d 738 (1987); *United States v. Perez*, 67 F3d 1371 (9th Cir 1995) (fact that defendant had used automobile to transport stolen coins to mall for sale 4 days earlier and was using it to return to collect money from sale day of search did not give authorities probable cause to search automobile).

The extent to which this application was based on the speculation and conjecture of the affiant is illustrated by the inclusion of "'blue boxes' or 'black boxes'" in the list of things to be seized. App 4. According to the affidavit, neither Morrissey nor any other source of information mentioned "blue boxes or black boxes" to the affiant. There is no mention of such devices in the affidavit until the affiant asks permission to search for and seize any he may find.²⁸

B. Overbreadth of Warrant

According to the Oregon Supreme Court:

///

Both the Fourth Amendment to the United States Constitution and Article I, § 9, of the Oregon Constitution require a search warrant "particularly describing the place to be searched." It has been explained that the historical motivation for this constitutional mandate was a fear of "general warrants," giving the bearer an unlimited authority to search and seize. More specifically, the aim of the requirement of particularity is to protect the citizen's interest in freedom from governmental intrusion through the invasion of his privacy. **If the search warrant describes premises in such a way that it makes possible the invasion of this interest in privacy without the foundation of probable cause for the search, the warrant is too broad and therefore constitutionally defective.** *State v. Blackburn/Barber*, 266 Or 28, 34, 511 P2d 381 (1973) (footnotes omitted; emphasis added).

²⁸. This point is reinforced by most of the instances of overbreadth, discussed in the next section. For instance, no data can be saved on a keyboard, and no informant suggests that it can. Yet the affiant applies for, and receives, permission to search for, and seize, keyboards. The same is true of "disk drives, floppy disk drives, monitor or monitors, * * * cables, expansion cards, plotters, printers, phone modems, computer mice, image scanners . . ."

The doctrine of "overbreadth,"²⁹ which was developed to protect the "particularity" requirement, is thus distinguished from the doctrine of "indefiniteness," which prohibits warrants that are so ambiguous that it is up to the investigating officer to determine the place to be searched. *Ibid.* at page 35; *State v. Ingram*, 313 Or 139, 145, 831 P2d 674 (1992). To pass statutory and constitutional muster, search warrants must be both definite and particular. ORS 133.565(2); Constitution of the State of Oregon, Article I §9; Constitution of the United States, Fourth Amendment; *State v. Ingram*, *supra*.

In *State v. Reid*, 319 Or 65, 872 P2d 416 (1994), the Supreme Court reaffirmed the distinction between the requirements of particularity and definiteness in a search warrant. The warrant in question had authorized the search of "persons present" at a certain residence in Eugene. The defendant was searched, pursuant to that provision, when he approached the front door during the execution of the warrant. In passing on the validity of the warrant, the Court stated:

This case does not involve the second of the two statutory limitations identified in [*State v. Ingram* *supra*] that a warrant must be definite enough to identify with a reasonable degree of certainty what is to be searched. 313 Or at 144. "Persons present" is definite and unambiguous.

What this case involves is, instead, the first statutory limitation identified in [*State v. Ingram* *supra*] a warrant may not authorize a search that is broader than the supporting affidavit supplies probable cause to justify. *Ibid.* There was no showing in the affidavit supporting the warrant that access to the Vales' residence was limited exclusively to persons as to whom probable cause exists to believe that they are engaged in criminal activity. The affidavit described a residence. Persons who might reasonably be expected to be found approaching the front door of a residence include a uniformed mail carrier or package delivery person, a volunteer soliciting donations for charitable purposes, or a neighbor seeking to borrow a cup of sugar. Indeed, there were small children present at the residence at the time the warrant was executed.

We conclude that, by authorizing police officers to search "persons present" at the Vale residence, the warrant in this case failed to satisfy the requirements of ORS 133.565(2)(b), because the affidavit did not

²⁹. This must be distinguished from statutory "overbreadth," which was argued in the Demurrer. This is an allegation that the warrant was overbroad because it allowed the seizure of items which it was not permissible to seize and it allowed searches of places which there was no probable cause to search.

demonstrate probable cause to believe that **all** "persons present" on the premises would be associated with the criminal activity taking place there. 319 Or at 71 (Footnote omitted; emphasis in the original).

Here, as in the *Reid* case, the warrant is much broader than the information in the affidavit can be read to support. The difference is that, in this case, there is no probable cause with which to begin. The fact that Intel personnel suggested that Schwartz might have been using some of his computer equipment for criminal purposes does not create probable cause to seize **every piece** of computer or electronic equipment in his house. Such a seizure violates the particularity requirements of Oregon statutes and the state and federal constitutions, for it authorizes the seizure and search of a wealth of non-seizable items which may also be contained in that house.

Even if one assumes that there **is** probable cause to examine the contents of the electronic memory in Schwartz's Apple laptop computer, this warrant is vastly overbroad. It authorizes the seizure of:

All computer systems, microcomputer systems, and laptop computers, as well as all component parts, including but not limited to the keyboards, hard (or internal) disk drives, floppy disk drives, monitor or monitors, motherboards, central processing unit, cables, expansion cards, plotters, printers, phone modems, computer mice, image scanners and all other related equipment.

///

This paragraph permits seizure of **all** computers; yet, **all** computers are not the instrumentality of any crime which might conceivably have been committed. At most, the affidavit can be read to support a search for computer records stored on the Apple laptop computer. The seizure of all computers and computer-related items is not justified.³⁰

Furthermore, if Schwartz's laptop computer was, based on the facts available to the affiant, the probable instrumentality of a crime, the seizure of that laptop would be the

³⁰The affiant asserted that it was not possible to know "exactly which disks contain the material sought by this affidavit," but that does not help. The affiant did not even know if such material existed. It must "probably" exist before any seizure is warranted.

extent of the intrusion permitted by law. Schwartz's activities were monitored carefully after Thursday, 10/28/93. 7-18-95 Tr. 150 l. 21 - Tr. 151 l. 1. A search and seizure warrant for the laptop could have been executed at Intel at any time on 11/1/93, the last day that Schwartz worked at Intel. Cower testified that Intel's main concern was the laptop. 7/18/95 Tr. 132, 148. If that was true, there was no legal reason for contriving to search Schwartz's home.

Additionally, as pointed out above, data cannot be stored on "floppy disk drives, monitor or monitors, * * * cables, expansion cards, plotters, printers, phone modems, computer mice, image scanners . . ." The affidavit states no facts indicating otherwise, yet the affiant seeks seizure of all such items.

Finally, this paragraph is not drawn narrowly and with enough specificity to eliminate the searcher's discretion and opportunity to intrude into the vast amounts of other material stored in any computer(s) that may be discovered. See *State v. Ingram*, supra, 313 Or at 145- 46; *State v. Blackburn/Barber*, supra, 266 Or at 34. And, that portion of the warrant designating ". . .and all other related equipment. . ." runs afoul of the holding in *State v. Ingram*, supra, that a search warrant for a certain premises and "all vehicles associated * * * with the occupants of said premises" was "ambiguous and potentially so broad, officers executing it could invade privacy interests not intended by the magistrate to be invaded and could conduct searches not supported by probable cause." 313 Or at 146.

The warrant authorizes the seizure of:

All telephones equipped with recording devices, automatic dialers or any other special equipment the examination of which can reveal information concerning prior use of the equipment.

Any "blue boxes" or "black boxes", that being devices specifically constructed for the purposes of using telephone services while avoiding detection or payment for the services provided.

There was no indication anywhere in the affidavit that Schwartz possessed "telephones equipped with recording devices, automatic dialers or any other special equipment . . ." or "blue boxes" or "black boxes." There is no factual basis to support probable cause to

believe either that Schwartz possessed these items, or that seizure of such items would produce evidence of a crime.

The warrant authorizes the seizure of:

All computer print-outs or other written records of materials produced by computer. Such information needs to be removed from the site for proper examination to determine if it relates to the offenses under investigation. Specifically including any information relating to the computers of the Intel Corporation and any of its business units or subsidiaries.

This is an astonishingly broad request, justified apparently only by the "need" for a subsequent examination to determine if the information seized even relates to any criminal offense.

Nothing may be seized unless there is **probable cause** supported by specific articulable facts³¹ to believe that it is:

(1) Evidence of or information concerning the commission of a criminal offense; (2) Contraband, the fruits of crime, or things otherwise criminally possessed; (3) Property that has been used, or is possessed for the purpose of being used, to commit or conceal the commission of an offense; or (4) A person for whose arrest there is probable cause or who is unlawfully held in concealment. ORS 133.535.

This paragraph illustrates the dangers inherent in general warrants. "[T]he problem [posed by the general warrant] is not that of intrusion *per se*, but of a **general exploratory rummaging in a person's belongings . . .**" *Andresen v. Maryland*, 427 US 463, 480 (1976) (brackets in original) (emphasis added); *State v. Blackburn/Barber*, supra. This portion of the warrant is not drawn sufficiently narrow, or with enough specificity, to eliminate the searcher's discretion and opportunity to intrude into the vast amounts of other material stored in the computer(s). *State v. Ingram*, supra, 313 Or at 146; *State v. Blackburn/Barber*, supra.

Indeed, the warrant authorized the seizure of printouts of any and all information stored

³¹. *State v. Carter*, supra, at 316 Or 12-13; *State v. Anspach*, supra, 298 Or at 380-81.

in the computer so law enforcement officers could examine it in the future to determine its evidentiary significance. The police cannot seize something because they think it might possibly contain evidence. It must **probably** be evidence when seized or searched for. ORS 133.535; *State v. Jones*, 103 Or App 316, 797 P2d 385 (1990).

In addition, there is nothing in the affidavit to support the implication that the possession, by Schwartz, of information relating "to the computers of the Intel Corporation and any of its business units or subsidiaries" was even criminal. In fact, Schwartz was fully authorized to possess such information. This fact was known to the affiant. 7/14/95 Tr. 209-210.

C. Article 1, §8 and First Amendment Implications.

There are "special restraints upon searches for and seizures of material arguably protected by the First Amendment." *Lo-Ji Sales, Inc. v. New York*, 442 US 319, 326 n.5 (1970)³². Where the object of a search and seizure includes materials which may be protected by Article 1, §8 and the First Amendment, both the particularity and probable cause requirements must be "accorded the most scrupulous exactitude." *Ibid.* 442 US at 325-26; *Stanford v. Texas*, 379 US 476, 485 (1965); *Voss v. Bergsgaard*, 774 F2d 402, 405 (10th Cir. 1985).

The application to search all of Schwartz's computer files and records, and to seize printed or written matter for which there was no probable cause not only violated his right to privacy, but it was an infringement on Schwartz's rights under Article I § 8 of the Constitution of the State of Oregon and under the First Amendment to the Constitution of the United States. The affiant was aware that Schwartz used his computer to access his email (electronic mail) and is a published author. App 3; 6/14/95 Tr. 216. The likelihood that seizure of all Schwartz's computers, equipment and records would impede his ability to communicate by email and cause a restraint of publication due to the potential

³². Article 1, §8 has been interpreted more expansively than the First Amendment. *State v. Henry*, 302 Or 510, 516, 732 P2d 9 (1987). Consequently, federal cases protecting First Amendment interests are authority for the minimum protections under Article 1, §8.

seizure of any written material was palpable.

Thus, this warrant was constitutionally defective because it allowed a search which vastly exceeded the information relied on to support the search both as to place(s) to be searched or as to objective(s) of search.

D. Violation of ORS 133.575

ORS 133.575 provides, in pertinent part:

(1) A search warrant may be executed only within the period and at the times authorized by the warrant and only by a police officer. A police officer charged with its execution may be accompanied by such other persons as may be reasonably necessary for the successful execution of the warrant with all practicable safety.

Cower, Stites and Pierce were invited to accompany the police on the execution of the search warrant. Permission of the magistrate was not sought to justify that.

A number of explanations, some not completely consistent with the facts or with each other, were advanced to justify this action. The District Attorney told the court that "the reason the Intel people were brought was safety in extracting the computer equipment so that the information would not be lost or destroyed. That's exactly why the Intel people were there. They were there as consultants to be able to take the computer equipment safely from Schwartz's home without destroying the information or the subject of the search, and I think that we are within the parameters of this statute." 6/13/95 Tr. 28. Det. Lilley, on the other hand, said that the Intel people were invited along to assist him in understanding Schwartz's answers to his questions, to help identify items of evidentiary value, to assist in maintaining the integrity of that evidence and to safeguard against damage to the computers so that the police would not get sued. 9/20/94 Tr. 80-81.

Those two stories are at stark odds with that told by Cower. He said that Pierce went along to fire Schwartz and that Stites went along to collect the badges that Intel had issued to Schwartz. 9/20/94 Tr. 101. Each was only in the room with Schwartz for a very brief period of time. 9/20/94 Tr. 105 ll. 6-8.

Cower was asked to look at a Macintosh computer that was downloading files, and he

told them that "it looked okay to [him]." 9/20/94 Tr. 102 lines 18-19. Other than that, **all Cower did** was participate in the interrogation of Schwartz for an aggregate time of about one hour. 9/20/94 Tr. 103. In fact, no one from Intel was needed to help safeguard the information on the computers. That was the subject of Det. Lazenby's training. 6/13/95 Tr. 69.

According to Pierce, he accompanied the officers, first and primarily, in order to represent Intel Corporation, to "fire" Schwartz and to terminate his access to any Intel buildings. 9/20/94 Tr. 136 ll. 11-18. Second, Pierce was there to identify, on behalf of Intel Corporation, the "assets" that might be located on diskettes or running on a computer screen somewhere. 9/20/94 Tr. 136 l. 19 -137 l. 1. Pierce explained that by "assets" he meant "trade secrets, password files or anything that would indicate that he had obtained other assets by using intelligence password files. 9/20/94 Tr. 137 ll. 18-21. So neither Pierce, Stites nor Cower were confused about whose bidding they were present to do or what their purpose was, and it was not to provide for safety of any kind or to help preserve evidence. They went along with the police for the purpose of representing Intel Corporation. The execution of this search warrant was a joint, Washington County-Intel Corporation mission.

The trial court simply found that 133.575 had not been violated. That was patently in error. A violation of ORS 133.575(1) alone would probably not warrant suppression of any incriminating evidence *found by the police*³³. Noncompliance with a provision similar to ORS 133.575(2) in a former, similar statute did not result in suppression. *State v. Valentine*, 264 Or 54, 504 P2d 84 (1972).

However, this flouting of the statute was not done in a vacuum. Instead, it was part and parcel of a series of events that included overt misrepresentations of information by the affiant relating directly to the nexus between the suspected crime(s) and the place to be

³³The state offered Cower's version of Schwartz's statements allegedly made during the execution of the search warrant at trial. 7/18/95 Tr. 138-140. That version was somewhat at odds with Det. Lilley's version, to say the least.

searched, careful tailoring of information for purposes of conveying false impressions to the magistrate and the deliberate omission of facts which carried implications contrary to those false impressions.

Under the Fourth Amendment to the Constitution of the United States, citizens are entitled to have the probable cause determination made by a "neutral and detached magistrate." *Connally v. Georgia*, 429 US 245 (1977). It was a violation of Schwartz's Fourth Amendment rights when Lilley decided for himself what relevant evidence the magistrate needed to know, and what relevant evidence he did not need to know, in order to secure the search warrant. This illustrates the dangers recognized by the U.S. Supreme Court in *Johnson v. United States*, 333 US 10, 68 SCt 367, 92 LEd2d 153 (1948):

The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the Amendment to a nullity and leave the people's homes secure only in the discretion of police officers. 333 US at 13-14.

Where, as here, the affiant provides the magistrate with only that information which supports the issuance of the warrant, and withholds all of the information which weighs against issuance of the warrant, the affiant effectively decides whether a warrant will be issued.

E. Suppression Required

The search and seizure which occurred pursuant to the warrant were unlawful and the state must be precluded from using any evidence obtained by exploiting that search and/or that seizure, including Det. Lilley's rendition of the statements made by Schwartz during the execution of the warrant. ORS 133.683; *State ex rel Juv. Dept. v. Rogers*, 314 Or 114, 836 P2d 127 (1992), *State v. Ingram*, supra, 313 Or at 237; *Wong Sun v. United States*, 371 US 471 (1963).

The search warrant process does not exist for the benefit of any private interests; its

purpose is to protect the rights of the citizens of Oregon against unreasonable search or seizure. Or. Const. Article I §9; *State v. Davis*, 295 Or 227, 666 P2d 802 (1983). Suppression is the remedy that vindicates those rights. *State v. Rodriguez*, 317 Or 27, 854 P2d 399 (1993).

ASSIGNMENT OF ERROR NO. 2

The trial court erred when, during the hearing on defendant's Demurrer, it denied the defendant the opportunity to offer evidence as follows:

MR. SUSSMAN: At this point I'd like to call Norman Kirth. 7/1/94 Tr. 13 ll. 6-7.

///

MR. TINTERA: Your Honor, I'm going to object to taking any testimony. It's my understanding that a demurrer is purely a legal issue. It does not require the production of any facts * * * 7/1/94 Tr. 13 ll. 8-11.

THE COURT: Sustain the objection. 7/1/94 Tr. 15 l. 13.

ARGUMENT

The prosecutor relied on *State v. Waldo*, 93 OrApp 613, 763 P2d 417 (1988) and *State v. Reed*, 116 Or App 58, 840 P2d 723 (1992) for the proposition that "the case law supports the proposition that facts are not to be considered at the trial court level in regard to a demurrer." 7/1/94 Tr. 13. Those cases are inapposite to this case. Both *Waldo*³⁴, and *Reed*, involved attempts by the defense to raise what were, in effect, defenses on the facts by way of demurrer by asking the court to analyze extrinsic facts in evaluating the sufficiency of the indictment. The demurrer in this case alleged that the statute which established the elements of those offenses **as charged against the defendant** was constitutionally flawed, not that the allegations were insufficient to state the offenses charged. ORS 135.630(5) provides the statutory basis for that demurrer.

In *State v. Moeller*, 105 OrApp 434, 806 P2d 130 (1991) rev. dismissed, 312 Or. 76,

³⁴The opinion cited *State v. Kurtz*, 46 OrApp 617, 624, 612 P2d 749 (1980), which in turn cites *State v. Gates*, 31 OrApp 353, 356, 570 P2d 670 (1977). Both those cases dealt with demurrers which alleged defects in the indictment. This demurrer alleged defects in the statute.

815 P2d 701 (1991), the defense offered the testimony of prosecutors from various counties around the state on their interpretation of the "scheme or network" language from the former OAR chapter 253, Division 4, appendix 4, in order to demonstrate that the challenged provision was unconstitutionally vague. The trial court was not required to "analyze" that extrinsic evidence. It was offered to illuminate the breadth of the statutory terms.

///

The same was true here. The defense challenged the statutory terms "alter" and "without authorization" as being unconstitutionally vague. The evidence was offered on the term "alter," which is not defined in the statute. Defense counsel, in what turned out to be an offer of proof, explained that the testimony of the expert computer systems engineer would show industry standards and how the statute's provisions would affect routine practices. App- 9. It would also provide a basis for determining whether the statute impermissibly proscribed permissible or protected conduct. 7/1/94 Tr. 13-15.

In *State v. Graves*, 299 Or 189, 700 P2d 244 (1985),³⁵ as in the case at bar, the statutory term was not defined by statute and was susceptible of any number of possible meanings. Those possible meanings, in the context of the use of computers, were the subject of the proffer of evidence. It was error to refuse to permit it and, as will be illustrated in the following Assignment of Error, the error was prejudicial and substantial, leading the court into even more serious error.

ASSIGNMENT OF ERROR NO. 3

The trial court erred when it denied defendant's Demurrer as follows:

* * * [T]his is not a first amendment issue . . . * * * In this particular case the two key words [in the statute] are alter and access. Access is defined in the statute, alter is not. Access, being defined by the statute has a very specific legal

³⁵The reference to *Graves* is not without some irony. In that case, the state offered, and the court admitted, the testimony of two police officers to the effect that screwdrivers were "commonly used" as burglar's tools in an ultimately unsuccessful attempt to defeat the defendant's demurrer based on the claim that the words "commonly used" were unconstitutionally vague. In this case, the state opposed the offer of any extrinsic evidence on any demurrer regardless of the grounds.

meaning. This meaning may be quite different from the average understanding of the word. In this particular case it's (sic) definition is directed specifically toward issues around computers and computer systems. Alter is not statutorily defined and therefore carries its usual and customary meaning. This meaning is different from the statutory definition of access.

When read as a whole, this statute is sufficiently clear for any particular individual to determine if their behavior constitutes a crime. * * * This particular statutes (sic) describes at least two different ways of committing a crime. One is to access a computer system for the purpose of doing some other bad act. Another way is to knowingly alter or damage a computer system when the individual knew he had no authorization to take such action. * * * App-6 to App-7.

I. VAGUENESS

A. Alter and Access

A criminal law is impermissibly vague if it is written so that it does not adequately distinguish between what conduct is permitted and what conduct is not. *State v. Moeller*, supra. In *State v. Hodges*, 254 Or 21, 27, 457 P2d 491 (1969), the Supreme Court said:

A law that permits the judge and jury to punish or withhold punishment in their uncontrolled discretion is defective as much for its uncertainty of adjudication as for its failure to notify potential defendants of its scope and reach³⁶.

* * * A vague statute lends itself to an unconstitutional delegation of legislative power to the judge and jury, and, by permitting the jury to decide what the law will be it offends the principle, if not the rule, against *ex post facto* laws. See Oregon Constitution, Art. I §.21"

The court here held that "alter" and "access" are two key words in the statute.³⁷ The statutory term "alter" is not defined.³⁸ It is the term in question here, since defendant was

³⁶One of the purposes of the Oregon Criminal Code is "To give fair warning of the nature of the conduct declared to constitute an offense and of the sentences authorized upon conviction." ORS 161.025(1)(c).

³⁷The statute in question, ORS 164.377(3), provides: "Any person who knowingly and without authorization alters, damages or destroys any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime."

³⁸The definition of "access" is in ORS 164.377(1)(a). "To 'access' means to instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system or computer network."

not charged with improper "access." As was noted by the court, the term "alter" must mean something different than the term "access," unless the legislature has performed a superfluous or meaningless act. The courts are generally not permitted to conclude that the legislature has done a superfluous or meaningless act. ORS 174.010; *1000 Friends of Oregon v. Wasco Co.*, 399 Or 344, 703 P2d 207 (1985); *Union Pacific R. Co. v. Bean*, 167 Or 534, 119 P2d 575 (1942).

The court held that the term "alter" in ORS 164.377 carried its usual and customary meaning. The problem is that the usual and customary meaning is the equivalent of "to change" or "to make different." *The Merriam-Webster Dictionary*. "Alteration" is defined as "a change of a thing from one form or state to another, making a thing different from what it was without destroying its identity." *Black's Law Dictionary*, 5th Edition, page 40.

If the word "alter" simply means "change," it is difficult to distinguish that normal, well-recognized meaning from at least some of the meanings given by the legislature to the word "access." Typing even one letter or number on the keyboard of an operational computer uses its resources, regardless of whether it is running a word-processing program, a graphics program, a spreadsheet or a CAD program. Storing data "changes" the computer. Virtually anything you do to a computer alters it. 7/14/95 Tr. 128-129, Tr. 140 ll. 23-25.

The data in a computer cannot be changed without communicating with it, instructing it, adding to or retrieving from its data and/or without using its resources. That is the same as "accessing" the computer according to the statutory definition of the term "access." While the court held that the term "alter" meant something different from the term "access," the court did not say what that difference was. In fact, as assigned as error above, the court prohibited the defense from proving that one must "alter" a computer to "access" it, and one must "access" a computer to "alter" it. An overabundance of possible interpretations and meanings which may be given to statutory terms is one of the hallmarks of an unconstitutionally vague statute. *State v. Graves*, supra.

Second, if the "usual and customary meaning" construction is adopted,³⁹ it is so all-encompassing that its effect is to criminalize both socially tolerable and socially intolerable conduct. For instance, an employee installing and playing of computer games on the company hard disk over the lunch hour without the express permission of the employer is clearly within the meaning of the statute given that construction.

During his argument on the demurrer, the prosecutor in this case admitted that the statute would reach utterly innocuous behavior:

* * * And, you know, Mr. Sussman says well, it could be so much as altering the color of a screen. The fact of the matter is if you want to do that and you're not authorized, I suppose you could be subject to criminal prosecution under this law.

7/1/94 Tr. 27 l. 25 - Tr. 28 l. 4.

While it may, in some circumstances, be inappropriate, changing the color on a computer screen is most emphatically not a permissible focus of the criminal law. In *State v. Sanderson*, 33 OrApp 173, 575 P2d 1027 (1977), the Court of Appeals held that a statute which prohibited "Engag[ing] in a course of conduct that alarms or seriously annoys another person and which serves no legitimate purpose" was unconstitutionally vague because it provided no basis to distinguish between socially tolerable conduct, e.g., consistently appearing late for social appointments, and the antisocial conduct intended to be prohibited, such as the making of obscene telephone calls. 33 OrApp at 176-177.

This "well-recognized meaning" construction of the word "alter" illuminates another problem with the statute: **There is no requirement that anyone be harmed.** This is underscored by the statutory language itself; "damage" to "any computer, computer system, computer network, or any computer software, program, documentation or data" is punishable independent of any alteration. Alteration and damage, separately delineated in the statute, are alternate ways of committing computer crime. See *State v. Tidyman*, 54

³⁹ The legislative history suggests that the law was aimed, primarily, at outside "hackers" calling in to a system maintained by a business and either securing information or manipulating data in aid of competition with that business.

OrApp 640, 650, 635 P2d 1355 (1981).

One of the consistent features of unconstitutionally vague criminal laws is that there is no requirement that harm occur. *State v. Blair*, 287 Or 519, 524, 601 P2d 766 (1979) (nullifying a statute which proscribed "harassment" by means of telephone calls to named persons in a manner both intended and "likely to cause annoyance and alarm").⁴⁰

This flaw is compounded when the definition of "computer" is considered:

"Computer" means, but is not limited to, an electronic device which performs logical, arithmetic or memory functions by the manipulations of electronic, magnetic or optical signals or impulses, and includes all input, output, processing, storage, software or communication facilities which are connected or related to such a device in a system or network." ORS 164.377(1)(b).

This definition must be considered in any attempt to interpret or construe the computer crime statute itself.

In interpreting a statute, the court's task is to discern the intent of the legislature. * * * To do that, the court examines both the text and context of the statute* * * the text of the statutory provision itself is the starting point for interpretation and is the best evidence of the legislature's intent. * * * Also* * *, the court considers the context of the statutory provision at issue, which includes other provisions of the same statute and other related statutes.

Also at the first level of analysis, the court considers the context of the statutory provision at issue, which includes other provisions of the same statute and other related statutes. (Citations omitted). * * * 317 Or at 611.

Portland General Elec. Co. v. Bureau of Labor and Industries, 317 Or 606, 610-11, 859 P2d 1143 (1993).

The definition of "computer" is part of the same statute. Most phone systems easily

⁴⁰Also, see, *State v. Ray*, 302 Or 595, 733 P2d 28 (1987) (telephone harassment statute which permitted jury to decide which calls were, and were not, obscene unconstitutionally vague and overbroad); *State v. Spencer*, 289 Or 225, 611 P2d 1147 (1980) (statute which criminalized speaking with intent to cause "public inconvenience, annoyance or alarm," whether such results actually occurred or not, unconstitutionally vague).

qualify under this definition, even without the "is not limited to" language. Indeed, most modern thermostats also qualify, and many employers, rightfully and with good reason, forbid changing the setting. But may fiddling with the office thermostat without the employer's permission be made a crime? More absurdly, since the statute also forbids unauthorized "access" to "computers", an employer could deny employees authorization to look at the thermostat and, under the statute, to do so would become a crime.

B. Authorization

The term "authorization" is also, as previously noted, undefined. To authorize, of course, generally means "to give a right or authority to act" or "to permit a thing to be done in the future." *Black's Law Dictionary*, 5th Edition, page 69. "Authority" is seen as "permission." *Ibid*, page 68. *Black's* lists a number of kinds of "authority," including apparent authority, authority by estoppel, authority coupled with an interest, general authority, implied authority, incidental authority, inherent authority, limited authority, special authority and naked authority. The problem with ORS 164.377 is that contains no standards for the determination, on any objective basis, of what sort of "authorization" is required, nor does it identify the **source** from which the authorization must originate. This omission distinguishes ORS 164.377(3) from virtually every other section of the Oregon Revised Statutes where the term "authorization" is used to mean "permission." Appendix A to defendant's demurrer in the trial court contains a list of the statutes involving the term "authorization" and the respective, designated source(s) and/or kinds of the authorization(s) required.

So the hapless engineer or programmer is left to guess, at his peril, whose permission he must seek if he is to "change" the data in the memory of a computer, and, in addition, what sort of permission it must be if he is to be safe from criminal prosecution. If he guesses wrong, prosecution may still ensue, but may not. This case provides an excellent, concrete example of why this term in this particular statute, without modifiers, fits the vagueness criteria to a "T." Schwartz answered directly to Robert Wilcox. 7/13/95 Tr. 94 ll. 4-5, Tr. 101 l. 20 - Tr. 102 l. 1. Schwartz was hired to monitor computer networks with UNIX

workstations. 7/13/95 Tr. 94 ll. 16-17. This requires an expert, and Schwartz's direct supervisor, Wilcox, was not an expert in that area. 7/13/95 Tr. 94 ll. 20-22. But Schwartz is. 7/13/95 Tr. 95 ll. 19-21; Tr. 123 l. 22- Tr. 124 l. 1.

The inevitable consequence was that none of the changes (read alterations) wrought by Schwartz in the ordinary course of his employment were "authorized" by anyone. He was hired by his supervisor for his expertise; expertise which the supervisor did not possess. Wilcox **relied** on Schwartz's expertise. 7/13/95 Tr. 124. In fact, Wilcox made it clear that **it is the systems administrators themselves** who know what is to be done and not to be done. 7/13/95 Tr. 102 ll. 2-14.

Schwartz's jobs were to administer the UNIX computer systems, to put them on the Intel network and see to it that they ran harmoniously with the rest of that network, to install network monitoring software and to "automate the administration of the network." 7/13/95 Tr. 95-97. This activity, by definition, involves altering the network. 7/13/95 Tr. 97-102. Yet no supervisor "authorized" what changes he made on a day-to-day, minute-to-minute basis.⁴¹ Nor did any supervisor have the authority to do so. Intel manages its independent contractors only as to results, not as to the means used to achieve them.⁴² 7/13/95 Tr. 120; Defendant's Ex. 106. In fact, the lack of control over the activities of independent contractors in the high tech industry is industry-wide. Patrick Reilly, co-founder of Isoqwan Technology which develops software for leading edge wireless communications systems, hired Schwartz as an independent contractor. 7/18/95 Tr. 111-12, 115. As an independent contractor, Reilly did not attempt to exercise control over what Schwartz did. He would "[g]ive him a broad task and tell him 'make it work' and not really be concerned about how he did it." 7/18/95 Tr. 119-120.

The way the statute reads, **any** alteration of a computer must be authorized. It is not tenable under either the Constitution of the State of Oregon or the Constitution of the

⁴¹This was illustrated again by the testimony on cross examination of Herb Mayer, the manager who hired Schwartz to perform some work on Brillig. 7/18/95 Tr. 88 l. 23 to Tr. 89 l. 15; Tr. 89 l. 25 to Tr. 90 l. 2. App-9-10.

⁴²This magnifies the danger of *ex post facto* application.

United States that an element of a crime be so ad hoc. *State v. Graves*, supra; *Giaccio v. Pennsylvania*, 382 US 399 (1966). It is another touchstone of unconstitutional vagueness. *Grayned v. City of Rockford*, 408 US 104 (1972). Not knowing from whence the requisite authorization must come, it is impossible to determine what kind of authorization it must be. Will apparent authority constitute a defense? Is implied authority enough? The statute contains no clue.

In *Galley v. Babb*, 50 Or App 617, 624 P2d 616, rev. den. 291 Or 117 (1981), an ordinance banning drug paraphernalia was struck down as unconstitutionally vague. The court said:

The city argues that the generality of the description can be cured by expert testimony at a trial for violation of the ordinance. The contention appears to be that recognized experts can determine if a particular item is used or intended for use in the illegal preparation or administration of drugs. By this method, the city argues, a judge or jury can be informed as to the character of the item the accused is charged with manufacturing, selling or delivering. The difficulty with that argument is that it is the antithesis of the requirement that a penal ordinance or statute inform the public and law enforcement personnel of the standard of conduct required. The ordinary citizen should not have to depend on the testimony of an expert at trial to determine if his conduct is prohibited by the ordinance. The law enforcement agencies must also have standards of enforcement in order that enforcement of the ordinance will not be arbitrary or capricious. Expert testimony presented in the adversary setting of a trial does not provide standards for the persons whose conduct is sought to be regulated or the police charged with enforcement of the ordinance. 50 Or App at 629.

Second, the potential for criminal prosecutions based on after-the-fact, ad hoc decisions by middle level corporate managers, among others, makes this term particularly susceptible to ex post facto application due to the lack of definition and standards. This potential is one of the main signals of fatal vagueness. *State v. Graves*, supra.

Another example of the vagueness of the term "without authorization" as applied in this case occurred in connection with the "alteration" of the computer named Mink by installation of the "gate" program which, according to the search warrant affidavit, bypassed Intel security systems. Dirk Brandewie, Schwartz's supervisor at the time, testified that what he actually told Schwartz about this program when he first discovered it was that it was not "secure enough." 7/18/95 Tr. 36 ll. 9-12. That does not mean it is not "authorized;" that means it is not secure enough. That was in March, 1993. 7/18/95 Tr. 8.

Later, after Schwartz had experimented with the program some more, Brandewie told him that he would require a waiver from Intel security to allow it to run on Mink, and Schwartz told Brandewie that if Schwartz could not use the program in its current form it was not useful to him and to close the account on Mink. 7/18/95 Tr. 14-15. No disciplinary action was taken against him for either incident. 7/18/95 Tr. 47 ll. 5-7. On 3-2-94, the Washington County Grand Jury decided that, somewhere along the line, Schwartz had committed Computer Crime, at least partly on account of those events. Indictment, Count 1.

Brandewie admitted that his computer system's security arrangements was based on Intel policy **as he understood it**. 7/18/95 Tr. 42 ll. 19-24. Thus, when he was talking to Schwartz about security policy, what he said had only to do with **his** computers. He had no idea whether policy manuals had been distributed to other employees, much less independent contractors.⁴³ 7/18/95 Tr. 43. Cower expressed doubt that security manuals had been distributed to independent contractors. 7/18/95 Tr. 173 ll. 11-17.

In fact, Schwartz had been directed to create a working port reflector⁴⁴ when he worked as a system administrator at IWARP.⁴⁵ 7/19/95 Tr. 123-124. The practice then was that machines that were accessible by internet did not have sensitive, proprietary information.

⁴³Morrissey testified in another context that the methods used by Intel were, to a very large extent, "ad hoc" and do not fully "close the loop." 7/14/95 Tr. 215 ll. 19-21.

⁴⁴A program that would accept internet connections from outside of Intel. The "gate" program was a port reflector, according to Brandewie. 7/18/95 Tr. 11 ll. 3-19.

⁴⁵One of the divisions that eventually became part of SSD. 7/19/95 Tr. 121 ll. 8-17 (testimony of James Reinders).

7/19/95 Tr. 125 ll. 6-15. The two-way access was critical to getting the job done. 7/19/95 Tr. 126 ll. 3-8. Schwartz helped see to security. 7/19/95 Tr. 126 ll. 12-13; Tr. 127 ll. 17-20. Inbound telnetting from the internet was still permitted on some Intel machines, despite this company-wide "policy," at the time of the trial. 7/19/95 Tr. 130 ll. 6-9.

Yet another example of the nebulous and subjective nature of "authorization" in this context is that it was generally against company policy, i.e., "unauthorized," for independent contractors to be system administrators. 7/18/95 Tr. 64 l. 23 to Tr. 65 l. 5. That policy was, up to and including the time of the trial, routinely ignored. 7/18/95 Tr. 65 ll. 6-11. Schwartz worked as a system administrator there for years. 7/18/95 Tr. 65 ll. 12-15. The Information Technology Manager at SSD saw that as a fundamental violation of company policy. 7/18/95 Tr. 65 ll. 22-24. Thus, from his point of view, Schwartz's employment by Intel was "without authorization." Yet Intel routinely paid the bills he sent, and routinely accepted the fruits of his labor.

So what was "authorized" and what was not was a matter of time, place and expediency. Criminal liability, or the lack of it, cannot be based on such flexibilities, because to do so violates basic due process principles, as well as Article I § 20 of the Constitution of the State of Oregon.

II. DEFINITENESS AND CERTAINTY

Defendant also demurred to Count 1 of the indictment on the ground that it was not definite and certain. ORS 135.630(6).

The specificity requirement for indictments is found both in statute, ORS 133.015(7), and the state and federal constitutions. *State v. Cooper*, 78 OrApp 237, 239-40, 715 P2d 504 (1986). Article I, §11 of the Oregon Constitution provides that an accused has the right to demand the nature and cause of the accusation against him. See, *State v. Green*, 245 Or 319, 422 P2d 272 (1966); *State v. Cooper*, *Supra*, *State v. Jim/White*, 13 OrApp 201, 508 P2d 462 (1973). The due process clause of the Fourteenth Amendment requires that an indictment describe an offense with sufficient precision and certainty to enable a presumptively innocent person to prepare for trial. *Barber v. Gladden*, 327 F2d 101 (9th

Cir.), *cert den* 377 US 971 (1964), *State v. Cooper*, 78 OrApp at 239-40.

The availability of discovery may not save an unspecific accusatory instrument from a challenge on specificity grounds. *State v. Sanders*, 280 Or 685, 572 P2d 1307 (1977). A complaint which does not set out the specific facts that the State intended to rely upon to prove a statutory violation can fail to be definite and certain and to state an offense, even if plead in the terms of the statute. *State v. Cooper*, 78 OrApp at 240-41.

For the reasons discussed above, the terms "alter" and "without authorization" in ORS 164.377(3) are unconstitutionally vague. As a result of their vagueness, the allegation in Count 1, that defendant ". . . did unlawfully, knowingly and **without authorization alter** a computer and computer network. . .", lacked the requisite specificity to provide defendant with the degree of notice of the criminal conduct the State intended to prove, which was necessary in order to enable him to prepare his defense for trial. *Barber v. Gladden*, supra; *State v. Kincaid*, 78 OrApp 23, 714 P2d 624 (1986). Moreover, these terms, as used in ORS 164.377(3), cannot be saved by a judicial interpretation because the statute has no foundations upon which to base a narrowing construction as in *State v. Yancey*, 32 OrApp 477, 574 P2d 358 (1977) (scienter requirement held to modify each other element which saved statute from being held unconstitutionally vague) .

The only conceivable construction that could save the statute is to read the word "alter" to mean: "To permanently erase data from the memory of the computer, computer system or computer network." Any other construction either 1) runs afoul of the definition of the statutory term "access" (which includes to store data **in** the memory or retrieve it, but does not include to erase it) or 2) leaves the reader so far out at sea that he has no idea what behavior violates the statute and what behavior does not. The first option is not available because it requires the court to declare either the term "alter" or the term "access" redundant. The second option renders the statute is unconstitutionally vague.

The difficulty with the "erasure" construction is that if the legislature had erasure in mind, the statute could easily have included that term. It did not, and the courts are strictly limited in what they may do by way of limiting construction. In short, courts may not

legislate. *State v. Robertson*, 293 Or 402, 408, 649 P2d 569 (1982); *State v. Moeller*, supra. Nor are they required to engage in tortured analysis or to amend a legislative enactment by inserting definitions and limitations or deleting terms enacted. *Galley v. Babb*, supra, 50 OrApp 628.

Indeed, because the common usage of both terms is so broad, there is nothing in Oregon law to provide guidance for an interpretation of the terms and this court would be required to fashion a definition, which would be tantamount to legislating. This is clearly not permissible.

ASSIGNMENT OF ERROR NO. 4

The trial court erred when it denied defendant's Motion for Judgment of Acquittal as follows:

* * * The jury could find this is a high-tech version of taking a TV set and putting it in a dumpster with the idea of coming back later that night and taking it out. I know that's sort of a simple comparison, but factually, it's very close to what Mr. Tintera has attempted to prove here. 7/19/95 Tr. 51 ll. 16-21.

* * * *

I do believe the evidence that has been produced here on all three counts is sufficient for the case to go forward and I'm denying the motion on all three counts. 7/19/95 Tr. 52 lines 9-12.

ARGUMENT

At the end of the state's case, the defendant moved for judgment of acquittal as follows:

MR. SUSSMAN: Well, Your Honor, I think there is no evidence that that -- theft requires that the State prove or the elements are that somebody take property which -- for the intent of appropriating it to themselves or with the intent to permanently deprive the owner of the usefulness of that. And in this particular case, there is -- a password and password file are information and are not objects which are subject to theft. That the theft statute does not fit the circumstances that you have or conditions that were created by copying and running a password -- running a Crack program on a password file. * * * And secondarily, the evidence is lacking that there was any purpose to commit, or intent to commit theft. * * * So on those grounds, that's the basis for my motion. 7/19/95 Tr. 51 ll. 7-24.

The trial court should have granted the defendant's Motion for Judgment of Acquittal on Counts 2 and 3, which charged violations of ORS 164.377(2)(c)⁴⁶, because nothing was

⁴⁶ (2) Any person commits computer crime who knowingly accesses,

taken, appropriated, obtained or withheld from Intel Corporation when Schwartz copied the password file from one Intel computer to another Intel computer. The evidence that both the SSD password file and its contents, i.e., the individual users' passwords, were still there and were actively doing their job after the copying occurred was not refuted or even challenged. 7/14/95 Tr. 131; 7/19/95 Tr. 69-70.

The state's express theory was that the acts of copying the file and running the password cracking program *on the copy* was an act of theft. 7/19/95 Tr. 11. The trial court agreed when it viewed defendant's acts as a high tech equivalent of an employee taking a television set and hiding it in a dumpster in order to steal it at a later time. App-13-15. Indeed, the prosecution argued that very proposition to the jury.

There is a critical difference in this case. When the store employee hides the television set, it is no longer on the shelf. No one can go over, turn it on and watch it. It is not available. But the password file was still at SSD and still working. All the individual passwords were still contained in that file, and the various users could log onto the system using them. The prosecutor anticipated this point and, when he was arguing to the jury, the best answer he had was that "the point" was that Schwartz had violated his position of trust and compromised the security of the Intel Corporation. 7/25 Tr. 26-27. However, that is not "the point." Schwartz was not charged with compromising the security of the Intel Corporation. He was charged with theft, and to commit theft one must take something from the owner or rightful possessor. The unassailable fact is that nothing was taken. Intel Corporation had everything after the SSD password file was copied that it had before the

attempts to access or uses, or attempts to use, any computer, computer system, computer network or any part thereof for the purpose of:

* * * *

(c) Committing theft, including, but not limited to, theft of proprietary information.

In pertinent part, ORS 164.015 defines "theft" as follows:

A person commits theft when, with intent to deprive another of property or to appropriate property to the person or to a third person, the person: (1) Takes, appropriates, obtains or withholds such property from an owner thereof; . . .

SSD password file was copied.

ORS 164.377(2)(c) does not apply to the acts which are alleged in Counts 2 and 3 of the indictment in this case. The facts established at trial, did not support a guilty verdict on those counts precisely because the acts admittedly done by Schwartz do not violate the section of the computer crime statute that was the basis of his conviction.⁴⁷ In short, the evidence did not support the verdict. ORS 136.445. The trial court should have granted defendant's Motion for Judgment of Acquittal on Counts 2 and 3.

ASSIGNMENT OF ERROR NO. 5

The trial court erred when it ordered restitution as follows:

There are special damages that could be recovered and I am going to order that restitution to Intel for those expenses, after deduction of the amounts that we've talked about for Mr. Stites, they now total \$59,692 will be recovered and they are the amounts of restitution.

* * * *

* * * Those amounts leave \$8,779.45 for the expense of the Miller, Nash firm in advising Intel in this rather complex matter and the total of those two amounts, the direct expenses incurred by Intel plus the outside counsel expense total \$68,471.45, if my math is correct.

And I find that those are pecuniary losses suffered by Intel as a result of the actions of the defendant. His actions directly caused that expenditure of money and that is a pecuniary loss that may be recovered by them and I find that that amount actually has been incurred as damages by the Intel Corporation.

ARGUMENT

ORS 137.106⁴⁸ allows a court to order restitution when a person's criminal activities have resulted in pecuniary damages.⁴⁹ There must be a causal relationship between the

⁴⁷More likely, this aspect of the case is one of the implications of criminally prosecuting a person when the most serious consequences of his actions should have been termination of his personal service contract.

⁴⁸ ORS 137.106 provides: Restitution to victims; criteria; objections by defendant. (1) When a person is convicted of criminal activities, or a violation under ORS 161.565, **which have resulted in pecuniary damages**, unless the presentence investigation report contains such a presentation, the district attorney shall investigate and present to the court, prior to or at the time of sentencing, evidence of the nature and amount of **such** damages. In addition to any other sentence it may impose, the court may order that the defendant make restitution to the victim. (Emphasis added).

⁴⁹ORS 137.103(2) defines "pecuniary damages" as "all special damages, but not general

crime and the damages. *State v. Dillon*, 292 Or 172, 181, 637 P2d 602 (1981). The state has the burden to prove that the amounts requested for restitution are justified because they were losses actually caused by the activities of the defendant. *State v. Lefthandbull*, 306 Or 330, 758 P2d 343 (1988).

Restitution is not the equivalent of an award of damages in a civil case. There are no general or punitive damages, and a defendant cannot be ordered to pay more than he is able to pay. *State v. Hart*, 299 Or 128, 139, 699 P2d 1113 (1985); *State v. Dillon*, supra, 292 Or at 179-180. This basic rule was lost on the state. At the beginning of the restitution hearing,⁵⁰ the state argued that the purpose of the hearing was "putting Intel in a monetarily whole state after the damage that Schwartz has inflicted on the company." 1/8/96 Tr. 3 ll. 2-5.

I. Attorneys Fees

Intel sought the services of outside counsel on several aspects of this case. 9/11/95 Tr. 5 ll. 1-13. The state relied on the case of *State v. Mahoney*, 115 OrApp 440, 838 P2d 100 (1992) for the proposition that the fees which Intel paid outside counsel were recoverable as restitution. 1/8/96 Tr. 3 ll. 11-12.

There is an apparent conflict in Oregon law over whether attorney's fees can be recovered under the restitution statute. *State v. O'Brien*, 96 OrApp 498, 774 P2d 1109, rev. den. 308 Or 466, 781 P2d 1214 (1989), which held that they are not recoverable, was cited with approval in *Raymond v. Feldmann*, 124 OrApp 543, 548-49, 863 P2d 1269 (1993):

In *Samuel v. Frohnmayer*, 95 OrApp 561, 770 P2d 914, rev'd on other grounds, 308 Or 362, 779 P2d 1028 (1989)], the plaintiff sought "damages" for the "attorney fees" incurred in seeking a declaratory judgment that the state was obligated to indemnify him in an action brought against him in his capacity as a state agent. He

damages, which a person could recover against the defendant in a civil action arising out of the facts or events constituting the defendant's criminal activities and shall include, but not be limited to, the money equivalent of property taken, destroyed, broken or otherwise harmed, and losses such as medical expenses and costs of psychological treatment or counseling."

⁵⁰The state was allowed two opportunities to prove its restitution claim. When it appeared that the state's burden of proof had not been met after the sentencing hearing, the trial court set a later restitution hearing to allow the state to provide evidence to in support of the restitution claimed. 9/11/95 Tr. 58- 59.

argued that the damages were the "direct and foreseeable consequence of defendant's breach of his statutory duty to defend and indemnify [him]." We said that what the plaintiff characterized as "damages" were in fact "attorney fees." In denying relief to the plaintiff, we reasoned:

" 'Damages' that are determined by the charges that an attorney makes for services in the action in which those damages are sought are attorney fees, although fees incurred in maintaining a lawsuit may at times be damages in some other action. 95 OrApp at 563, 770 P2d 914." (Emphasis in original.) See also, *Sizemore v. Swift*, 79 OrApp 352, 358, 719 P2d 500 (1986).

In *State v. O'Brien*, [supra], we relied on our holding in *Samuel*. We held that the trial court erred in requiring defendant to pay restitution for attorney fees incurred by the victim in pursuing civil claims against defendant. The court was authorized to impose only those special damages which the victim could recover in a civil action against the defendant. We held:

"Attorney fees are not considered damages when sought in the same action in which the services are rendered. However, they may be damages when sought in a separate action. Here, the victim could have recovered attorney fees in a breach of contract action. However, if recovered in that action, they would not have been considered damages. Therefore, under ORS 137.103(2), attorney fees are not 'special damages' recoverable in a civil action arising out of defendant's criminal conduct and, accordingly, are not recoverable as part of restitution." 96 OrApp at 505, 774 P2d 1109. (Citations omitted.) 124 OrApp 548-549.

The fact that *Raymond* post-dates *State v. Mahoney*, supra, by one year suggests that the Court of Appeals has *sub silentio* adopted the dissent of Judge Joseph in *Mahoney*, 115 OrApp at 444.

Second, even if some attorneys fees were assessable as restitution, it would be necessary to show that the fees were reasonable and necessary expenses caused by defendant's conduct. *State v. Dillon*, supra. Here, the state did not show this connection and the trial court ruled that defense counsel's attempt to inquire into that area was irrelevant. 1/8/96 Tr. 43.

Restitution for attorneys fees was assessed in the amount of \$8,779.45. 1/8/96 Tr. 82. The trial court excluded only the amount billed for research into the question of contact with members of the jury after the trial, 1/8/96 Tr. 79, leaving it to this court to "back out some of the numbers" if the total bill was not assessable as restitution. 1/8/96 Tr. 80.

II. Non-Recoverable Salaries and Expenses

Intel sought restitution in excess of \$70,000.00. The amount actually assessed, including the disputed attorneys fees, was \$68,471.45. 1/8/96 Tr. 82 l. 15. That amount included salaries and expenses for employees which the state did not show were actually incurred due to Schwartz's actions. The criminal activity must have "caused" the expense, and causation is met by applying a "but for" standard. *State v. Bullock*, 135 OrApp 303, 899 P2d 709 (1995).

When employees are "diverted" from their normal duties their salaries are assessable as restitution. *State v. Lindsly*, 106 OrApp 459, 808 P2d 727 (1991). Thus when Intel sought restitution for the salary of its security specialist, Clyde Stites, the state conceded that Stites' salary was not recoverable as restitution, because his activities on the case were encompassed in his job description. 1/8/96 Tr. 79 ll.17-22. That was clearly correct.

Yet the state secured restitution for Rich Cower's salary during the investigation. Exh. 1 to the Restitution Hearing. Cower's job also was in security. 6/14/95 Tr. 188 l. 19; Tr. 192 ll. 2-3; App-2 (Cower described in affidavit as "Network Security Specialist). His "opinion" on security issues was presented by the state as that of an "expert" during the state's rebuttal. 7/24/95 Tr. 49. If Stites' base salary for the time he was involved in the Schwartz affair was not assessable as restitution, then neither was Cower's. The trial court erroneously included that salary in the restitution amount assessed against Schwartz. 1/8/96 Tr. 80.

One of the expenses listed was related to the construction of case notebooks for trial. 1/8/96 Tr. 22. Another was for hardware and software purchased by Morrissey and then delivered to the Washington County Sheriff's office. 1/8/96 Tr. 39. The state offered no explanation of how Schwartz's conduct caused the necessity for those outlays.

Those expenses were not proper subjects for restitution in any event. The state is charged with prosecuting the case, not Intel. There is no authority for awarding a victim of a crime restitution for what essentially are expenses incurred to assisting the state in litigating the criminal case. The state offered no theory of civil liability to support a

recovery of these expenses as "pecuniary damage" as defined by ORS 137.103(2). *State v. Carillo*, 125 OrApp 52, 56, 865 P2d 379 (1993).

III. Employee Benefits

The restitution amount imposed by the court included the full cost to Intel for each employee as well as the expenses of those Intel employees involved in any part of the investigation and/or rectification of the activities of Randal Schwartz. 1/8/96 Tr. 25; Tr. 28. These "burdened" costs included taxes, benefits, and in some instances executive bonuses and stock participation. 1/8/96 Tr. 6. 14 ll. 5-6; ll. 8-17.

The state offered no evidence to show a causal connection between the activities which led to Schwartz's conviction and Intel's duty to pay taxes or employee benefits. *State v. Bullock, supra*. The trial court made no distinction between the "burdened" costs and those expenses directly related to the investigation, such as Cower's travel expenses, which clearly are assessable as restitution.

IV. Failure to Meet Burden of Proof

Intel had the details about hours spent and actions actually taken by all employees in connection with this matter. 1/8/96 Tr. 29. According to the schedule submitted by Intel (State's Ex. 2 on Restitution), hourly rates ranged from just over \$20 to \$41. Yet according to State's Ex. 1 on Restitution, Cower's hourly rate computes at approximately \$195 and Carlene Ellis, who was not mentioned in any police report or other official document, was billed at approximately \$250 per hour. There was no indication of what she did in relation to the case. These discrepancies were pointed out to the trial court. 1/8/96 Tr. 69. The state offered no evidence to support the claims for these salaries, and failed to meet its burden to prove that the restitution claimed was actually caused by the activities of the defendant. *State v. Lefthandbull, supra*.

If the victim of a crime suffers inconvenience, but no financial loss attributable to the crime, then there are no pecuniary damages and no restitution can be ordered. *State v. Heath*, 75 OrApp 425, 706 P2d 598 (1985). ORS 137.103(2) specifically restricts recovery to special damages and, therefore, applies only to expenses actually incurred and to those

expenses which are easily measurable. *State v. Barkley*, 315 Or 420, 435, 846 P2d 390 (1993).

Should Mr. Schwartz's conviction be affirmed, some of the expenses suffered by Intel are assessable against him as restitution. However, many of the costs and expenses claimed by Intel were either not proved to have been traceable to Schwartz's conduct or there was no evidence explaining how those costs were actually incurred correcting the results of that conduct.

ASSIGNMENT OF ERROR NO. 6

The trial court erred by denying the defense Motion to merge Counts 2 and 3 as follows:

With regard to Counts 2 and 3, there is the issue of merger. I'm of the opinion that they don't merge and the basis of that is * * * I'm of the opinion that Counts 2 and 3 allege separate acts and the evidence in this case was that they were separate acts and as a matter of fact, the dates alleged are different. One alleges and incident November 1st, 1993, and the other October 25th, 1993, so we have different acts, a little over a week apart, and they are separate crimes and although they do allege violations of the same statute, 164.377, Subsection 4, they are separate incidents and separate crimes and I'm going to sentence separately.

ARGUMENT

The defendant, before the time of sentencing, filed a Memorandum of Law Supporting Merger of Counts 2 and 3. Tr. Ct. File. The prosecutor argued in part, and the trial court found, that Counts 2 and 3 involved "separate timeframes." 9/11/95 Tr. 22 ll. 2-3. The "timeframe" in Count 2 is from 8-1-93 to and including 11-1-93. The "timeframe" in Count 3 is from 10/21/93 to and including 10-25-93. Thus, the so-called "separate timeframe" in Count 3 is wholly encompassed and contained within the "timeframe" in Count 2.

Additionally, there is no difference between the "Intel SSD's password file" (Count 2), and the "Intel SSD individual user's (sic) passwords" (Count 3). The "password file" is simply a grouping of data which is the sum of the individual users' passwords. 7/20/95 Tr. 108 ll. 21-22.

ORS 161.062⁵¹ provides, in pertinent part:

⁵¹ORS 161.067 addresses itself to the same subject matter and is, in pertinent part, identical. These statutes have been referred to as the "anti-merger statutes." *State v. Lyons*, 124 Or App

(1) When the same conduct or criminal episode violates two or more statutory provisions and each provision requires proof of an element that the others do not, there are as many separately punishable offenses as there are separate statutory violations.

* * * *

(4) When the same conduct or criminal episode violates only one statutory provision and involves only one victim, but nevertheless involves repeated violations of the same statutory provision against the same victim, there are as many separately punishable offenses as there are violations, except that each violation, to be separately punishable under this subsection, must be separated from other such violations by a sufficient pause in the defendant's criminal conduct to afford the defendant an opportunity to renounce the criminal intent. * * *

There is no merger, even if the offenses are part of the same episode or transaction, if proof of one includes proof of an element that is not necessary to prove in the other. *State v. Atkinson*, 98 OrApp 48, 777 P2d 1010 (1989); *State v. Zuniga-Ocegueada*, 111 OrApp 54, 824 P2d 427 rev. den. 313 Or 211 (1992). For purposes of merger under ORS 161.062 and ORS 161.067, elements of proof are controlled by statute, not the facts of the individual case; the issue is one of statutory comparison. *State v. Heneghan*, 108 OrApp 637, 816 P2d 1175 (1991) rev. den.; *State v. Sumerlin*, 139 OrApp 579, 584, 913 P2d 340 (1996); *State v. Nunn*, 110 OrApp 96, 821 P2d 431 (1991) rev. den. 313 Or 211 (1992); *State v. Wallock/Hara*, 110 OrApp 109, 821 P2d 435 (1991), rev. den. 313 Or 75 (1992).

The test for whether separate convictions should be entered is: "(1) Did defendant engage in acts that are 'the same conduct or criminal episode,' (2) did defendant's acts violate two or more 'statutory provisions,' and (3) does each statutory 'provision' require 'proof of an element that the others do not.'" *State v. Crotsley*, 308 Or 272, 278, 779 P2d 600 (1989).

Here, there is no difference in the statutory elements because both counts are charged under the same section of the same statute. Under the *Crotsley* test, it is of no consequence that one count charges intent to commit theft of a password and the other charges intent to commit theft of a password file, because the question is *statutory*, not factual. No *statutory* element is present in Count 2 that is not present in Count 3, and vice versa.

The only remaining question is whether copying the SSD password file and running the "Crack" program on the SSD password file was part of the same criminal episode. ORS 131.505(4) defines "criminal episode" as "continuous and uninterrupted conduct that establishes at least one offense and is so joined in time, place and circumstances that such conduct is directed to the accomplishment of a single criminal objective."

Schwartz denied that his objective was criminal. He testified that he was testing a new version of the password cracking program for use in his ongoing duties as a systems administrator. 7/21/95 Tr. 150-151. Still, Schwartz was convicted of having copied the SSD password file and then running "Crack" on the passwords in that file. He copied it in the first place, admittedly, to run "Crack" on it to see how many of the passwords were guessable. 7/21/95 Tr. 154. Both acts were clearly part of a single criminal episode. 7/21/95 Tr. 150-162. The convictions should have been merged.

CONCLUSION

For the reasons stated above, appellant respectfully submits that this Court should order the evidence secured through the execution of the search warrant suppressed, declare the terms "alter" and "authorization" in ORS 164.377 unconstitutionally vague, reverse the trial court's denial of defendant's Motion for Judgment of Acquittal of Counts 2 and 3 or, in the alternative, order them merged and reverse the trial court's restitution order.

Marc Sussman, OSB#77368
Attorney for Defendant-Appellant

CERTIFICATE OF SERVICE

I certify that on July 24, 1998, I served two certified copies of the forgoing *APPELLANT'S OPENING BRIEF* by mailing them to: Mr. Michael D. Reynolds, Solicitor General, Appellate Division, Department of Justice, 1162 Court Street NE, Salem, Oregon 97310

Dated this 24th day of July, 1998.

Marc Sussman, OSB #77368
Attorney for Defendant-Appellant

APPENDICES