

Monday, January 10, 2000, the Washington state governor, attorney general, auditor, also University of Washington officials and regents, received a prepublication notice from *Contra Cabal*. The notice introduced a new web site that contains a series of essays that refer to them and their official actions. It contained a declaration that *Contra Cabal* conforms to the journalism codes of conduct and ethics mainly tested by courts in both Great Britain and the United States of America. It also gave named individuals an opportunity to respond to charges affecting their reputation and moral character within ten days and before publication. That time has now expired and they have not responded in a civilized manner.

Instead, University of Washington officials have hacked and crashed the *Contra Cabal* computers. Hacking or cracking computers violates both state and federal law. This instance follows a succession of similar occurrences since *Contra Cabal* first published during 1992. Moreover, it clearly shows a documented pattern and practice of unlawful acts designed to prevent publication of reports about criminal activity by public officials.

A remarkable parallel exists between the activities of the University of Washington crackers and Kevin Mitnick. The authorities released Mitnick, the notorious computer hacker, January 21, 2000. He has spent almost five years in federal custody in Lompoc, California. Upon his release he immediately accused New York Times reporter John Markoff of a breach of journalistic ethics. Markoff covered the latter portion of the two-and-a-half-year pursuit of Kevin Mitnick and published an article about him entitled "Cyberspace's most wanted." He also covered the latter portion of the trial.

Markoff has stood by his reporting. He said that he found it really disappointing that in the past five years, and perhaps in the last twenty years, Mitnick had not learned anything. Especially, that he might have learned from all his time in prison not to break into other people's computers. The authorities had arrested Mitnick five times during the previous twenty years for similar computer hacking offenses.² Not surprisingly, a recent poll showed that 2614 people (62%) think Mitnick rates as a prankster and not as a criminal.³ Apparently, a majority among the nerds consider him a hero. However, he probably classifies more as a digital terrorist who exhibits a variety of psychopathic traits.

The behavior of Ronald A. Johnson, Vice President, Computers and Computing, University of Washington, and several people among his staff, differs little from that of Mitnick and his associates. They also have apparently learned nothing during the past five years. Gorged with political power and technocratic hubris they flaunt their bloated taxpayer-funded salaries and remain devoid of any social mores.

Last week, State employees at the University of Washington hacked into the Messaging Application Program Interface (MAPI) of the *Contra Cabal* computers. They used the Northwest

Link ISP server as a gateway. In addition, they entered the voice mail program through the US West telephone lines. Both these intrusions have since caused considerable damage and repeated computer crashes. Over an extended period, Johnson and his team have arbitrarily destroyed computer programs and databases that contained intellectual property belonging to other people.

Many computer users think they have nothing on their computers worth hacking. However, malicious hackers (or crackers) irrationally access and cause damage to unsecured computers claims a security expert and senior systems engineer. He said that recently hackers deposited payloads in about a half-dozen computers on his campus. These payloads contained instructions for remote hacking that could prevent future use of the network.⁴

University of Washington employees use the knowledge gained from prevention research to deposit computerized payloads. They reverse their own rules for computer protection. Almost five years ago they destroyed upwards of twelve years of academic research data. Later they deposited a payload that required reformatting the hard drive and reloading all the programs and data. That project took sixty hours.

Fantastic as these allegations may sound, one must remember that one deals with intellectual thugs who follow anarchist policies. They have no morals or ethics and, consequently, do not care about state or federal law. With new technologies, one may protect oneself more than in the past. However, not completely when adversaries have unlimited expert time and resources at their disposal provided by the taxpayer.

Filing complaints with a university that holds a mandate to investigate itself, which consistently finds no reasonable or probable cause at clandestine hearings, means that no due process exists on that campus. In fact, one of the UW computer hackers chaired a university investigating committee. Moreover, Christine O. Gregoire, the Washington State Attorney General, although informed five years ago about these criminal acts, continues to turn a blind eye to them. She neither responds to correspondence nor investigates the charges. In fact, her assistant attorneys general actively cover up unlawful activities at the university and thwart attempts to obtain due process of law. For example, former assistant attorney general Carol S. Niccolls (now executive assistant to the UW president) deliberately obstructed an ACLU investigation that found reasonable and probable cause for prosecuting the same allegations.

A complaint sent by certified mail January 31, 2000, to Seth P. Waxman, Solicitor General of the United States, cites UW officials. It requests a full and independent investigation of alleged federal crimes committed by state employees. Generally, the complaints allege that state employees have hacked into the *Contra Cabal* computers over a period of almost five years and violated federal law 18 USC § 1030(a)(5) and other sections of that title.

Contra Cabal classifies as a lawfully published Internet column that exposes academic and state corruption. Its content explores the murky depths of academic and state totalitarianism.

Published since 1992, it will soon appear as a web site. University officials have tried, without success, for almost five years to apply prior restraint to this writer through unlawful practices including computer fraud.

However, after possessing an international press card for more than forty years, this writer does not easily succumb to intimidation by Johnny-come-lately nerds. The web site will soon appear using backup offline computers beyond the reach of hackers. It will eventually contain all new and previously published work. However, the size and complexity of the overall project determine a practical need to publish periodically. Several hundred essays have reached stages of final copyediting, final investigation, validation, or verification.

Publishing in stages allows for complete verification and validation of facts. It also provides a practical way to protect the databases from a fifth attempt to destroy them. The site presently comprises four volumes numbered six through nine (volumes one through five published 1992-99 using electronic mail will eventually form part of the web site). Some essays result from excerpting from work previously published in journals. Other essays report new revelations that frequently occur during investigation of disclosures made by sources. Some will result from contributions by other writers.

Many delays in verification have occurred during the past two years because the Washington State Attorney General and the University of Washington continue unlawfully to deny access to public records. They use this tactic, and many other bureaucratic ploys, to cover up crimes at the University of Washington that the Attorney General should have prosecuted long ago.

The University of Washington continues to try to hack/crack then sabotage *Contra Cabal* computers and databases. Therefore, please report any unusual technical difficulties or suspicious occurrences to webmaster@contracabal.org for onward transmission to state and federal authorities. Meanwhile, Richard L. McCormick, President, University of Washington <rlm@u.washington.edu>, Governor Gary Locke <leslie.frank@gov.wa.gov>, and Attorney general Christine O. Gregoire <mariang@atg.wa.gov>, await readers' messages of consternation and disgust about the alleged unlawful behavior of Washington state employees.

1. Hackers. A person who illegally gains access to another's electronic system.
Crackers. Hackers who intentionally cause damage to another's electronic system.
2. Robert Lemos, Mitnick: I was manipulated, That's how hacker Kevin Mitnick feels after almost five years behind bars, *ZDNet News*. Updated January 21, 2000 3:41 PM PT.
3. *ZDNet News* (00-0127-1542 PST)
4. Florence Olsen, Any Computer Can Be a Launching Pad for Hackers, Security Expert Warns, *The Chronicle of Higher Education*, 21 Jan 00.

© Copyright 2000 by Paul Trummel
All Rights Reserved: 27 Jan 00/15:21 PST
Edition: #804-01-00-0130-1427
Feedback: webmaster@contracabal.org

Paul Trummel

PO Box 1854, Renton, WA 98057-1854, USA

VOX: 01 (206) 568-3137

EMAIL: trummel@nwlink.com

FAX: 01 (206) 568-3137

31 Jan 00/08:00

[By Certified US Mail]

The Honorable Seth P. Waxman
Solicitor General of the United States
US Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530-0001

Dear Mr. Solicitor General:

As an accredited journalist with more than forty years experience, I lawfully publish an Internet column that exposes academic and state corruption. Published electronically since 1992, it will soon appear as a web site. University of Washington (UW) officials have tried for almost five years to apply prior restraint to me. They have used unlawful methods that include computer fraud to cover up the violations of law about which I write. They have also convened kangaroo courts to deprive me of my university computer rights.

Monday, January 10, 2000, the Washington state governor, attorney general, auditor, also UW officials and regents, received a prepublication notice from me. It introduced a new web site that contains a series of essays that refer to them and their official actions. It also gave them an opportunity to respond to charges affecting their reputation and moral character within ten days and before publication. That time has now expired and they have not properly responded.

Instead, UW officials broke into my computers violating 18 USC § 1030(a)(5) and other sections of that title. This series of unlawful acts shows a pattern and practice of trying to prevent publication of my reports about criminal activity involving public officials.

Over an extended period, Ronald A. Johnson, Vice President, Computers and Computing, University of Washington, and his team have arbitrarily destroyed computer programs and databases that contained intellectual property belonging to me. Last week, state employees broke into the Messaging Application Program Interface (MAPI) of my computers. They used the Northwest Link Internet Service Provider (ISP) server as a gateway. In addition, they entered the software of my voice mail program through US West telephone computers and lines. Both these intrusions have damaged programs and caused computer crashes.

UW employees have used knowledge gained from prevention research to deposit computerized payloads. They have reversed the rules for computer protection. Almost five years ago they destroyed upwards of twelve years of academic research data belonging to me. Later they deposited a payload in my computer that required reformatting the hard drive and reloading all the programs and data. Repairs took sixty hours.

Filing complaints with a university that holds a mandate to investigate itself, which consistently finds no reasonable or probable cause at clandestine hearings, means that virtually no due process exists on that campus. In fact, one of the alleged UW computer hackers chaired a university investigating committee.

Moreover, Christine O. Gregoire, the Washington State Attorney General, although informed five years ago about these alleged criminal acts, continues to turn a blind eye to them. She neither responds to correspondence nor investigates the charges. In fact, her assistant attorneys general actively cover up these unlawful activities and thwart attempts to obtain due process of law. For example, former assistant attorney general Carol S. Niccolls (now executive assistant to the UW president) deliberately obstructed an ACLU investigation that found reasonable and probable cause for prosecuting the same allegations.

Many delays in verification and validation of my copy have occurred during the past two years because the Washington State Attorney General and UW continue unlawfully to deny me access to public records. They use this tactic, and many other bureaucratic ploys, to cover up crimes that I believe the Attorney General should have prosecuted long ago.

Please take the action prescribed by law and mount an independent investigation into the allegations that I have made. I possess documents that fully support them.

Sincerely,

Paul Trummel

International Federation of Journalists, Brussels (Press Card #GB 6929)

National Union of Journalists, London (Press Card #025057)

National Writers Union, UAW Local 1981/AFL-CIO

Society of Professional Journalists, Greencastle, Indiana (#491793)

Investigative Reporters and Editors (#21107)

Associate Professor, Communication and Rhetoric (Retired)

enc - Statement of Facts.

Statement of Facts

1. Beginning January 31, 1995, and continuing until the present time, University of Washington employees: **Oren W. Etzioni, Ronald A. Johnson, Edward D. Lazowska, Sandra S. Moy, James D. Nason, and Carol S. Niccolls**, aided and abetted by others both known and unknown, carried out several schemes to defraud **Paul Trummel** (the Complainant), and to obtain his intellectual property by means of false pretenses, representation, and promises, by:
 - (a) obtaining unauthorized access to databases on the University of Washington computers containing intellectual property belonging to the Complainant;
 - (b) obtaining unauthorized access to other computers belonging to the Complainant;
 - (c) stealing, copying, and misappropriating the Complainant's proprietary intellectual property defined as computer programs, also academic and journalistic databases.
 - (d) obtaining unauthorized access to computers belonging to an Internet service provider and a telephone company.
2. The Internet Service Providers and Educational Institutions involved:
 - (a) Northwest Link (NWL), an Internet Service Provider (ISP) headquartered in Bellevue, Washington. For a fee, NWL provides customers with computer user accounts that customers may use to access other computer systems on the Internet.
 - (b) US West (USW), a telephone company headquartered in Denver, Colorado. For a fee, USW provides customers with telephone services suitable for transmitting data using a computer, a telephone line, and a computer "modem" (a device that allows computers to communicate over telephone lines). This allows their customers to access other computer systems on the Internet.
 - (c) The University of Washington (UW), an educational institution located in Seattle, Washington. For a fee, UW provides students with computer user accounts that they may use to access other computer systems on the Internet using their own computers and commercial ISP accounts. UW also owns, maintains, and operates a number of computers for the authorized use of UW faculty, students, contractors, administrators and other authorized personnel and provides Internet access to authorized users.
3. During the time relevant to this complaint, the Complainant developed computer software, academic research, and investigative journalism data, that he maintained as highly confidential proprietary information. This proprietary information, communications, and computer software he lawfully stored in computers belonging to the University of Washington, Northwest Link, and on computers owned by him.
4. In order to circumvent computer security measures employed by the Complainant to safeguard his proprietary computer software and databases, the individuals named above needed to obtain user account information and corresponding passwords for the UW computers, the ISP computers, and the computers belonging to the Complainant. Then they could access these computers as part of the scheme to obtain his proprietary software and databases also to damage or destroy them.
5. The individuals named in this complaint, aided and abetted by others both known and unknown:
 - (a) used their state and federally funded positions with UW to access confidential records and obtained confidential computer user accounts and corresponding secret passwords on the University computers;
 - (b) aided and abetted by others known and unknown, used a variety of electronic mail techniques to obtain other user account information and corresponding passwords;

(c) intercepted and read private electronic mail (email) communications containing confidential, private, and personal information.

(d) used fraudulently obtained user account numbers and corresponding passwords to gain unauthorized access to the Complainant's computers and to computers belonging to Internet service providers, telephone companies, and educational institutions.

(e) concealed their identity, and to further avoid detection, some of them used "clone" telephones, computer modems, and Internet connections to access the Complainant's computers, databases, and Internet service provider;

(f) obtained initial unauthorized access to the Complainant's university accounts and computers then fraudulently obtained user accounts and passwords to circumvent security measures installed on the Complainant's computers. By this they prevented him from regularly using the equipment and accessing information stored in protected parts of the computer systems or in other authorized user accounts. Specifically, they ran unauthorized computer "hacking" programs on the computers of the Internet service provider and the University of Washington and altered or replaced the existing legitimate programs installed on the Complainant's computers. They circumvented computer security to obtain unrestricted access to the Complainant's user accounts, confidential information, and email stored on the Complainant's computers and in his authorized university accounts.

(g) disabled computer logs that ordinarily provide a record of the dates and times when a computer is accessed; and

(h) made unauthorized entries into computer systems invisible to computer department personnel responsible for maintaining and securing those computers.

(i) used University of Washington computers to store misappropriated and stolen proprietary databases and intellectual property belonging to the Complainant.

6. In the State of Washington and elsewhere, the named individuals aided and abetted by others known and unknown, for the purpose of executing the scheme described above to commit fraud and to obtain property by means of false and fraudulent pretenses, representations and promises, caused the following transmissions by wire communication in interstate and foreign commerce:

(a) used computers located outside Washington, knowingly, and without authorization, altered, damaged and destroyed information contained in, and prevented authorized use of, the Complainant's computers.

(b) In altering, damaging, and destroying information contained in, and preventing authorized use of, the Complainant's computers and databases caused losses to the Complainant aggregating at least \$5,000 in value during any 1-year period.

Oren W Etzioni
Associate Professor, Computer Science & Engineering
209 Sieg Hall
University of Washington
Box 352350
Seattle, WA 98195-2350

Telephone: 206 685 3035
Fax: 206 543 2969
Email: etzioni@cs.washington.edu

Ronald A Johnson
Vice President, Computing and Communications
240 Gerberding Hall
University of Washington
Box 351208
Seattle, WA 98195-1208

Telephone: 206 543 8252
Fax: 206 543 4641
Email: ronj@cac.washington.edu

Edward D Lazowska
Professor and Chair
Computer Science and Engineering
114 Sieg Hall
University of Washington
Box 352350
Seattle, WA 98195-2350

Telephone: 206 543 4755, 206 543 1695
Fax: 206 543 2969
Email: lazowska@cs.washington.edu

Sandra S Moy
Director, University Computing Services
Computing and Communications
4545 15th Ave NE, Room 112
University of Washington
Box 354842
Seattle, WA 98195-4842

Telephone: 206 543 4563
Fax: 206 685 4054
Email: sandy@cac.washington.edu

James D Nason
Professor, Anthropology
University of Washington
Box 353010
Seattle, WA 98195-3010

Telephone: 206 543 9680
Fax: 206 685 3039
Email: jnason@u.washington.edu

Carol S Nicolls
Executive Assistant to the President
Office of the President
302 Gerberding Hall
University of Washington
Box 351230
Seattle, WA 98195-1230

Telephone: 206 543 3083, 206 543 5010
Fax: 206 616 1784
Email: csn@u.washington.edu

Paul Trummel
PO Box 1854
Renton, WA 98057-1854

Telephone: 206 568 3137
Fax: 206 568 3137
Email: trummel@nwlink.com

Excerpts from United States Code

Title 18 - Crimes and Criminal Procedure

Part I - Crimes

Chapter 47 - Fraud and False Statements

Sec. 1030. Fraud and related activity in connection with computers

(a) Whoever -

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

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

(5)

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;

(b) Whoever attempts to commit an offense under subsection (a) of this I section shall be punished as provided in subsection (c) of this section.

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

(2)

(A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(C), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under [2] this subparagraph; and (3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and (3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and (B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(e) As used in this section -

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or

communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer -

(B) which is used in interstate or foreign commerce or communication;

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information, that -

(A) causes loss aggregating at least \$5,000 in value during any 1-year period to one or more individuals;

The term “copyright” protects rights to the intellectual property that Paul Trummel (Nmesis) has created and associated with *Contra Cabal*. It includes text, photographs, cartoons, and illustrations. It protects him against unauthorized use of his work and entitles him to benefit from that work. The term “moral rights” refers to attribution (bylines, credits). British law protects the author from derogatory treatment of, or alterations to, original material in any way that prejudices the author or his reputation. This includes editing in any way that distorts the original meaning or deliberately introduces mistakes.

No person or organization may use or reproduce in any form any part of *Contra Cabal* inconsistent with the author’s copyright or moral rights. This prohibition applies to unauthorized uses or reproductions, for public or private use. It applies to reproduction in any form or by any means, electronic or mechanical. This includes photocopying, printing, recording, information storage and retrieval, also all electronic applications. However, intending publishers may obtain a one-time publication license signed by the author. Publication of the same or similar material in other titles or electronic media, besides the medium covered by the original license, requires additional licenses.

Reviewers may extract brief quotations and embody them in critical articles and reviews published in printed periodicals or newspapers, without permission. However, both licensed publishers and reviewers must attribute the author. They must also send him a printed copy of the published article or review within thirty days of publication. No person or organization shall, by way of trade or otherwise, circulate any part of *Contra Cabal* without appending a reference to the publisher’s license. This condition also applies to subsequent sub-licensees.

The author employs the Authors’ Licensing and Collecting Society to collect reproduction fees from publishers for material published, in whole or in part, in any medium. Additional fees fall due from publishers for licensed rights beyond first use or for reprints in any printed or electronic media.

Paul Trummel

International Federation of Journalists, Brussels (Press Card #GB 6929)

National Union of Journalists, London (Press Card #025057)

Society of Professional Journalists, Greencastle, Indiana (#491793)

Investigative Reporters and Editors, Columbia, Missouri (#21107)

PO Box 1854, Renton, WA 98057-1854, USA

Vox: 01 (206) 568-3137. Fax: 01 (206) 568-3137

Email trummel@nwlink.com

© Copyright 1998 by Paul Trummel

All Rights Reserved: 27 Aug 98/12:19 PST

Edition: #004-01-00-0111-0605

Feedback: webmaster@contracabal.org