



WCCRC FOCUS

White Collar Crime Research Consortium
February 2003

PRESIDENT'S REMARKS

INSIDE

PRESIDENT'S REMARKS

RAND CRIMINAL JUSTICE REOR- GANIZATION

IDENTITY THEFT CASE

MEMBER NEWS

LEGAL BEAT

EVENT CALENDAR

NW3C RESEARCH SECTION

The White Collar Crime Research Consortium: Some Prospective Projects

by David O. Friedrichs, WCCRC President

What follows is a version of some brief remarks delivered at the bi-annual luncheon of the White Collar Crime Research Consortium, at the American Society of Criminology Annual Meeting, Chicago, on Friday, November 15, 2002.

The past year has arguably witnessed more sustained media and public attention to white collar crime (or an especially significant form of it) than has been true at any earlier time. It is my guess that there has been more sustained coverage of it than in the Progressive Era (trust-busting), the post-1929 New Deal Era, the Great Society Era of the 1960s and 1970s, and in connection with the Insider Trading and S & L scandals of the Reagan/Bush Era. Of course this is really a hypothesis that requires systematic investigation. But there can be no question that the series of allegations directed at Enron, WorldCom, Global Crossings, Adelphia, Tyco International, and other large corporations or their highest level executives since Fall 2002, add up to landmark events in the history of white collar crime in America. It remains to be seen whether these cases will produce a fundamental and enduring transformation in public consciousness about crime; enduring reforms and a basic shift in criminal justice system priorities; a broader inclusion of white collar crime courses in the criminology/criminal justice curriculum; and a new wave of research on white collar crime, leading to new understandings and insights.

These are exciting and challenging times for professional students of white collar crime. The White Collar Crime Research Consortium (WCCRC) can ideally play a role in fostering interest in, and a better understanding of, white collar crime and its control.

The Focus of the WCCRC and NW3C

More than one member of the WCCRC has shared with me a concern that NW3C (National White Collar Crime Center) has been principally focused upon various forms of fraud, but certainly not on larger scale white collar crimes such as corporate crime. I share this concern, but I see no reason why the focus of the NW3C couldn't be broadened over time, and perhaps the WCCRC itself can play a role in promoting such a broadening of focus.

This could begin with the broadening of WCCRC's membership. I want to encourage all those who define themselves as white collar crime scholars—certainly including those who focus on corporate crime and its control—to become active with the WCCRC. In the most recent issue of *WCCRC Focus* past president Jay Albanese raised the point that considerable conceptual and practical overlap exists between white collar crime, organized crime, computer crime, some forms of terrorism, delinquency, and gang-related crimes. I agree that the boundaries between at least some of these areas can indeed be blurred. However, in my view we should be cautious about extending an overly inclusive invitation to scholars in these many diverse fields to join our Consortium, insofar as a real risk of losing any focused identity could arise. My take on this is that we should simply encourage all those who define themselves as white collar crime scholars to join us; if their interest happens to be linked to a larger interest they may have in some other realm of inquiry (e.g., terrorism). This is fine, but the basis for becoming affiliated with the WCCRC should be rooted in an identifiable connection with white collar crime and its control, not something else.

The Functions of the WCCRC

From my point of view the WCCRC plays a useful role if it does no more than facilitate contact between white collar crime scholars and researchers, through biannual luncheons at meetings of the American Society of Criminology and the Academy of Criminal Justice Sciences, and the distribution of contact information. At present, we have a *WCCRC Focus* newsletter, distributed by NW3C, and a monthly electronic newsletter, *WCCRC Update*, developed by Jay Albanese. The ongoing usefulness and viability of these endeavors depends importantly on members contributing appropriate items to these newsletters. These newsletters certainly have the potential to serve as a means whereby white collar crime researchers become aware of the current research projects of others in the field. Some other possible initiatives are as follows:



PRESIDENT'S REMARKS (cont'd)

Annual Workshops: Ideally, annual workshops could be held, focusing on enduring or topical issues of concern to the white collar crime research community.

Lobbying: The WCCRC could ideally make contact with appropriate legislators, lobbying in favor of sound new legislation pertaining to white collar crime, and in favor of more funding and support for white collar crime research.

Creation of White Collar Crime Scholars Directory: The production of a directory of white collar crime scholars with specific areas of competence, and contact information for broad distribution to the white collar crime research community and to the media, could be useful. For the first-named of these constituencies, it could foster or facilitate contacts between scholars working on related research projects. For the second-named constituency, it could elevate the visibility of the white collar crime research community, and ideally produce more sophisticated understandings of white collar crime related issues. A number of our WCCRC members were contacted for and quoted in a recent *Fortune* magazine story on white collar crime. But it seems to me that we could take some steps to facilitate contacts between the media and white collar crime scholars who have specialized knowledge, especially during a period when major white collar crime cases are unfolding. We might also consider a format for the efficient dissemination to the media of news about significant white collar crime research findings.

White Collar Crime Journal: One or more members of the Consortium have proposed, over the years, that a journal focusing exclusively on white collar crime and its control be established. Alternatively, an exploration of optimal strategies for ensuring the representation of white collar crime research and scholarship in existing journals can be undertaken. I personally have some major reservations about "ghettoizing" white collar crime research in a journal with such a focus, but if a significant number of Consortium members feel differently about this they may want to explore the viability of establishing a white collar crime journal.

White Collar Crime in the Criminal Justice Curriculum: The WCCRC could play some role in gathering and disseminating data and information about the representation of white collar crime in the undergraduate and graduate criminal justice curriculum. It is my understanding that WCCRC member Debra Ross is engaged in such a project, and I would encourage other members to cooperate with her in any way possible. Can the WCCRC play an effective role in "lobbying" for much broader representation of white collar crime courses in the curriculum; at present such courses continue to be disturbingly underrepresented, to the best of my knowledge.

White Collar Crime Curriculum Resources: The WCCRC could conceivably play a useful role in the production of syllabi sets, pedagogical resources, master lists of books and articles, relevant Web sites, databases, and so forth. Any such efforts can obviously contribute to the objective stated above: promotion of the broader representation of white collar crime courses in the curriculum. Again, Debra Ross has taken some initiative on at least one of these projects—involving syllabi sets—and I hope she will have the ongoing cooperation of the membership here as well.

Economic Crime Summit: The focus of the Economic Crime Summit sponsored by NW3C and the Coalition for the Prevention of Economic Crime (CPEC) has been directed toward only some forms of white collar crime, and white collar crime researchers have been involved with this Summit to date in only a rather limited way. Can initiatives be undertaken to broaden the focus of the Economic Crime Summit, and bring in a higher level of involvement of the white collar crime research community?

Conclusion

Other initiatives are possible, but at the end of the day depend upon some critical mass of interest among the membership, and the willingness of a significant number of members to make these things happen. In addition, of course, the viability of at least some proposed initiatives depends upon the availability of funding support from NW3C. ☞

WHITE COLLAR CRIME HEADLINES

RAND Criminal Justice Reorganized into RAND Public Safety and Justice

RAND is pleased to announce that its Criminal Justice research unit has been reorganized into RAND Public Safety and Justice. This reorganization reflects increasing involvement in recent years in public safety issues that transcend criminal justice, including illegal immigration and border control; domestic counterterrorism, terrorism preparedness, and threat and vulnerability management; and emergency first-response capability. Jack Riley will continue as Director of RAND Public Safety and Justice, with Susan Turner as Associate Director for Research and Quality Coordinator, and Andrew Morral serving as Associate Director in RAND's Washington area office.

Research within RAND Public Safety and Justice has been reorganized into three centers: Criminal Justice Center (headed by Susan Turner), Drug Policy Research Center (a joint effort with RAND Health, headed by Martin Iguchi), and Public Safety Center (headed by acting director, Russ Glenn). RAND will continue its longstanding commitment to careful analysis of important criminal justice policy questions. For more information, please see: www.rand.org/psj/index.html ☞

U.S. Announces What Is Believed The Largest Identity Theft Case In American History; Losses Are In The Millions

James B. Comey, the United States Attorney for the Southern District of New York, and Kevin P. Donovan, the Assistant Director in Charge of the New York Field Office of the FBI, today announced the arrest of a defendant, Philip Cummings, in what authorities believe to be the largest identity theft case in U.S. history. Comey also announced the arrest of Linus Baptiste and the guilty plea of Hakeem Mohammed in related cases.

In a Complaint unsealed today, the United States charged Cummings with wire fraud and conspiracy in connection with his participation in a massive identity theft scheme that spanned nearly three years and involved more than 30,000 victims. As alleged in the Complaint, Cummings worked at Teledata Communications Inc. ("TCI"), a company in Long Island that provided the computerized means for banks and other entities to obtain consumer credit information from the three commercial credit history bureaus - Equifax, Experian and TransUnion. TCI provided software and other computerized devices to its client companies that enabled these companies, through the use of confidential computer passwords and subscriber codes, to access and download credit reports of consumers for legitimate business purposes.

As alleged in the Complaint, Cummings worked at TCI from about mid-1999 through about March 2000 as a Help-Desk employee, and was responsible for helping TCI's clients. As such, he had access to these companies' confidential passwords and codes. With these codes, he had the ability to access and download credit reports himself, it was charged.

As alleged in the Complaint, starting in early 2000, Cummings agreed to provide credit reports to a co-conspirator who is now a cooperating witness in the investigation ("CW"), in return for money. CW knew individuals who were willing to pay up to \$60 per credit report, and CW offered to split that money with Cummings, it was charged. Thereafter, CW dealt with 20 or more individuals in the Bronx and Brooklyn, who would bring lists to CW filled with names and addresses and/or Social Security numbers, and would ask CW to provide credit reports in those people's names. They would then pay him \$60 for each credit report that he was able to provide to them, it was charged, and CW, in turn, would split that money with Cummings.

As alleged in the Complaint, when CW began receiving lists from these co-conspirators in the beginning, he would contact Cummings, and Cummings would bring a laptop computer to the CW's home in New York and download the credit reports and give them to CW. CW in turn would sell them to his co-conspirators on the street.

At some point in 2000, Cummings moved to Georgia but allegedly ensured that the scheme could continue by traveling to New York to download credit reports for CW and then later giving a pre-programmed laptop computer to CW for CW to use to download the reports. He also allegedly taught CW how to access the Credit Bureaus and download the reports.

As alleged in the Complaint, Cummings provided passwords and codes to CW that enabled CW to access all three Credit Bureaus—Equifax, TransUnion, and Experian—over time. At various points in the scheme, when CW found that a code and password that CW had been using no longer worked, he allegedly called Cummings. Cummings would then allegedly give him a new password and code to use to continue the scheme. This happened on numerous occasions, the Government charged.

According to the complaints, the other co-conspirators to whom CW sold the credit reports provided, in the aggregate, tens of thousands of names and hundreds of thousands of dollars to CW for consumer credit reports. CW provided the credit reports to these other co-conspirators and split the money that they provided to CW with Cummings.

One entity whose confidential TCI password and subscriber code were allegedly misappropriated in the used for approximately 10 months to download approximately 15,000 credit reports from Experian. Ford discovered scheme was Ford Motor Credit Corp. at its Grand Rapids, Michigan, branch. That branch's password and code were the scheme after reviewing bills sent by Experian for those credit histories and receiving numerous complaints from consumers who had been the subject of identity theft and fraud. After searching its databases, Experian found that the passwords and subscriber codes of Washington Mutual Bank in Florida and Washington Mutual Finance Company in Crossville, Tennessee, had also been compromised, resulting in approximately 6,000 more credit reports for consumers being improperly downloaded.

According to the Complaint, Equifax determined that the password and subscriber codes for Ford's Decatur, Illinois, branch had been used improperly to download 1,300 credit reports from its databases in September and October 2002. The passwords and codes of Washington Mutual Finance's branch in St. Augustine, Florida, were used to download another 1,100 credit reports, and more than 4,000 additional credit reports were downloaded using the passwords and codes of six more entities: Dollar Bank in Cleveland, Ohio; Sarah Bush Lincoln Health Center in Illinois; the Personal Finance Company in Frankfort, Indiana; the Medical Bureau in Clearwater, Florida; Vintage Apartments in Houston, Texas; and Community Bank of Chaska in Chaska, Minnesota.

As alleged in the Complaint, Central Texas Energy Supply's codes were used improperly to download approximately 4,500 credit reports from TransUnion in September 2002.

All of the companies described above whose codes were compromised and misused have all been confirmed as TCI client companies, according to the Complaint.

WHITE COLLAR CRIME HEADLINES (cont'd)

As alleged in the Complaint, the number of victims in this case exceed 30,000, and the Government is in the process of determining the extent of the loss. To date, more than \$2.7 million in financial loss has been confirmed.

Consumers whose credit reports have been stolen in this scheme have reported many forms of identity fraud. As alleged in the Complaint, bank accounts holding tens of thousands of dollars in savings have been depleted; credit cards have been used to the tune of thousands of dollars without authorization; address changes have been made to accounts at various financial institutions; checks, debit cards, ATM cards and credit cards have been sent to unauthorized locations; and identities of victims have been assumed by others.

In a related case, Linus Baptiste was arrested on October 29, 2002, on a wire fraud charge related to the Cummings case. According to that complaint, phone numbers registered to Baptiste's residence were used to dial into Equifax's databases and download 400 - 600 credit reports in August 2002 in the scheme. Credit reports, laptop computers and a document bearing Cummings' name were found in Baptiste's home.

In a related case involving fraud perpetrated on several of these victims, on July 30, 2002, a defendant using the name Hakeem Mohammed was charged with mail fraud in connection with an address change made to a line of credit opened by two of the Ford victims and the opening of accounts and lines of credit in the names of two other Ford victims. Mohammed entered a guilty plea to mail fraud and conspiracy charges on October 2, 2002, and is scheduled to be sentenced before United States District Judge Gerald E. Lynch on January 8, 2003.

Cummings is expected to be presented in Manhattan federal court this afternoon on the Complaint unsealed today. If convicted, Cummings faces, with respect to the wire fraud charge, a maximum term of 30 years' imprisonment and a maximum fine of \$1 million or twice the pecuniary gain or loss resulting from the offense. Cummings faces, with respect to the conspiracy charge, a maximum term of 5 years' imprisonment and a maximum fine of \$250,000, or twice the gross gain or loss resulting from the crime.

Mr. Comey stated: "With a few keystrokes, these men essentially picked the pockets of tens of thousands of Americans and, in the process, took their identities, stole their money and swiped their security. These charges and the potential penalties underscore the severity of the crimes. We will pursue and prosecute with equal vigor others who may be involved."

Mr. Donovan stated: "The defendants took advantage of an insider's access to sensitive information in much the same way that a gang of thieves might get the combination to the bank vault from an insider. But the potential windfall was probably far greater than the contents of a bank vault and, using 21st century technology, they didn't even need a getaway car. Using the same technology, we determined what was done and who did it, proving that technology is a double-edged sword."

Mr. Comey praised the investigative efforts of the Federal Bureau of Investigation and thanked the United States Secret Service and the United States Postal Inspection Service for assisting in the investigation as well. Mr. Comey also stated that the investigation is continuing.

Assistant United States Attorneys Katherine M. Choo and Julian Schreiber are in charge of the Cummings and Baptiste prosecutions. Assistant United States Attorney Harry Chernoff is in charge of the Mohammed prosecution.

The charges contained in the Complaints are merely accusations, and the defendants are presumed innocent unless and until proven guilty.

Persons who believe they may have been victims of identity theft are advised to contact the Federal Trade Commission at: (877) ID THEFT, (877) 428-4338, or via its Web site at www.ftc.gov. ☞

MEMBER NEWS

Membership Drive

NW3C, in an effort to bolster membership in the WCCRC, is beginning a membership drive. As current members know, there is no cost to being a member of the WCCRC and the benefits include access to the WCCRC members and information, as well as a public forum for exchanging ideas and thoughts on white collar crime. If any current members of the WCCRC believe that they know an individual who would benefit from joining the WCCRC, please have them contact Jamie Sellaro at jsellaro@nw3c.org or 304-291-2080, ext. 288. ☞

New Members

- ♦ Stephen Carlton, Security Analysts, Inc.
- ♦ Mike Lynch, University of South Florida
- ♦ Robyn Mace, University of Memphis

New Member Spotlight

Robyn R. Mace, Ph.D., is a visiting assistant professor in the Department of Criminology and Criminal Justice at the University of Memphis. In addition to teaching courses, directing the internship program, and conducting research, she instructs law enforcement officers in strategic planning, problem-solving, and supervision issues through the Mid-South Training Institute. She is currently involved in research on public safety partnerships, crime commissions, entertainment districts, and zoo security.

Dr. Mace received her doctorate at Rutgers, the State University of New Jersey, in Newark at the School of Criminal Justice. Her doctoral survey of federal, state and local prosecutors, "Prosecution Organizations and the Network of Computer Crime Control," was completed in 1999, and reflected her longstanding interest in technology to facilitate and control crime. Her dissertation research was partially funded by the United States Department of Justice, National Institute of Justice, and examined prosecution organization responses to the computer and high technology crime. Dr. Mace graduated from the Wharton School, University of Pennsylvania in Philadelphia, with a bachelor of science degree in Economics in 1987. That same year, she received her master of science degree in Criminology at the Sellin Center for Criminal Law and Criminology, directed by criminologist Marvin Wolfgang.

Dr. Mace served from 1994-1998 as the Principal Program Development Specialist at the Jersey City Police Department in Jersey City, NJ. In this capacity she performed a variety of organizational development, strategic planning, crime analysis, capacity building, funding and municipal interface functions. She initiated, managed or directed a variety of projects, including the Domestic Violence Crisis Intervention Team pilot program, the Anti-Gang Initiative project and various federal hiring and program grants. She was instrumental in directing funds and hiring designated personnel to begin the Department's advanced crime analysis function. During her service with the Department, Dr. Mace managed and obtained over three million dollars in federal and state monies. During her tenure at the JCPD, she became a certified New Jersey State Police Training Commission Trainer; this enabled her to instruct recruits as well as middle and senior police managers.

Prior research experience includes working at the Center for Crime Prevention Studies at Rutgers-Newark, NJ, and evaluating mediation programs as an alternative to misdemeanor court proceedings with the Institute of Government at the University of North Carolina, Chapel Hill, N.C. She has conducted research programs within police, court and jail settings, including projects on mortgage fraud in New Jersey, white collar crime in U.S. District sentencing and policing urban drug markets. She has instructional experience in university, police academy and continuing educational settings, and regularly presents research findings at national and international venues.

She is active in several professional organizations, including the American Society for Industrial Security. She is also a member the Information Systems Security Association, the High Technology Crime Investigators Association, and the American Society of Criminology.

Robyn joined the WCCRC in order to become re-involved with research on computer and white collar crime. ☘

LEGAL BEAT

Copyright and Law Enforcement's Use of Seized Computers

by Christian Desilets, NW3C Research Attorney

Here's a scenario for you- suppose that you image a suspect's drive, boot up the image, and load his Internet browser to check out his history file- have you done anything wrong? The answer, like so many answers to legal questions, is a resounding "possibly." The problem here is copyright law. Copying and using material on the computer may very well violate copyright protections.

How We Got Here

Generally, one can have a copyright in any expression of creative thought fixed in a tangible medium. This includes computer programs and document files. Having a copyrighted work gives the creator certain legal rights- one of which is the right to control the copying and distribution of the work. In other words, if the computer contains anything of creative value -and if it's got an operating system, then it does- then copying it without the author's permission is against the law. Now, of course, people generally already know this in the abstract. Software pirates are arrested every day for illegally copying computer software and selling the copies. A few years ago, there was no liability for copying copyrighted works without profiting, which would have clearly exonerated most police uses of copyrighted software. This all changed after an infamous court case wherein a hacker who had posted free copies of expensive software to bulletin boards was found innocent of copyright infringement because he didn't attempt to make money from it. Congress responded to the incident by amending 17 U.S.C. § 106 to prohibit copying and distribution in general. Liability still exists even without an imaged disk, as the courts have ruled (in *MAI Sys. Corp. v. Peak Computer, Inc.*) that the very nature of computer software results in a copy of a used program being loaded into the computer's dynamic memory. Therefore, merely loading up someone else's software on their computer results in an infringing

LEGAL BEAT (cont'd)

copy being made. Modifications to 17 U.S.C. § 117 explicitly allow people to make such copies as are necessary for using the software (including the copy that gets loaded into RAM), but these allowances are only made for people who have permission to use the original copyrighted work, which would be the individual(s) the software is licensed to. In most cases, this is not law enforcement.

Fair Use

So what to do? Well, the main defense here is something called "Fair Use". Fair use is codified in 17 U.S.C. § 107. It reads as follows:

"... the fair use of a copyrighted work, including such use by reproduction in copies ... for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include:

1. the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
2. the nature of the copyrighted work;
3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
4. the effect of the use upon the potential market for or value of the copyrighted work.

The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors."

The biggest problem with all of this is that it's impossible to know for sure whether any given court is going to decide that the factors weigh in favor of fair use or not before one goes to trial. Merely using the copyrighted material for research purposes (and certainly, criminal investigation is a kind of research) isn't enough. Numerous researchers have been found guilty of copyright infringement for extensively quoting authors whose writing style or handwriting they were analyzing, or for quoting the research of others in a way that the courts found unfair. Similarly, the bare assertion that a practice is needed, sensible, just, or in the public interest isn't enough. Of course, there are no guidelines on either how each factor should be weighed or on what other factors might be included. If you noticed, the four proffered factors are only required to be included in the list - there's nothing against adding a half dozen other factors to the mix. Still, looking at each of the factors that we're given can shine some light on things, so let's give it a shot.

1. **The nature of the work:** Here, we consider the type of material we're looking at, with some types customarily being protected more highly than others. Generally, predominantly factual information (prescription drug interaction information, for example) is available for fair use in most instances and creative material is more closely guarded. Further, unpublished work is more closely guarded than published works (as the original author is deemed to have a strong interest in whether and when the work is published). While much of the material found on a computer (Windows swap files, for example) might well be deemed to have little creative value, computers also tend to hold extremely personal creative content. Letters, essays, school assignments, e-mail, and Internet search strings all fall under this banner. It is also important to note that, in this context, publication requires an attempt to distribute to a broad audience. While a web page might well be considered published, an e-mail sent to an eight person recipient list generally would not. This factor cuts against a fair use argument for copying an entire hard drive, as purely creative, unpublished works are almost certainly going to be copied.
2. **The amount used:** The courts acknowledge that there's a world of difference between quoting a phrase from a larger work and including the entire document as an appendix. Short excerpts are given more leeway than larger portions, and verbatim copies of the entirety of a work, especially when they could substitute for the original, are presumed unfair. When imaging a drive, the software applications, personal letters, password lists, and any other materials are copied in their entirety. This is far more threatening to the author's control over the original document than a mere one-line quotation. In fact, one of the main purposes of making the image is to eliminate the need for the original in the first place. Again, this cuts against forensic imaging.
3. **The effect of use on the potential market:** This one's a little harder to nail down. Clearly, selling a document that effectively supplants copyrighted material that it incorporates wouldn't tend to be a fair use. Contrariwise, photocopying an article that you've already purchased so that you can make comments in the margin would tend to be fair. In this case, there wouldn't normally be a market at all for much of the content on a hard drive. No one buys "Slack Space Anthology." For some of the other content (personal correspondence and such), there might or might not be a market but since law enforcement isn't publishing the material to the public the market, if any, is unaffected (though it is possible that some of the content might be published by the court through inclusion in a public record). For the software applications on the machine, however, a public market clearly exists and the software companies are losing business. Who's business? Law enforcement's. One of the big tip-offs here is that buying a copy of every program that officers might run into on a suspect's computer would be ruinous for local police on tight budgets. If the costs to implement such policies would be prohibitive, than the benefit for the software industry would also be great. It's a catch-22. The more unrealistic it would be to demand that the agency purchase the software, the more compelling the reasons to make them buy it. Of course, law enforce-

Event Calendar

Academy Of Criminal Justice Sciences
March 4 - 8, 2003
The Globalization of Crime and Criminal Justice
Boston, Massachusetts
www.acjs.org/

Economic Crime Summit
May 4-7, 2003
Economic Crime & Terrorism: 2003 and Beyond
Washington, D.C.
www.summit.nw3c.org

The International Society of Criminology 13th
World Congress of Criminology
August 10-15, 2003
Theme: Reducing Crime and Promoting Justice:
Challenges to Science, Policy and Practice
Rio De Janiero, Brazil
perso.wanadoo.fr/societe.internationale.de.criminologie/index_ang.htm ☞

ment isn't turning around and selling these programs on the open market, but if law enforcement in general doesn't need to buy the software because they're using a copy of the suspect's software, then this decreases the number of units the copyright holder is likely to sell to law enforcement. This leaves this factor with some wiggle room, but in the end the market (at least the law enforcement market) is still damaged, and so this would also count against fair use.

4. The purpose and character of use: Here, finally, is the one factor that clearly favors fair use. There is a strong public policy interest in allowing law enforcement to copy and use protected material. Criminal investigations may require examining the contents of the hard drive (loading the files into RAM and creating what would normally be an infringing copy since law enforcement is not an authorized user in the first place), and imaging a hard drive preserves evidence and testifies to the authenticity of the resultant evidence. Of course, there's still a question regarding program use. The police have an interest in viewing evidence left on the drive, but they don't have as clear an interest in using the suspect's viewing program rather than their own. There might be a government interest in reading a suspect's e-mail, but does it allow one to create an unauthorized copy of Microsoft Outlook to do it? Does this one factor outweigh the other three? Maybe.

Other Uses That Are Generally Fair

The copyright office (pursuant to 37 CFR 201.2) issues copies of copyrighted materials to attorneys involved in actual or prospective litigation involving the work (though they must get assurances that the reproduction will only be used in connection with the litigation), so we can assume that that use is considered fair. How different, then, is this? The copyright office furnishes complete copies of creative, marketable works to parties who are directly adversarial to the copyright holder's interests, knowing that there is a chance that they might be revealed publicly in court documents. Surely, if the Copyright Office had one of the suspect's copyrightable letters in their possession they would also release it in similar fashion. The main difference here is that, while the suspect's e-mails may be the subject of a legal proceeding, Microsoft Windows, generally, is not. An argument could be made that the entire computer is part of the subject of the case (and this may well suffice before a sympathetic judge). Generally, however, while unique material may be considered for fair use, parties in court cases have not been allowed to use this exception to escape paying the customary fees for publicly available products. In the case of imaging a hard drive, there is an argument that the entire unit is a unique document that must be preserved in its entirety (to examine the slack space and look for hidden or deceptively named files) and could not be purchased on the open market. However, this same argument doesn't carry over to copying the suspect's software into RAM unless there is a possibility of unique features or modifications that could not be found in the retail version. As a general rule, courtroom utility may not be cited as a reason for refusing to pay customary fees for products. When a commercially available copy of the copyrighted work is needed at trial, an unauthorized copy of the work may not be substituted. The suspect's copy of the software may only be used, then, when there is something special about this particular copy of the software.

Conclusion

In the final analysis, keeping in mind that a court has the leeway to decide things either way, the safest way to seek a safe harbor within the Copyright Act's fair use provision would seem to be to purchase copies of any publicly available, non-unique and non-uniquely configurable software that would be needed to access the suspect's files. (Though a court might not even require that much.) Other than those programs, law enforcement would seem to have a clear fair use for forensic images. There is a strong government interest in being able to copy and examine the contents of the hard drive (including the overall image), there is no lost revenue from sales to law enforcement (as that particular hard drive is not publicly, commercially available), and the material is the subject of the investigation. Just keep in mind that the courts are still free to judge each case separately and may not accord the same weight to the same factors twice. ☞

NW3C RESEARCH SECTION

On Friday November 15, NW3C sponsored the 2002 American Society of Criminology White Collar Crime Research Consortium (WCCRC) luncheon at the Palmer House Hilton, Chicago Ill. WCCRC luncheon members met to welcome our new President, Dave Friedrichs and wish a fond farewell to outgoing President Jay Albanese. The WCCRC luncheon was well received, with over 30 members taking time out of their busy presentation schedules to attend. During the luncheon, Dave Friedrichs remarked on the future of the WCCRC, while Jay Albanese discussed the past and how far the group has come in a short time. NW3C Research Manager John Kane reminded the members of the importance of the WCCRC and implored members to take an active role in furthering the research of the white collar crime and the WCCRC itself. The meeting concluded with a presentation by Ronald Burns on his NW3C funded research into Internet Fraud and law enforcement preparedness.

Another WCCRC luncheon will be held on Friday, March 7, 2003, in Boston, Mass., at the Marriott Copley Place at the 2003 annual Academy of Criminal Justice Sciences meeting. All members are welcome and more details will follow through the listserv as details are finalized. ☞

Contact Us

John Kane	Research Manager	jkane@nw3c.org	(877) 693-2874 ext. 302
Don Mason	Research Attorney	dmason@nw3c.org	(877) 693-2874 ext. 255
Christian Desilets	Research Attorney	cdesilets@nw3c.org	(877) 693-2874 ext. 271
Shawn Hutton	Research Associate	shutton@nw3c.org	(877) 693-2874 ext. 243
Adrian Mascari	Research Assistant	amascari@nw3c.org	(877) 693-2874 ext. 263
Sandra Haantz	Research Assistant	shaantz@nw3c.org	(877) 693-2874 ext. 290
Jamie Sellaro	Section Coordinator	jsellaro@nw3c.org	(877) 693-2874 ext. 288 ☞

EDITOR'S NOTE

The WCCRC Focus is a publication of the White Collar Crime Research Consortium (WCCRC). It welcomes articles and announcements relevant to individuals and organizations involved in white collar crime or related research. NW3C sponsors, funds, and coordinates the activities of the WCCRC. Please direct comments, suggestions, and materials to WCCRC Editor and NW3C Research Associate Shawn Hutton at shutton@nw3c.org or by calling 877-693-2874, ext. 243.

This publication is produced with the support of grant #99-WC-CX-0002, awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The Assistant Attorney General, Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.