AN A.S. PRATT PUBLICATION
AUGUST/SEPTEMBER 2015
VOL. 1 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis®

Pratt's Privacy & Cybersecurity Law Report

VOLUME 1 NUMBER 1 AUGUST/SEPTEMBER 2015

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:

Deneil C. Targowski at	908-673-3380
Email:	Deneil.C.Targowski@lexisnexis.com

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at	(800) 833-9844
Outside the United States and Canada, please call	(518) 487-3000
Fax Number	(518) 487-3584
Customer Service Web site	http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or	(800) 223-1940
Outside the United States and Canada, please call	(518) 487-3000

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
David Kalat, *Day One: The Origin Story of Computer Forensics*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [4] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2015–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. Copyright 2015 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Day One: The Origin Story of Computer Forensics

By David Kalat*

The author of this article looks back at how the field of computer forensics began to better understand some of the special challenges faced today.

For years, computer forensic investigators have had the luxury of encountering a typical IT environment: Microsoft Office-based applications running on a Windows operating system on magnetic hard disks installed in individual workstations and servers inside corporate data centers. Meanwhile, a set of forensic tools (such as Guardian's EnCase, Access Data's FTK, and Magnet Forensic's IEF) have evolved to simplify the ability of examiners to extract commonly encountered artifacts from these technologies. As examiners in both civilian and law enforcement capacities use the same tools in a variety of investigations, a sufficient body of case law has developed to accept these practices as established, and even as familiar.

A tipping point is coming. The once relatively uniform IT environment of corporate America is giving way to a more diverse IT ecosystem. Businesses are shifting from administering their own data centers to managing third-party cloud providers; Apple Macs are appearing where PCs once were. Employees are conducting work on an unlimited variety of mobile devices. Forensic investigators are increasingly likely to encounter unfamiliar technologies that demand new analytical techniques. In order to make sure that these techniques are accepted in courts of law, modern investigators must be prepared to explain and defend their innovations in a way that is understandable and persuasive to non-specialists.

LOOKING BACK: THE WARD CASE

To see how investigators will face these challenges in the future, it is instructive to look back at how they faced them in the past. How did the first computer forensic investigators address these needs, before the concept of "computer forensics" even existed? Computer forensics is an older field than one might think, and its history can be instructive in terms of understanding some of the special challenges faced today.

In the early 1970s, Donn B. Parker, a pioneering researcher at the intersection of computer science and criminal justice—at a time when it was an uphill battle to convince people that those two concepts deserved to be spoken of in the same

* David Kalat, a computer forensic investigator and eDiscovery project manager at Berkeley Research Group, LLC, manages data preservation, forensic analysis, and review hosting for government agencies, international banks, pharmaceutical companies, higher education institutions, and corporate clients.

sentence—assembled a survey of hundreds of incidents of computer crimes, fraud, and abuse dating back to the mid-1950s. One case study stands out as the most promising to nominate as the dawn of computer forensic science: the highly publicized trial of Hugh Jeffry Ward in 1971 for theft of trade secrets.

In many ways, the Ward case seems impossibly prehistoric. It would be 16 years before Access Data was founded and 26 years before Guidance Software. Widespread training of law enforcement in computer forensics would not start for another 24 years. The prevalent computer model in those days, and the one in this case, was the Univac. It was a mainframe computer the size of a room, whose memory banks consisted of giant spinning wheels of magnetic tapes. The Univac carried a price tag equivalent to $7 million in today's dollars. The name stood for "UNIVersal Automatic Computer" but also connoted its key attribute: at its heart was an array of vacuum tubes, like the ones used on radio amplifiers. This was the state of high tech in 1971.

In other ways, the Ward case is a prototype of the kinds of theft of trade secrets matters that are the bread and butter of many computer forensic professionals today. For example, Univacs were so expensive, enormous, and difficult to operate that few businesses had their own. Most companies used local terminals to remotely access a Univac owned and leased by a computer services supplier—much like today's enterprises have outsourced data centers to cloud service providers.

The Information System Design Incident

Oakland's Information System Design, Inc. ("ISD") was one such computing service provider. Among other things, ISD rented time on its Univac 1108, which could be accessed by authorized users who dialed in over the phone lines using an unlisted number and providing the log-on credentials of a site designation code and a user account code.

In early 1971, ISD's data center shipped to one of its customers, Shell Development Company, a neatly bound set of 515 punch cards imprinted with Shell's account number. The officers and employees at Shell were puzzled—no one recalled ordering these cards. After a few days of fruitless inquiry, staff at Shell chalked it all up to "computer glitch" and tossed the cards in the trash.

A quick word about punch cards is in order, for the benefit of today's reader: Having a bunch of cards punched in 1971 was the equivalent of copying a file onto a USB stick or a CD. This was the process by which a user would export a copy of an executable file onto portable media, with which to move it from one system to another and reload it.

When an ISD sales representative doing his rounds saw those cards in Shell's trash, he was not so easily satisfied with the "computer glitch" explanation. He was a computer science professional—*his* computers did not make random errors. *Somebody* ordered those cards to be printed, and if no one at Shell did. . .

He examined the cards. They contained the source code of PLOT/TRANS, a proprietary remote plotting program. The program allowed ISD customers to input design specifications at one terminal and then output a full-scale engineering drawing at another terminal. The punch cards would enable the recipient to load the program into another Univac, which Shell did not have—that's why they rented time on ISD's.

Only two copies of this program had existed: one on the Univac mainframe's memory bank and a backup copy on a reel of tape in secure storage. But now a third was sitting in the trash bin of a customer. Could there be other copies?

At ISD's offices, an internal investigation unfolded more of the story. On January 19, 1971, shortly after the end of the normal business day, a user dialing in with the (possibly stolen) Shell logon credentials had initiated an 11-minute session, bee-lined to the plotting program, and initiated the punching of cards.

Except when the user commanded the system to punch the cards, he or she probably expected that the cards would be printed out at their local terminal, not at the ISD mainframe. As a result, the cards were useless—they'd been printed using Shell's account and would be delivered to Shell in the normal course of business. Whoever was hacking the system would need another way to steal the program.

That is exactly what the data showed next. According to ISD's account activity logs, after commanding the punch card export, the same user requested that the file be printed. Locally. It would be hundreds of lines of source code on paper, which would have to be manually retyped into the target system, but at least the hacker now had a local copy of the prize.

Who was the Hacker?

The only question left: who was the hacker? ISD figured the most likely culprit was its chief competitor, University Computing Center ("UCC"), in Palo Alto. UCC's chief programmer was Hugh Jeffry Ward, who had been trying to woo the Aerojet account away from ISD. Aerojet was a heavy user of PLOT/TRANS, and UCC would need to offer similar functionality to be competitive. Ward had previously worked for another vendor to Shell and might have learned the log-on credentials that way.

After ISD filed a criminal complaint on February 17, 1971, the authorities issued a subpoena to the phone company. Pacific Telephone confirmed there was an 11-minute, 32-second outgoing call from UCC to ISD at the date and time that the Univac was accessed.

It was enough evidence to draw up a search warrant, issued on February 19. This is a particularly noteworthy historical artifact: the first American search warrant to call for the search of computer storage and memory in connection with a criminal case. Here is where the world of computer forensics was born.

Forensic Evidence Principles

Several principles govern whether forensic evidence can be used in a legal proceeding in the United States:

- Is it admissible (is the evidence legally obtained?);
- Is it authentic (is the evidence to be trusted?);
- Is it reproducible (is the process scientifically sound?); and
- Is it reliable (is the evidence understandable in a way that can be probative?).

Each of these principles was at play in some crucial and instructive fashion in the story of Hugh Ward.

The Principles at Play in the Ward Case

The February 19 search warrant provided a clear articulation of what Sergeant Terence Green of the Oakland Police Department's Fraud Detail was allowed to collect. Under ordinary circumstances, evidence collected pursuant to a properly executed search warrant would be presumptively admissible in court. But Sergeant Green had a pair of problems with this search warrant, and they gave rise to a thorny issue involving the principle of authenticity.

Green's first concern was how the types of computer storage itemized in the search warrant were volatile things. It would not take much to render punch cards irrevocably unreadable, and there was concern that a quick swipe of a magnet could leave reels of tape worthless. In practical fact, magnetically erasing reels of tape would take a considerable degree of time and a high-powered magnet, but at the time it was popularly believed that a handful of ordinary household magnets were anathema to computers. (Data centers in those days typically came with magnetometers installed in the doorways, as a show of protection against an essentially nonexistent threat.) Sergeant Green's second problem was that he had no idea what the things listed in the search warrant would look like or how to make sure he'd found them all or received them safely. If the first problem involved the risk that the target of the investigation might destroy evidence on purpose, the second involved the risk that investigators might do so out of ignorance.

Sergeant Green enlisted a technical advisor. This expert consultant was ISD programmer Keith Marcelius. That the only member of the team actually capable of executing the terms of this unprecedented search warrant was a representative of the victim company would later prove to be a controversial point in the prosecution of Hugh Ward.

In order to consider Marcelius' evidence as having probative value, the court had to first become comfortable that his evidence was true and accurate. In today's practice of computer forensics, various procedures are used to help address this concern. Meticulous documentation of the chain of custody is crucial, and the use of hash-value verifications has become a widely accepted standard to demonstrate that a copy is bit-for-bit identical to the suspect device.

On February 19, 1971, Marcelius took the rudimentary steps now familiar to computer forensic professionals preserving evidence in the field: he made a complete copy of the entire contents of UCC's computer system, encompassing dozens of reels of magnetic tape, among other sources. This was before the existence of tools with which to create forensic bit-for-bit hash-verified images, but the basic premise was in place: make a copy, examine the copy.

In examining that copy, Marcelius found evidence he felt conclusively established that Ward had been copying data from ISD's systems for almost a year, including but not limited to the copying of the PLOT/TRANS source code. Here we find the principle of reproducibility: Marcelius was not the only technical expert to examine this evidence. Marcelius' technical findings gain credibility when they can be corroborated by other examiners.

The Legal Proceedings

Two distinct legal proceedings followed. One was a civil case brought by ISD against UCC for unfair competition; the other was a criminal case against Ward. The district attorney decided to prosecute Ward under California's new trade secret law, because he was doubtful he could convince jurors that the theft of 489 lines of computer code could be counted as $25,000 worth of "property." The district attorney, however, had no way around the fact that he would be stuck presenting a case that depended largely, if not entirely, on the highly technical expert testimony of a computer programmer.

The testimonies of Marcelius and other technical experts brought in by the various combatants highlight the importance of the principle of reliability. In order to serve any probative value for a factfinder, expert testimony must be, at a minimum, comprehensible. Technical gibberish that can be understood only by other experts, even if factually correct, will not be persuasive.

During Marcelius' extensive and patiently detailed testimony, the court reporter asked for a break to ask him to spell out a confusing term. The judge admitted he too was having trouble following what Marcelius was saying. What was this "synon" he kept talking about? The deputy district attorney explained that Marcelius was saying "sign on," not "synon."

Another point of confusion arose with respect to the concept of encryption. One legal question in the case was whether the program could be classified as a trade secret under the new law. If it was not a "trade secret," Ward's intrusion into ISD's network might not be actionable. One way to help identify the program as a trade secret was the degree to which ISD attempted to protect it. If the program was encrypted, for example, this would have legal significance.

PLOT/TRANS existed on ISD's system in two forms: the original source code as the programmers had written it, and compiled in a relocatable binary form that could actually be run. This concept and the terminology used to explain it were strange to the court. The judge and the lawyers got tangled up in the misapprehension that the source code was in a human readable language, whereas the compiled binary version was unreadable by humans and therefore *encrypted*. Eventually, the court came to accept that *both* versions were theoretically understandable to humans, if properly trained, but that the binary version would just be unpleasantly hard to read.

This, though, meant that neither version was encrypted, despite the availability of encryption as a tool on ISD's systems that could have been deployed for additional protection. Marcelius testified that ISD was in the process of encrypting its files but had not reached the PLOT/TRANS program by the time of its theft. But the technical confusion was potentially muddying an important legal point: was this evidence that ISD did not consider this program important enough to secure via encryption?

Meanwhile, a separate civil trial against UCC began, with ISD asking for $6 million in damages. According to Donn Parker's first-person account of attending the trial, both sides carefully stage-managed the civil trial to deliberately obfuscate the technical issues, with each litigant apparently hoping to make the technology confusing so that their more emotional arguments might sway. Both sides presented an array of expert witnesses but reportedly prevented them from testifying much beyond "yes/no" responses to questions posed with such technical ignorance as to be incomprehensible. Parker writes that he all but pleaded with one attorney for the opportunity to take the stand to clear up the rampantly mounting misinformation, and was rebuffed.

The attorneys for the defendant UCC followed the tack suggested by Ward's criminal defense attorneys: that the program was not being treated as a trade secret, that hacking into a computer system and fishing around for data is a routine practice in the programming community (*everybody does it!*), and that besides, all Ward did was take a *copy*. The original is still there, perfectly fine! What kind of theft is it if the "stolen" object is still there?

The Verdict

The courts ultimately found sufficient evidence that Ward had stolen a trade secret to certify the case for trial. The jury in the civil trial returned a verdict for plaintiff ISD, ordering UCC to pay ISD $250,000 in compensatory damages and $50,000 in punitive damages. In the criminal proceeding, Ward pled guilty to one count of theft of trade secrets and was sentenced to three years of probation and a $5,000 fine.

FRAUD INVESTIGATIONS TODAY

Forty-four years after Ward's trial, computer forensics has grown into a recognized field of forensic science that informs civil and criminal proceedings in a wide variety of cases. The amount of digital information created worldwide has been steadily doubling every two years—in 2005, there was an estimated 132 exabytes of digital data in the world (that is 132 billion gigabytes), and by 2020 there is projected to be 44 zetabytes (44 trillion gigabytes), or as many digital bits as there are stars in the universe. The average American worker produces around 5,000 megabytes every day. The vast majority of information is now created in digital form, and nearly all of it stays in digital form as well. Today's fraud investigator must be prepared to conduct examinations in that paperless world. Although tools and techniques have matured, and the types of digital information to be examined have ballooned in quantity and variety, the fundamental issues that drove the Ward case almost a half-century ago continue to inform how computer forensic investigators conduct their work.