

Computer and Intellectual Property Crime: Federal and State Law 2004 Cumulative Supplement

By A. Hugh Scott and Kathleen Burdette Shields

Boston, MA, 2004, The Bureau of National Affairs, Inc., Paper: ISBN1-57018-421-6,
(Price \$165 Supplement Only, \$325 main text and 2004 Supplement)

Reviewed by Anne Wolfe, LL.M. in Global Technology Law
Journal of High Technology Law
Suffolk University Law School

Much of the literature available on intellectual property protection focuses on the traditional forms of trademark and patent prosecution, trade secret protection and copyright regimes. These forms of civil protection are important, but overlook the critical aspect of crime involving intellectual property. Technological development has given rise to substantial amounts of fraud, theft, infringement and piracy, much of it facilitated through computer use. With the economic costs of computer and intellectual property crime running into the billions of dollars,¹ the criminal aspects of this area are crucial and cannot be overlooked. Since the first computer crime statute appeared on the books in 1984,² this area of law has developed rapidly, and the current pace of evolution remains fast and furious. There was a notable absence of a cohesive work in this area, and the need for compiling such a text remained unmet until the original text of “Computer and Intellectual Property Crime” (“CIPC”) was printed in 2001. Highlighting the quick development of this area of the law was the almost immediate need for a substantial supplement. Between the time the original text of CIPC went to the printers

¹ The Federal Trade Commission’s Identity Theft Survey Report estimates total loss to businesses from identity theft in 2003 to be \$33 billion. <http://www.ftc.gov/os/2003/09/synovaterreport.pdf>. Microsoft’s anti-spam division estimates that currently \$20.4 billion is lost annually to repairs and lost work time. <http://www.cnn.com/2004/BUSINESS/09/13/go.cyber.security/index.html>

² See Computer Fraud and Abuse Act, Pub.L.No. 98-473, Title 22, Chapter XXI, 2102(a), 98 Stat. 1837, 2190 (1984) (enacting 18 U.S.C. 1030)

and its arrival on the bookshelves, the terror attacks of 9/11 had occurred, resulting in the prompt passage of a number of statutes delineating criminal activity on-line and providing for police and security services monitoring of computer and on-line activity. Further rapid evolution of the law in this area outside the realm of national security surveillance has continued to require substantial revisions to the main text, resulting in what are now annual cumulative supplements. With the 2004 supplement weighing in at 946 pages, the time for an entire new edition of the main text is fast approaching.

For many texts, annual updates take one of two tracks. Either a hasty compiling of every piece of legislation that comes down the pike by the submission deadline with bits of knowledgeable sounding filler is provided for an increasingly flummoxed reader, or ambitious undertakings are made in what are perceived as newsworthy areas, often leaving out key technical points for the sake of increasing book sales. The CIPC Supplement text manages to avoid both of these pitfalls in an extremely comprehensive, systematic and thorough treatment of the issues raised. Entire chapters are re-written, added or removed from year to year, with substantial minor additions created as necessary.

Recognizing the amount of effort it would take to maintain the depth of analysis originally provided in CIPC while dealing with such rapidly developing statute and case law, Hugh Scott took on a co-author, Kathleen Burdette Shields. Two minds, in this instance, do indeed prove better than just one by permitting in-depth analysis over a greater range of topics. Both parties are practicing litigators in this area of law, and their expertise shows in this work. Practitioners will appreciate the ease with which the book educates about the necessary points of law, which include not just the reproduction of

statutes, but commentary pertaining to when each particular bar or subsection of a statute is triggered. While crime is the focus, other points of intellectual property protection discussed include how to protect disclosures, including trade secrets, during litigation and other public and administrative matters. These practical aspects allow practitioners to achieve full protection of their client's interests.

All aspects of crime are covered, from means and methods for reporting crime if to the appropriate authorities a client is a victim to sentencing guidelines. Additionally, there is a fifty state survey of relevant legislation. While state surveys may prove helpful in some circumstances, given the increasing practicalities of computer crime and intellectual property crime as a cross-jurisdictional phenomenon, and intellectual property as a primarily federally protected entity, the state tables are less useful than they might at first appear, and there remains the danger that a practitioner may rely solely on the state law sections than the federal law provisions. Given that a single computer crime can easily, almost routinely, encompass an actor in one state, a victim in another state, a server in a third state, and a bank account in a fourth state, transmitted over federally regulated wires and systems, state law becomes increasingly irrelevant. The true value of this work is in its exhaustive treatment of federal crimes.

The wide range of federal crimes covered includes those that would not ordinarily occur to someone focused on intellectual property crime. The Export Administration Act and postal fraud at first glance do not readily relate to the cyber-age. The laws on the books, however, cannot be updated quite quickly enough to keep up with technological developments, so reliance on old statutes is frequently the only venue available to stop fraudulent activity. The comprehensive outlook is relentlessly practical in its outlook,

providing for example the statutes against trafficking in counterfeit labels and computer program documentation and packaging,³ overall a simpler charge to prove than computer piracy or copyright infringement, but one that in relation to software is likely to equally threaten a software pirate. Such offenses are extremely useful in deterrence and negotiation with defendants, and deserve the type of thorough treatment as Scott and Burdette give here.

All sections of the book follow a consistent and efficient format. A brief overview is given, followed by the text of relevant statutes and a synopsis of the legislative history. Elements of the offence are broken down and discussed individually, followed by jury instructions, commentary (including discussion on current levels of enforcement and sentencing guidelines), and finally a discussion of appropriate civil remedies which may overlap the criminal offenses. It is in the discussion of the elements of a crime, including potential defenses, where the book particularly shines, followed closely by the discussion of enforcement. A practitioner can easily access all relevant information he would need to successfully follow a matter presented to him to its conclusion. As such, it is a valuable library asset for anyone who encounters this area with any regularity.

Of particular interest in the 2004 supplement is the chapter on electronic mail crime (under the new CAN-SPAM Act⁴). In the absence of precedent, due to the recent enactment of the statute, Scott and Burdette cut straight to the point, and while providing a breakdown of the offenses created under CAN-SPAM, note that the act “has been almost entirely ineffective to date in decreasing the amount of spam or making the

³ 18 U.S.C. § 2318

⁴ Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat 2699 (Dec. 16, 2003)

senders of spam easier to identify.”⁵ This type of practical information is essential to practitioners when trying to make a decision as to the most effective avenues available to clients. Additionally, there are strong new sections pertaining to case law developments regarding damage to computers by computer viruses, identity theft, and child exploitation. Developments of the case histories are quick and straight to the point, but with sufficient detail and context that permit a quick grasp of concepts contained therein.

One of the few drawbacks to the supplement approach readily becomes apparent – without the original text, the book suffers, as in an effort to minimize space, there are many edits that say “replace footnote 56” or “replace table XYZ” with text then provided. While this can easily be accomplished for figures and minor edits, the net result requires that in order to stay up to date in an area presented, the two books must be read simultaneously. This interferes with the otherwise clear and straightforward presentation of the information. The main drawback of the supplement premise is its sheer length. At just shy of 1000 pages which edit or replace the 1,600 page main text, the book rapidly becomes unwieldy. Turning the book into a loose-leaf multi-volume treatise would assist with keeping the book up to date, as well as separating the federal from the state law.

As a treatise, this is not a book for bedtime reading. For litigators involved in criminal prosecution or defense in relatively new fields, however, the book is an essential manual. To be caught without it on the practitioner bookshelf would be a crime in itself.

⁵ Computer and Intellectual Property Crime, 2004 Cumulative Supplement, p 127. See Keith Ferrell, Spam, Lovely, Spam (Sept 8, 2004) available at www.securitypipeline.com/ShowArticle.jhtml?articleID=46802544.