The Attorney's Legal Obligations When Coming into Inadvertent Possession of or Access to Child Pornography

By Sean L Harrington

Introduction

With this Comment, I hope to provide practitioners with the applicable law and procedure for situations in which attorneys or their agents (including experts) may inadvertently come into possession of child pornography (hereinafter, "Contraband") outside of a law enforcement setting, or the rare instance that a circuit court finds that law enforcement has failed to make contraband evidence reasonably available for inspection by the defense.[1] Although the subject has received little attention in the literature, I have witnessed at least three occurrences during my tenure as a digital forensics examiner and attorney, and it has been my impression that attorneys are unprepared in such instances. As discussed herein, I make a distinction between the unwitting acquisition of contraband as opposed to willful or reckless acquisition by a practitioner: the former triggers an affirmative duty of dispossession; the latter may be unlawful and subject the attorney or the attorney's agent to a risk of criminal prosecution.

Willful or Reckless Production or Acquisition

The following two examples are of willful or reckless acquisition by lawyers, each with very different outcomes that are instructive.

The first example is an Ohio attorney. The attorney established himself as a defense expert in the subject matter of contraband, and championed the novel theory that "it is now impossible for any individual to know from a mere viewing of digital images on a computer whether or not those images portray actual children."[2] In support of his thesis, the attorney

---

[1] *See* WI Stat § 971.23(11)(c)(2); State v. Bowser, 2009 WI App 114, 321 Wis. 2d 221, 772 N.W.2d 666

[2] United States v. Shreck, N.D. Oklahoma No. 03-CR-0043-CVE, 2006 WL 7067888 (May 23, 2006).

testified in April 2004 as an expert witness on behalf of a defendant charged with actual or attempted possession of contraband.[3] He presented "before" photographs of children that he had obtained as stock images, and followed by photographs which he altered ("morphed") to depict the same children engaging in sexually explicit conduct with adults. The attorney-expert's defense theory was that if he could fabricate contraband so easily, then there should be reasonable doubt that the alleged contraband with which defendant was charged might also have been fabricated.

At the conclusion of that hearing, the prosecution asserted that the attorney-expert's "after" exhibits were contraband. The judge pointed out the exhibits were prepared "at court order," but instructed attorney-expert to delete them. Instead, the attorney-expert called the US Attorney's office in his hometown, Cleveland, for an opinion as to whether these exhibits were contraband. He did not receive a return call, and thereafter shipped his computer from Oklahoma to Ohio, where he continued to use the exhibits in testimony in Ohio cases.[4]

The following month, the Federal Bureau of Investigation ("FBI") began investigating the attorney-expert's conduct related to the contraband images he had fabricated. The FBI obtained a search warrant for his home and seized devices containing electronic files. The U.S. Attorney's Office asserted that attorney-expert's prepared exhibits were contraband under 18 U.S.C. § 2256(8)(C), which defines as "child pornography" any image that is created, adapted, or modified to make it appear that an identifiable minor is engaging in sexually explicit conduct. To avoid prosecution, the attorney-expert executed a pre-trial diversion agreement in which he admitted he violated federal law 18 U.S.C. § 2252A(a)(5)(B) by morphing the images of identifiable children into contraband.

The problems for the attorney-expert did not end there. After Federal prosecutors had identified two children in the stock photos and contraband and informed the children's parents, the parents sued him under 18 U.S.C. § 2255 (the civil-remedy provision of the federal child pornography statute), which provides statutory minimum damages of $150,000 to victims of child pornographers. After an appeal to and remand from the United States Court of Appeals for

---

[3] *Ibid.*

[4] In re Boland, 68 Bankr.Ct.Dec. 51, 946 F.3d 335 at 337-338, (6th Cir. 2020).

the Sixth Circuit, judgment was entered against the attorney-expert for $300,000.[5] He was also ordered to pay plaintiffs $43,214.11 in attorney fees.[6]

Our second example is a South Dakota attorney. He was indicted on one count of possession of child contraband and two counts of distribution in connection with visiting Web sites or using file sharing software that his client had allegedly visited or used so that he could understand what the client was doing. He asserted that he was a "criminal defense attorney who specializes in representing persons accused of pedophilia and other sex crimes against children."

In his Motion to Dismiss, the attorney argued that, in the course of his law practice, some of his clients sought advice about whether particular websites contained material that constituted child pornography, and that in order to properly advise those clients, he would access the website on his office computer and "analyze the website's contents and render an opinion about whether the particular website contained pornography." He argued that he was allowed under South Dakota law to access and view child pornography in his capacity as a criminal defense attorney representing persons who are charged or who may be charged under the child pornography statutes, citing S.D.C.L. § 22-24A-19:

> The provisions of [the state's child pornography and child sexual exploitation laws] do not apply to the performance of official duties by any law enforcement officer, court employee, attorney, licensed physician, psychologist, social worker, or any person acting at the direction of a licensed physician, psychologist, or social worker in the course of a bona fide treatment or professional education program.

The attorney sought to assert the state law as an affirmative defense with the jury instruction, ". . . that it is a defense to a child pornography charge if the purpose of [the defense attorney] in viewing child pornography was to render legal advice to a client. If such facts exist, they create a defense to the charge of possession of child pornography."

After litigating the issue of whether South Dakota's law was preempted by Federal law, the attorney was allowed to assert the affirmative defense,[7] and was acquitted of all charges. One wonders whether this same approach might've worked for the Ohio attorney-expert in our

---

[5] Doe v. Boland, 630 F.3d 491 (6th Cir. 2011); *see also* Doe v. Boland (In re Boland), 946 F.3d 335 (6th Cir.2020)
[6] Disciplinary Counsel v. Taylor, 2024-Ohio-1082; *see also* Roe v. Taylor, 2024-Ohio-2714.
[7] U.S. v. Flynn, 709 F. Supp. 2d 737 (D.S.D. 2010)

first example, who, in 2010, tried a different approach by bringing suit for declaratory and injunctive relief against the Attorney General of the United States, seeking to enjoin the United States from enforcing any of the child pornography statutes against Ohio criminal defense attorneys or defense experts, based on a similar state statute in Ohio and lack of Federal preemption. That effort was not successful.[8]

I am aware of only one instance in which a non-attorney computer forensics examiner requested and was granted permission to remove contraband to his lab, after an analysis of preemption issues by the state district court in Minnesota.[9] Because his activities were, apparently, not known or challenged by Federal authorities, the providence of his actions and the state court's ruling remains unsettled.

Unwitting Acquisition

The unwitting acquisition of contraband by an attorney is a significant risk. In my digital forensics practice, I have been a witness to and an affected party on three different occasions, described below. To guard against this risk, I include the following language in my boiler-plate services agreement, a copy of which I provide to counsel:

> If a forensic examination in a setting **outside of a law enforcement facility (during a defense examination)** reveals the existence of possible child pornography on the examined media, [digital forensics company] will immediately cease its examination and advise CLIENT and appropriate law enforcement authorities of the nature of the materials found. [digital forensics company] will not actively search for child pornography unless instructed to do so by CLIENT or CLIENT's counsel, however, it is possible that [digital forensics company] may inadvertently come across contraband images. Reporting and activities incident thereto constitute "Professional services" for purposes of this Agreement.

In one case, I was sent an alleged victim's mobile device. The alleged victim was a minor child. The attorney who provided the phone had not inspected the phone, but understood there was a

[8] Boland v. Holder, Case No.: 1:09 CV 1614 (N.D. Ohio Sep. 30, 2010).
[9] Order granting Motion to Compel Discovery, Third Judicial District Court, No. 81-CR-09-1180, State of Minnesota v. Carney-Blount

possibility of nude photos created on the phone by its owner. We discussed the protocol prescribed in my services agreement. Unfortunately, I did encounter such photos. I contacted him first as a courtesy and then contacted my local law enforcement agency to take possession of the device. I completed a secure wipe of my processing computer's hard drive to render any data forensically unrecoverable, in accord with law enforcement's instructions.

In the second case, a prosecutor had provided voluminous discovery to defense counsel (my client). Digital photographs were among them. My client made these available to me via Dropbox. I paid no attention to file names when I was reviewing the discovery, and so was shocked to discover an image of child pornography on my screen (and in my own Dropbox account). The file in question had some variation of the phrase "child pornography" as part of the file name, which should have served as a warning to all of the parties involved in the handling and transfer. Again, I followed my protocol. First, I placed a courtesy call to my client and then to the FBI field office local to me. I was instructed by the special agent to delete the image, and he referenced the safe harbor provision of 18 U.S.C. § 2252(c).

In the third case, an attorney had provided her client's phone to me via courier. She had read my contract and raised no concerns. The phone, she said, had already been in the custody of law enforcement, so neither of us had even considered the possibility of contraband. I performed an extraction and returned the device via Fedex overnight. A few days later, when I began examining the phone, I encountered what I believed to be contraband. Again, I followed my protocol (a courtesy call first to the client, followed by a call to law enforcement). In this instance, my local ICAC liaison consulted with our local FBI field office, and requested a copy of the extraction, and instructed me to delete the original.

My client in this last example initially and strongly believed that I was not required to contact law enforcement and did not believe she needed to notify law enforcement about the device that was now in her office. Citing to Ethics 8/76B,[10] concerning whether a lawyer has an obligation to reveal a client whereabouts when they are a fugitive, she believed she had an obligation to keep the phone privileged. She also cited E-85-10, believing she should keep the

[10] "If the attorney is required to reveal the client's whereabout by court order so that DR 4-101(c)(2) applies, but the attorney's knowledge qualifies as privileged, s/he could still resist disclosure under Wis. Stat. sec. 905.03(3)."

phone privileged, because it was possible evidence of a past crime, not an ongoing or future crime. She believed these perceived obligations transcended to me, as her agent.

Likewise, another client took exception to the proviso in my contract. He wrote, "As a contractor working for me on behalf of the client, you become part of our circle of attorney/client confidentiality. If you discover something illegal on my client's device, I can't have you making a report to the police. The same as if I know that my client did something illegal, I'm not allowed to report them to the authorities." [11]

Respectfully, I submit that the foregoing arguments in support of not contacting law enforcement by the attorney or his or her agent (*e.g.,* digital forensics expert) are mistaken. These arguments fail to distinguish between knowledge of a client's past crime and the preset committing of a crime by the attorney or the attorney' agent in possessing, producing, or transporting contraband.[12]

Section 119 of the Restatement Third, The Law Governing Lawyers, provides that a lawyer must notify prosecuting authorities of the lawyer's possession of the physical evidence of a client crime:

> With respect to physical evidence of a client crime, a lawyer: (1) may, when reasonably necessary for purposes of the representation, take possession of the evidence and retain it for the time reasonably necessary to examine it and subject it to tests that do not alter or destroy material characteristics of the evidence; but (2) following possession under Subsection (1), the lawyer must notify prosecuting authorities of the lawyer's possession of the evidence or turn the evidence over to them.[13]

---

[11] I did not strike the clause in the agreement, and will decline work if a client were to insist.

[12] As for the fugitive client analog offered by one of the attorneys, *supra,* that fails for the same reason in that it doesn't distinguish between knowledge of a fugitive client's location and the crime of providing aid and harboring a fugitive by the attorney.

[13] *See also* ABA Standards for Criminal Justice: Defense Functions §4-4.6, which advises that counsel can receive an item which constitutes contraband "for a reasonable period of time" if counsel, *inter alia*: "reasonably fears that return of the item to the source will result in the destruction of the item"; "intends to test, examine, inspect or use the item in any way as part of defense counsel's representation of the client"; or the item cannot be returned to its source."

During my research, I have found very little on the subject of an attorney's obligations in these circumstances. As noted with the ***Flynn*** case, *supra,* some states create a privilege for certain persons to possess contraband and, because the Adam Walsh Act is construed as applying to Federal judicial proceedings with regard to the handling of contraband by the defense, state law is not preempted.

I did, however, find an interesting *Above the Law* blog post, in which the author construed 18 U.S.C. § 2252, which criminalizes anyone who "knowingly possesses" contraband, as a strict liability offense for attorneys, subject to the safe harbor provision of three or less images § 2252(c).[14] The author wrote, "At the moment when your computer — or a computer in your custody or control — has child pornography on it, you knowingly possess it." He continued, "There's no 'I didn't possess it for a creepy reason' defense in the statute . . . So assuming you have more than three images, what are your options?"

However, I think that author has misconstrued the statute, which, owing to a judicial precedent, is subject to a more reaonable construction. In United States v. X-Citement Video, Inc.,[15] the Supreme Court considered subsections (1) and (2) of the same statute, and inferred a scienter element, such that a defendant should not be liable without wrongful intent. The high Court relied on Staples v. United States, for the proposition that the standard presumption in favor of a scienter requirement should apply to each of the statutory elements that criminalize otherwise innocent conduct.[16]

---

[14] Matt Kaiser, A Child Pornography Puzzle, Above the Law (Nov. 12, 2015), last retrieved March 01, 2025 from https://abovethelaw.com/2015/11/a-child-pornography-puzzle/

[15] 513 U.S. 64 (1994)

[16] 511 U. S. 600, 619. *And see* State v. Schaefer, 2003 WI App 164, 266 Wis. 2d 719, 668 N.W.2d 760, (Criminal responsibility may not be imposed without some element of scienter, the degree of knowledge that makes a person legally responsible for the consequences of the person's act or omission.)

Another commentator to consider the issue in the context of representing a minor victim wrote, "[T]here is no codified safe harbor for the possession or receipt of sexually explicit images by counsel . . . At a minimum, counsel . . . should report the sexually explicit images . . . to the Cyber Tipline of the National Center for Missing and Exploited Children referenced in 18 U.S.C. §2258 and report the images to federal law enforcement. Further, if law enforcement declines to prosecute, counsel should ask the Court to escrow the images upon initiating a civil legal action."[17]

There are few examples in the criminal law where a statute applies in such a way that creates an affirmative obligation to act. I have not come across any cases that have explored this academic facet of the Federal possession prohibition, but I would contend that, once a person becomes aware that he or she is in possession of contraband, an affirmative duty to dispossess himself or herself of the contraband is triggered. Other commentators have come to similar conclusions.[18] While the law does not prescribe the period of time that must past when scienter attaches, I would expect courts to apply a reasonableness standard.

I should clarify here that, while an attorney (and his or her agent) is required to dispossess himself or herself of the contraband, the lawyer is still bound to protect the client's confidence. These two obligations may come into conflict, especially where the attorney know

---

[17] Russell Bogard, *Representing Teen Victims of Online Pornographic Postings: Litigation Challenges and Strategies,* 18 NYLitigator 1, New York State Bar Ass'n, 2013, last retrieve 01 March 2025 from https://nysba.org/NYSBA/Publications/Section%20Publications/Commercial%20and%20Federal%20Litigation/NY%20Litigator/PastIssues2000present/Summer%202013/NYLitSum13.pdf#page11

[18] *See, e.g.,* Matthew L. Mitchell, "What to do when your client discovers child pornography on workplace computers?" 56 Boston Bar Ass'n 3, 2012, last retrieved March 5, 2025 from https://bostonbar.org/journal/what-to-do-when-your-client-discovers-child-pornography-on-workplace-computers/; see also H. Michael Steinberg, *Defending Against Sex Crimes — Understanding Your Rights During the Investigation Phase,* ("One principle emerges clearly from the case law: When the lawyer takes physical possession of incriminating evidence, he has an affirmative duty to give the incriminating evidence to the proper authorities."), last retrieved March 05, 2025 from https://www.colorado-sex-crimes-lawyer.com/the-sex-crimes-investigation-phase-issues-and-tactics/colorado-criminal-law-defending-against-sex-crimes-investigations-understanding-your-rights-during-the-investigation-phase

that surrendering a device that contains contraband to law enforcement is tantamount to exposing the clint (because law enforcement may be able to independently identify the owner of the computer or phone). But, even as an attorney is required to protect the client's confidence, neither the attorney nor his or her agent should continue to possess, reproduce, transport, or tamper with the contraband (except to the extent that 18 U.S.C. § 2252 authorizes destruction of three or fewer images).

CONCLUSION

An attorney or his agent, who, comes into inadvertent possession of contraband, is not privileged to hold on to the evidence, and must turn it over to law enforcement after a reasonable period of non-destructive inspection. The moment that knowledge is attained, scienter attaches for the willful failure to execute this affirmative duty. Likewise, the attorney cannot expect his agent (*e.g.,* digital forensics examiner, private investigator, or paralegal) to commit the crime of possessing, reproducing, or transporting contraband in violation of Federal law.

As a best practice, discuss with your client whether contraband may exist on a device before you provide the device to a digital forensics examiner.[19] Likewise, discuss with your examiner what protocol will be observed if contraband is encountered, whether the case civil or criminal. The details of the examiner's protocol for incident handling should be memorialized in the services contract. You may wish to instruct the examiner that dispossession does not mean the examiner is required to affirmatively disclose the client's identity or other confidential details

[19] N.B., the risk may be substantially greater when working with devices that belong to adolescents who may be exchanging lewd images, and who may be reluctant to be transparent with the attorney regarding such activities.

of the engagement that would otherwise be protected under the work product doctrine. Nevertheless, law enforcement may demand the examiner to disclose the identities of both you and your client, and may demand the passcode for unlocking the device, against which your client's Fifth Amendment rights cannot be vicariously invoked by the examiner. Likewise, because the attorney-client privilege has not yet been extended to the Wisconsin attorney's experts, your examiner will be unable to invoke the privilege on your client's behalf.[20] In such instances, the interests of your client and the interests of the examiner may diverge.

[20] WI stat. § 905.03(3). *See also* Attorney-Client Privilege and the Kovel Doctrine: Should Wisconsin Extend the Privilege to Communications with Third-Party Consultants? , 102 Marq. L. Rev. 605 (2018).