



Creating Opportunity Through Criminal Record Clearing

Equal Justice Conference Preconference

May 8, 2019 | Louisville, KY



Record clearing, through expungement, sealing and other legal remedies, is a perfect fit for pro bono initiatives, as well as law school clinics, civil legal aid programs, and defender programs. The demand for these legal services is overwhelming, as an estimated one out of three American adults has a criminal record, many of which are eligible for clearing. Representation is usually brief and time limited, and the cases are relatively easy. But there are complex issues that can arise in the record clearing world.

This preconference will address challenges and opportunities common across the fifty states in establishing and growing an expungement/sealing practice. The day-long session will include the following topics: barriers to growing a practice; ensuring record clearing is fully and properly implemented; navigating large-scale and complex pro bono partnerships; record clearing for immigrant clients; and moving the needle when legislative efforts stall.

Outline of the Day

**8:30-10:00 a.m. Breakfast & Introductions: Record Clearing Basics
and Report Out from the Field**

During this session, there will be an overview of record clearing basics to set a foundation and common understanding for the rest of the day's advanced sessions. Participants will have an opportunity to introduce themselves and speak briefly about their practice, as well as what they are hoping to get out of the preconference.

Presenter: Janet Ginzberg, Senior Supervising Attorney, Community Legal Services

10:00-10:30 a.m. Record Clearing for Immigrant Clients: Risks & Opportunities

When people who are not citizens wish to get their records cleared, they may not be aware that it can have implications for removal, applications for citizenship, and more. Advocates must be prepared to properly screen for these issues, counsel clients in consultation with immigration lawyers, and take proactive steps to protect their clients' interests. This session will review best practices for representing immigrant clients in the record clearing process.

Presenter: Seth Lyons, Staff Attorney, Community Legal Services

10:30-10:45 a.m. Break



Creating Opportunity Through Criminal Record Clearing
Equal Justice Conference Preconference
May 8, 2019 | Louisville, KY



10:45-11:45 a.m. Record Clearing Aftercare

You've filed a petition for expungement/sealing, and it was granted by a judge. What comes next? This session will explore the ways record information is collected and disseminated, and what advocates must do to ensure records are cleared from as many sources as possible. This will include discussion of commercial background check companies, FBI records, court and law enforcement databases, and websites such as mugshots.com.

Presenters: Sharon Dietrich, Litigation Director
Seth Lyons, Staff Attorney, Community Legal Services

11:45 a.m.-12:45 p.m. Lunch

12:45-1:30 p.m. Scaling up Pro Bono Partnerships: Challenges & Opportunities

Record clearing can be a great avenue for working successfully with pro bono partners. But how to manage such partnerships when there is an overwhelming need for services and volunteers? This session will explore several examples of large-scale pro bono partnerships to bring legal help to thousands of people who would otherwise go without. The benefits and challenges of such large-scale partnerships will be discussed.

Presenters: Leigh Wicclair, Pro Bono Program Manager, NC Pro Bono Resource Center
Terri Hendley, Pro Bono Coordinator at Troutman Sanders
Jamie Gullen, Supervising Attorney, Community Legal Services

Moderator: Seth Lyons, Staff Attorney, Community Legal Services

1:30-2:45 p.m. Barriers to Growing a Record Clearing Practice

This session will cover several of the most common barriers to starting or scaling up a record clearing practice, including access to court records, criminal court debt, filing fees, and how to effectively provide pro se assistance. There will be an opportunity to hear about best practices in various states and brainstorm ideas for overcoming barriers.

Presenters: Kristy Vick-Stratton, Staff Attorney, Legal Aid of Kentucky
Lisa Foster, Co-Director of the Fines & Fees Justice Center
Jamie Gullen, Supervising Attorney, Community Legal Services

Moderator: Janet Ginzberg, Senior Supervising Attorney, Community Legal Services

2:45-3:00 p.m. Break



Creating Opportunity Through Criminal Record Clearing
Equal Justice Conference Preconference
May 8, 2019 | Louisville, KY



3:00-4:30 p.m. Moving the Needle on Record Clearing Reform

While many states have been passing new legislation to increase access to record clearing, some states are stuck without viable legislative strategies, and others may have reached a plateau for legislative reform. Yet there is much advocates can do to continue pushing for expanded access to record clearing even in such an environment. This session will explore a variety of avenues including litigation, partnering with prosecutors' offices, using communications to shift narratives, working with researchers, and forging relationships with helpful partners including business leaders, law enforcement, and more.

Presenters: Holly Harris, Executive Director, Justice Action Network
Akil Roper, Vice President & Assistant General Counsel, Legal Services of New Jersey
Emma Goodman, Staff Attorney, Special Litigation Unit, Legal Aid Society
Sharon Dietrich, Litigation Director, Community Legal Services

Moderator: Jamie Gullen, Supervising Attorney, Community Legal Services

4:30-5:00 p.m. Debrief & Close Out

Participants will discuss in small groups their takeaways from the day and identify next steps they will take back with them to their practices.

5:00 p.m. Meet in hotel bar for an informal happy hour to keep the conversation going!



Creating Opportunity Through Criminal Record Clearing

Equal Justice Conference Preconference

May 8, 2019 | Louisville, KY



Participants List

Natasha Alladina

Georgia Justice Project
Atlanta, GA
natasha@gjp.org

Adrian Barr

Prairie State Legal Services
Bloomington, IL
abarr@pslegal.org

Erica Briant

Legal Aid Of Southeastern Penn
Norristown, PA
ebriant@laspp.org

Ginny Mayo Brimm

West TN Legal Services
Jackson, TN
ginny@wtls.org

Caitlin Brown

Community Legal Services
Philadelphia, PA
CBrown@clsphila.org

Christine Campbell

Kansas Legal Services
Wichita, KS
campbellc@klsinc.org

Hsindy Chen

Georgia Justice Project
Atlanta, GA
hsindy@gjp.org

Richard Cozzola

Legal Assistance Foundation
Chicago, IL
rcozzola@lafchicago.org

Leslie Crow

Lone Star Legal Aid
Houston, TX
lcrow@lonestarlegal.org

Renee Danser

The Access to Justice Lab
at Harvard Law School
Cambridge, MA
rdanser@law.harvard.edu

Sharon Dietrich

Community Legal Services
Philadelphia, PA
SDietrich@clsphila.org

Erin Donahue-Koehler

Georgia Justice Project
Atlanta, GA
erin@gjp.org

David Farley

Kentucky Legal Aid
Bowling Green, KY
dfarley@klaid.org

Lisa Foster

Fines & Fees Justice Center
Washington, DC
lfoster@finesandfeesjusticecenter.org

Janet Ginzberg

Community Legal Services
Philadelphia, PA
JGinzberg@clsphila.org

Emma Goodman

The Legal Aid Society Criminal
New York, NY
egoodman@legal-aid.org

Jamie Gullen

Community Legal Services
Philadelphia, PA
JGullen@clsphila.org

Marilyn Harp

Kansas Legal Services
Topeka, KS
harp@klsinc.org

Holly Harris

Justice Action Network
KY / DC,
holly@justiceactionnetwork.org

Terri Hendley

Troutman Sanders
Atlanta, GA
terri.hendley@troutman.com

Judy Kuhns**Ashley Lee**

Kentucky Legal Aid
Bowling Green, KY
alee@klaid.org

William Lonn

Still She Rises, Inc.
Tulsa, OK
williaml@stillshe rises.org

Samuel Lowe

Kentucky Legal Aid
Bowling Green, KY
slowe@klaid.org

Seth Lyons

Community Legal Services
Philadelphia, PA
slyons@clsphila.org

Mitch

Neighborhood Law Clinic, University of
Wisconsin-Madison Law School
Madison, WI
mitch@wisc.edu

Jarrell Mitchell

Neighborhood Legal Services
of Los Angeles County
Pacoima, CA
jarrellmitchell@nlsa.org

Jennifer Modell

Neighborhood Legal Services
Pittsburgh, PA
modellj@nlsa.us

Nathan Moorehouse

Kentucky Legal Aid
Madisonville, KY
nmoorhouse@klaid.org

Aizul Ortega

Travis County Law Library
Austin, TX
Aizul.Ortega@traviscountytx.gov

Rob Poggenkloss

Iowa Legal Aid
Des Moines, IA
rpoggenkloss@iowalaw.org



Creating Opportunity Through Criminal Record Clearing
Equal Justice Conference Preconference
May 8, 2019 | Louisville, KY



Participants List

Faye Rachlin

Community Legal Aid
Worcester, MA
frachlin@cla-ma.org

Samantha Reiser

Legal Action Center
New York, NY
sreiser@lac.org

Satcha Robinson

Legal Aid Society of DC
Washington, DC
srobinson@legalaiddc.org

Karen Robinson

Volunteer Lawyers For Justice
Newark, NJ
krobinson@vljnj.org

Akil Roper

Legal Services of New Jersey
Jersey City, NJ
aroper@lsnj.org

Sarah Sallen

Legal Assistance Foundation
Chicago, IL
ssallen@lafchicago.org

Brenda Smeeton

Georgia Justice Project
Atlanta, GA
brenda@GJP.org

Justin Synhorst

White & Case
Houston, TX
justin.synhorst@whitecase.com

Larri Thatcher

Legal Aid Society
Orlando, FL
lthatcher@legalaiddcoba.org

Sonja Tonnesen

Root and Rebound
Oakland, CA
stonnesen@rootandrebound.org

Kristen Uhler-McKeown

Equal Justice Works
Washington, DC
kuhlermckeown@equaljusticeworks.org

Kristy Vick-Stratton

Kentucky Legal Aid
Bowling Green, KY
kvickstratton@klaid.org

Elizabeth Wehner

Legal Aid of West Virginia
Charleston, WV
ewehner@lawv.net

Sarah Whittington

Justice and Accountability Center
New Orleans, LA
Sarah@JACLouisiana.org

Leigh Wicclair

NC Pro Bono Resource Center
Raleigh, NC
leigh@ncprobono.org

Employment Rights and Criminal Records

May 9, 2018



Employment Law: The Basics

- **“Employment at Will”**

- The general rule is that the employer or the employee can terminate the relationship for any reason and at any time
- This means that employers can hire and fire people for unfair reasons, or no reason at all

Employment at will does not apply to:

- Workers covered by union contracts;
- Civil service workers; and
- Workers with contracts (very rare)

In these cases, termination usually limited to cases where employer has “just cause,” and employee may be entitled to a hearing.

Exceptions to Employment at Will Principle

- Employment discrimination laws (federal, state or local)
- Other statutes, e.g. Family and Medical Leave Act
- Retaliation for making an employment law or benefit claim

Barriers to Employment: Criminal Records

HUGE PROBLEM! The single largest category of employment cases that CLS sees.

- Some jobs are barred by law.
- Others, employers won't hire a person with a criminal record.
- Employers have easy access to records.

Barriers to Employment

- Some laws prohibit employers from hiring people with certain convictions
- Includes occupational licenses
- Check out criminal record restrictions before training for a new field

Strategies for Helping Ex-Offenders Get Employment

- Assert legal rights against being rejected for (or fired from) jobs
- Job search techniques – answering questions, bonding, etc.
- Impact Litigation/advocacy
- “Clean up” the record, if possible
- Representation before licensing boards

Legalities: Ex-Offenders Do Have Employment Rights

Employment at will does not always carry the day!

Relevant laws:

- 1) Title VII (discrimination law)
- 2) State law on considering criminal records
- 3) Philadelphia Fair Hiring Ordinance
- 4) Fair Credit Reporting Act

TITLE VII

- Title VII prohibits racial discrimination, including policies/practices that have a “disparate impact.”
- More African Americans and Hispanics have criminal records than others.
- Therefore, employers must have a “business necessity” for the policies.

TITLE VII

Factors to be Considered

EEOC says employers must consider:

- 1) Nature and gravity of offenses;
- 2) Time that has passed since the conviction and/or sentence;
- 3) Nature of the job.

TITLE VII

General Rules

- Employers cannot have blanket policies requiring “clean criminal records.”
- Arrests without convictions usually cannot be considered. Employers are supposed to look into situation, not rely on fact of arrest.

TITLE VII

Enforcement

- File a race discrimination charge at the EEOC within 300 days
- Lawsuit can be filed if EEOC charge fails, but very difficult and costly.
- Don't underestimate value of just discussing law with employers.

State and Municipal Remedies

Your Mileage May Vary

Pennsylvania Remedies

Pennsylvania Human Relations Act

Criminal History Records Information
Act

Philadelphia Remedies

Fair Criminal Records Screening Standards (AKA Ban the Box)

- Employers may not ask about criminal records until after a conditional offer of employment
- Employers may not consider arrests
- Employers may not consider convictions that are older than 7 years (unless mandated or authorized by law or regulation)

State Law

Enforcing Legal Rights

- No EEOC jurisdiction; only lawsuit.
- CLS writes demand letters.
- Consider bringing state law to employer's attention.
- Representation before licensing boards

Systemic Reform

Legislative activity

Advocacy with local and/or state agencies

Challenges to state laws

FCRA - Employers

- Applies only when employers use private background check companies.
- Duties on employers
 - Must get written authorization
 - Must provide a copy five days before action taken.
 - Must notify person that action was taken based on the report.

FCRA

Background Check Companies

- May not report arrests that are more than 7 years old (no time limit on convictions)
- Must use reasonable procedures to insure maximum possible accuracy
- Must re-investigate if person challenges record.

Other Strategies to Help Ex-Offenders Find Jobs

- Talk with them about how to answer applications (read the question carefully, answer it accurately, and explain if helpful).
- Job development to focus on employers who will hire ex-offenders (or avoid those who can't or won't).

How Should One Deal with Criminal Record on Applications?

- Read questions carefully and don't give more information than required.
- Be prepared to talk about record even if application doesn't require disclosure.
- Consequences to lying on application (e.g. provides separate grounds for termination not protected by the law, can lead to denial of unemployment compensation).

SCALING UP RECORD CLEARING PRO BONO PARTNERSHIPS

TIPS AND STRATEGIES TO COMBAT PRO BONO CHALLENGES AND MAXIMIZE OPPORTUNITIES THROUGH MEANINGFUL PROJECT DESIGN, RECRUITMENT, AND RETENTION

RECORD CLEARING PRO BONO CHALLENGES AND OPPORTUNITIES:

CHALLENGE

Attorney volunteers are over-worked and over-obligated.

Some volunteers lack skills or experience with record clearing: 69% of attorneys who take a pro bono case do so within their practice area.

There are limited staff resources, time, and buy-in to manage pro bono projects.

It is difficult to recruit volunteers.

Record clearing work appears to be a partisan issue; some firms want to steer clear of second chance work.

OPPORTUNITY

Record clearing lends itself to limited scope pro bono legal service.

Record clearing and collateral consequences work matters! Plus, it's getting a lot of media attention.

Pro bono attorneys report being most motivated by empathetic or ethical impulses, such as reducing social inequalities.

There are lots of record clearing resources and training modules available.

With the right project design and partnership, pro bono can increase staff resources.

There are potential partnerships that have untapped volunteer resources: large firms, corporate counsel, and other transactional attorneys.

Educate the partner firm about how record clearing is a bipartisan effort.

**CONNECT
WITH US**



facebook.com/ncprobono



twitter.com/ncprobono

linkedin.com/company/ncprobono



ncprobono.org



PO Box 2448

Raleigh, NC 27602

TIPS FOR PROJECT DESIGN

- Get clear on your needs and what resources you can devote to the project: does this particular project lend itself to pro bono participation? If the entire project isn't a good fit (it's too complicated or difficult to manage), is there a task that pro bono attorneys may support?
- Invest in the volunteer experience – make your ultimate goal to create long-term partnerships and repeat volunteers; process creation may take more resources on the front-end but utilizing pro bono attorneys will save resources long-term.
- Decide in advance who will be your organization's point person for questions and issues that come up during completion of the project.
- Prepare a timeline with deadlines and designate who is responsible for each task.
- Create a project evaluation process and rely on this process to continuously test and improve the project.

TIPS FOR VOLUNTEER RECRUITMENT

- Relationships, relationships, relationships.
- Marketing matters! Develop your project "elevator speech" and get all staff on the same page.
- Develop a specific task for volunteers. Do not start recruiting volunteers without having a plan in place for utilizing their work.
- Get your "ask" into the right hands at the firm – who is the firm or corporation's local, or national, "pro bono cheerleader"?
- Explore bar associations, the Association of Pro Bono Counsel, and the Association of Corporate Counsel.

TIPS FOR BEGINNING THE PRO BONO PARTNERSHIP

- Create a Partnership Agreement (a.k.a. Memorandum of Understanding).
 - Really. Please. Every time. Even when you have a longstanding relationship.
 - State in detail what each person is responsible for and define vague terms like "support and mentorship."
- Ask questions about the firm or volunteer's motivations and expectations for the project:
 - Tell me about your firm's pro bono program. What other projects are you working on right now?
 - What about this project most appeals to you?
 - What do you need from me to ensure that this is a positive experience for you and your colleagues?
- Be direct about YOUR needs.
- Be direct about the project's "pain points" – elicit help from the firm, if possible.

TIPS FOR PRO BONO PROJECT TRAINING

- Design trainings that are succinct and interactive.
- Design thoughtful, concise materials that volunteers can refer to throughout the project.
 - DO include only information that the volunteer needs to complete the project.
 - DO NOT email "everything but the kitchen sink" and rely on volunteers to sift through materials to determine significance.
 - DO include as many sample materials as possible (emails, document requests, petitions, even scripts to use with clients!).
 - DO spend time on cultural competency, ensuring that the training is tailored to the volunteers' level of experience working with vulnerable populations.

TIPS FOR RETAINING VOLUNTEERS

- Find ways to highlight volunteers.
 - Social media, your website, bar award nominations, etc.
- Give a special designation to committed volunteers and elicit these volunteers to help with recruitment, training, and project logistics.
 - For example, Expungement Pro Bono Project Advisory Board.
- Share project metrics with volunteers – volunteers are invested in the outcome.
- Say thank you!
- Require a specific time commitment in exchange for training.

Record Clearing for Immigrant Clients: Risks & Opportunities

May 8, 2019

Seth Lyons

slyons@clsphila.org



Background on Convictions and the INA

Criminal convictions, even convictions that have been expunged, can have negative immigration consequences for anyone who is not a citizen of the U.S. That includes:

- **Lawful Permanent Residents**
 - “LPRs”
 - Green card holders
- **Asylees**
- **Refugees**
- **Temporary visas**
 - U, T, H-2B
- **Undocumented individuals/families**
 - “EWI”



Statutorily Defined Grounds of Removability

Immigration definition of a conviction:

- A formal admission or adjudication of guilt, combined with some restraint on the defendant's liberty
- Includes some diversion programs

Grounds of Removability (defined by the Immigration and Nationality Act)

- Aggravated felony
 - List of 20+ crimes
 - Many of them are not felonies
 - Many of them are not “aggravated”
 - Many depend on sentence (actual or possible) or amount of \$\$ at stake
 - Eliminate access to discretionary relief and bond
- Crimes Involving Moral Turpitude (“CIMTs”)
 - Vague
 - Timing matters



Criminal-Record-Based Enforcement Priorities

- **Separate from the grounds of removability**
- **Changes under current administration**
 - Main focus used to be on people with certain types of convictions: felonies and serious misdemeanors
 - Executive Order 13768 (1/25/17) → enforcement priorities include anyone with an arrest record, even if no conviction



Expunging Records for Non-Citizens

- **Two Main Questions:**
 - 1) Can record-clearing help address immigration consequences?
 - 2) Are there immigration-related risks to filing petitions on behalf of immigrants?



Expunging Records for Non-Citizens

- Factors to consider:
 - 1) Purpose of expungement (immigration issues or traditional collateral consequences?)
 - 2) Immigration status
 - 3) The type of record-clearing mechanism



Immigration Benefits of Record-Clearing

- Two main categories of record-clearing tools for immigration purposes:
 - **1) Standard expungements, sealing, etc.**
 - Hide or eliminate record, but do not change the fact of a conviction
 - Do not generally help for immigration purposes
 - **2) Post-conviction relief that does something to undermine, undo, or change the conviction**
 - E.g. Pardons, some vacatur, sentence/grade modifications
 - Often do help for immigration purposes



Immigration Benefits of Record-Clearing

Standard Expungements/Sealing → Do NOT usually help with immigration consequences

- Legally → expunged convictions still count as convictions for immigration purposes. *In re Pickering*.
- Logistically → Likely don't eliminate info from ICE database
- Exception → Some DACA applicants, drug possession convictions in 9th Circuit prior to 2011



Immigration Benefits of Record-Clearing

Tools that alter or undo the conviction → Often can help with immigration consequences

- Pardons → INA says that convictions pardoned by governor or president will not count as convictions for immigration purposes
- Vacatur/PCRA → If conviction is vacated due to defect (not humanitarian reasons)
- Sentence/grade modifications
 - e.g. Prop 47 in California (“wobblers”)
 - Some grounds of removability depend on sentence length (actual or potential)



Addressing Collateral Consequences for Non-Citizens

Effectiveness of record-clearing for addressing barriers to housing, employment, etc. may depend on client's immigration status

- **Documented immigrants** → benefits of record-clearing are basically the same as for US Citizens
- **Undocumented immigrants** → less clear
 - For most jobs that conduct background checks, lack of work authorization will be more of a barrier to employment than their criminal record
 - Potential exceptions for certain types of jobs or occupational licenses?



Potential Risks of Record-Clearing

1) General risk of filing petitions on behalf of immigrant clients or bringing them to court

- ICE at courthouses
- Public filings

2) Record-clearing may complicate immigration proceedings

- Does record-clearing tool eliminate court documents?
 - For affirmative immigration applications (like applications for citizenship), the applicant has the burden of proving there is not a bar to eligibility
- Still have to disclose expunged records



Best Practices – Before Filing

- 1) Screen for citizenship status?
- 2) Advise client that clearing a criminal record—even a conviction—will likely **not help with immigration issues** (like applying for permanent residency or citizenship, or coming back into the country from abroad)
- 3) Discuss client's goals for clearing record → address an immigration issue or traditional collateral consequences?



Best Practices – Before Filing (cont.)

4) Assess possible immigration risks

- *Does the client have an active bench warrant?*
- *Has the client been previously removed?*
- *Has the client ever had a PFA order entered against them?*

5) Weigh risks with benefits. If any red flags, consult with an immigration attorney *before filing*



Best Practices – Filing & Court Procedures

- 1) Consider using your organization's address on the petition
- 2) Make sure your client has obtained **certified dispositions** BEFORE THE PETITION IS GRANTED
- 3) If possible, don't bring your client to court



QUESTIONS?

????????





Navigating the Complexities of Expunging Records for Immigrant Clients

Arrest and conviction records create barriers to employment, housing, and other basic needs and services. For immigrant clients, a record may be even more damaging, as it can lead to immigration detention, mandatory deportation, and permanent lifetime banishment.

Filing some types of record-clearing petitions on behalf of immigrant clients may pose immigration risks while providing limited benefits. Other record-clearing mechanisms can actually help clients obtain crucial immigration relief. This guide examines how advocates can assess the risks and rewards for non-citizens seeking to clear their records, and offers strategies for protecting these clients.



Contacts:

Seth P. Lyons
Staff Attorney
slyons@clsphila.org

Sharon M. Dietrich
Litigation Director
sdietrich@clsphila.org

September 1, 2017

Millions of people in the United States, including non-citizens, suffer from the collateral consequences of having a criminal record. Even old, minor convictions or arrests not resulting in conviction can make finding a job or housing difficult. Record clearing through expungement, sealing, pardons, vacatur, habeas, or other mechanisms can be effective tools for relieving these barriers. **However, the recent changes in immigration enforcement priorities make it crucial for advocates to understand the risks and rewards of clearing criminal records for non-citizen clients.**¹ Filing expungement petitions on behalf of non-citizens may complicate immigration proceedings by eliminating required documentation, and advocates should at least consider whether filing a petition or bringing a client to court will risk contact with immigration authorities.

As described below, any arrest or contact with the criminal justice system—even without a conviction—could lead to detention and removal of undocumented immigrants. Criminal records can also make documented immigrants (like green card holders) deportable, even for old and minor convictions. For example, any “aggravated felony” conviction—which is defined by federal law and need not be classified as a felony under state law—can subject non-citizens to removal and bar them from certain kinds of immigration relief, like cancellation of removal, voluntary departure, and asylum. Vaguely defined “crimes of moral turpitude,” domestic violence offenses, drug convictions, and even some non-conviction records can also put non-citizens at risk.

On the other side of the scale, the benefits of clearing an immigrant’s record largely depend on that person’s immigration status and the type of record-clearing mechanism available. **Importantly, standard expungement petitions rarely help with immigration-related issues,** like applications for citizenship/naturalization, green cards, or other visas, or with re-entering the country. However, some forms of post-conviction relief that attack the validity of the underlying conviction can provide crucial immigration-related benefits (see below).

Furthermore, the effectiveness of record clearing on employment, housing, and other collateral consequences may depend on the client’s immigration status. For example, although they may help some immigrant clients overcome barriers to employment, expungements do not necessarily benefit undocumented workers whose immigration status generally prevents them from working in jobs that conduct criminal background

This guide uses “expungement” as a general term to refer to standard record-clearing petitions that do not attack the validity of a criminal conviction, but simply erase or seal the criminal record information. Different states use different terms for these procedures, including sealing, expunction, erasure, shielding, etc., and these remedies may function somewhat differently.

checks anyway. With some exceptions,² **the immigration risks of filing a standard expungement petition likely outweigh the benefits for most undocumented clients.**

In general, the risks and benefits of record clearing **may hinge on whether the client is a U.S. citizen, an undocumented immigrant** (sometimes referred to as unauthorized or illegal), **or a documented immigrant** (which includes Lawful Permanent Residents/green card holders, asylees, refugees, and visa-holders).

Status	<i>U.S. Citizen</i>	<i>Documented</i>	<i>Undocumented</i>
Risks	Low to none	Low to high	Medium to high
Benefits for collateral consequences	High	High	Low to none
Benefits for immigration issues	n/a	Low to high	Low to high

The following steps are intended to provide a basic overview of the issues advocates need to consider when deciding whether expungement is appropriate for an individual client. **Because immigration enforcement priorities are constantly changing, however, it is highly recommended that advocates continue to consult with local immigration experts even after doing a risk assessment based on the information below.**

Can record-clearing help with immigration issues?

In most states, record-clearing petitions simply erase criminal record information—often relating to non-convictions—or seal it from public view. These standard record-clearing tools rarely provide any benefit for immigration purposes. First, with very few exceptions, expunged convictions still count as convictions for immigration purposes. Second, Immigration and Customs Enforcement (ICE) maintains its own records that are unaffected by state-level expungements. **The main exception to this rule is for Deferred Action for Childhood arrival (DACA) applicants**, for whom expunging certain convictions may remove specific bars to eligibility.³

However, some states have record-clearing mechanisms that allow the petitioner to challenge the underlying validity of a conviction, or otherwise mitigate its immigration consequences. Common examples include pardons, habeas petitions, and vacatur. In California, for example, people can petition the court for a sentence modification—even long after the sentence has been imposed—to downgrade the offense from a felony to a misdemeanor or reduce a sentence from 1 year to 364 days.⁴ **This post-conviction relief can actually eliminate immigration consequences for convictions that previously triggered removability.**

Expungement advocates should consult with local immigration attorneys to see if your state's record-clearing laws can protect clients from adverse immigration consequences!



Expunging Records for Immigrant Clients

Before Filing a Petition

1. **Explain that expunging a criminal record likely will not help with immigration consequences, even though it may carry other, non-immigration benefits.**

Immigration and Customs Enforcement (ICE) maintains its own database of arrest records that is unaffected by standard record clearing tools, like expungement and sealing. Moreover, except for some drug offenses in the Ninth Circuit, expunging a conviction record does not eliminate the immigration consequences of that conviction. Thus, with the limited exception of some DACA applicants, expunging your client's criminal record will not make them less likely to be deported or more likely to be eligible for permanent residency, citizenship, or any other immigration relief. In fact, as discussed below, clearing a non-citizen's record could create unintended problems for immigration purposes.

2. **Assess the risk of filing a petition by reviewing the following questions:**

- a) *Does your client have an active bench warrant?*

If so, filing a petition or bringing your client to court could result in their arrest, and potentially trigger removal proceedings. Have your client consult with a criminal defense and immigration attorney about how to deal with the bench warrant.

- b) *Has your client been previously removed?*

Re-entering the United States after a being deported can not only bar someone from certain types of immigration relief, it can lead to criminal prosecution and imprisonment. If your client has been removed before, consult with an immigration attorney before filing a petition.

- c) *Has your client ever had a protection from abuse (PFA) order entered against them?*

Criminal convictions are not the only legal proceedings that can make someone removable. Violations of protective orders can also lead to deportation. If your client has violated a protective order, there may be increased risk with bringing them to court.

3. Explain the potential risks of filing an expungement petition and help weigh these risks with the collateral consequences (barriers to employment, housing, etc.) that your client is facing.

Because of the uncertainty surrounding new ICE tactics, many advocates fear that simply filing a petition on behalf of an immigrant client could somehow alert ICE to that client's presence. Fortunately, as of the publication of this guide, we have not yet heard of a situation where filing an expungement petition triggered removal proceedings. In fact, ICE likely already knows about their record, and filing an expungement petition is not likely to affect ICE's awareness of this record one way or the other. That said, expungement petitions are public records, and it is at least worth investigating whether your local court has a policy of sharing information with immigration authorities before you file.

Moreover, in some jurisdictions, if the petition is granted, your client's criminal record will be completely destroyed. However, immigration authorities will still have a record of the initial arrest, and your client will often have the burden of proving what happened in their criminal case when applying for immigration relief, citizenship, etc. Thus, before the record is cleared, your client must obtain certified copies of their criminal record and keep them in a safe place. Make sure the certified copies include the disposition of the charges! Without a certified copy, your client may not be able to prove to immigration authorities that their arrest did not result in conviction for a removable offense, and their application for immigration relief, including naturalization, could be delayed or denied.

4. If your client has any convictions on their record, or if there are any red flags for immigration problems (e.g. undocumented client, previous removal or contact with ICE, PFAs, or bench warrants), consult with an immigration attorney *before filing*.

Because undocumented workers are not legally permitted to work anyway, criminal background checks rarely create the same barriers to employment that they do for authorized workers. With the exception of some occupational licensing applications,⁵ expungement does not generally provide a great benefit to undocumented workers. The immigration risks, however, are more pronounced, so advocates should usually consult with an immigration attorney before filing a petition on behalf of an undocumented client.

Certain convictions can also make someone removable even if they have legal status, including permanent residency (a green card). These include, but are not limited to, aggravated felonies, drug offenses, some domestic violence offenses, crimes involving moral turpitude, and firearms offenses. The crimes



that make someone removable are defined by federal statutes or case law, and do not necessarily depend on how states classify these offenses. For example, even a state misdemeanor conviction could meet the federal definition of an aggravated felony, while a state felony could have no immigration consequences. Because removable offenses differ from state to state, it is essential to consult with a local expert on criminal immigration law (sometimes referred to as “crimmigration”) when issues arise.

5. Investigate your local court’s policies on sharing information with immigration authorities.

Make sure you understand if and how the court collaborates with immigration authorities. In some jurisdictions, courts may have policies against sharing immigration status information with ICE, while in other areas information sharing may be common practice. In fact, there have been increased reports of ICE showing up at courthouses to detain non-citizens over the past several months. While most of these incidents have been directly related to criminal proceedings, expungement petitions are usually filed in criminal court, and ICE has reportedly shown up at other types of proceedings as well.

Filing & Court Procedures

1. If local rules permit, consider using your organization’s address on the expungement petition.

If ICE is monitoring court filings, using a “care of” address instead of your client’s home address could keep ICE from finding out where your client lives.

2. Make sure your client has obtained certified copies before the expungement petition is granted.

In some states, the criminal record will be destroyed almost immediately after the petition is granted, so there may not be time to obtain a certified copy after the hearing. If you file on paper only, this could be shortly after you send your paperwork to the court.

3. If possible, consider advising your client to not come to the hearing.

As discussed above, there is always some risk in bringing an immigrant client to court, especially criminal court. In Philadelphia, for example, an

expungement petition is first reviewed by a trial commissioner, and is granted if the District Attorney's office does not object. Because there is no opportunity for the client to testify at this stage, there is no reason to risk bringing the client to court.

Even if the client can testify, make sure to re-evaluate the questions above to determine whether the benefits of bringing the client to court outweigh the potential immigration risks.

Navigating the complexities of representing immigrant clients in the record-clearing context can often be difficult and time-staking. Some record-clearing mechanisms can keep clients from being deported, while others could potentially put them at risk of removal or block them from obtaining important immigration benefits. The importance of thoroughly evaluating the risks and benefits of expungement in these cases has never been more important, and advocates must do their best to guide their clients through this tricky analysis.

¹ On January 25, 2017, President Donald Trump signed an executive order entitled “Enhancing Public Safety in the Interior of the United States.” Among other things, the executive order expanded immigration enforcement priorities to include people who have “been convicted of any criminal offense,” people charged with, but not yet convicted of, any crime, and anyone who has “committed acts that constitute a chargeable criminal offense.”¹ Although these enforcement priorities do not alter the grounds of removability—the statutorily defined rules that dictate which crimes will render immigrants deportable and bar non-citizens from obtaining certain immigration relief—the changes drastically increase the risks for immigrants with criminal records. Exec. Order No. 13768, 82 Fed. Reg. 8799 (January 25, 2017), <https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united>.

² For example, occupational licensing agencies in California cannot consider immigration status but can evaluate criminal records in licensing decisions. Cal. SB 1159 (2014). For more information, see Educators for Fair Consideration, *Career License Opportunities for ALL!*, http://www.e4fc.org/images/CareerLicense_Final.pdf.

³ In addition, standard expungements of first time drug possession convictions that occurred before July 14, 2011 in every state within the 9th Circuit can also eliminate the conviction for immigration purposes. See *Helping Immigrant Clients with Proposition 47 and Other Post-Conviction Legal Options*, Californians for Safety and Justice (2016), 35, <https://www.ilrc.org/sites/default/files/resources/csj-immigrationtoolkit-final-online.pdf>.

⁴ For more information on Proposition 47 and other California record-clearing mechanisms that can provide immigration relief, see *Helping Immigrant Clients with Proposition 47 and Other Post-Conviction Legal Options*, Californians for Safety and Justice (2016), <https://www.ilrc.org/sites/default/files/resources/csj-immigrationtoolkit-final-online.pdf>.

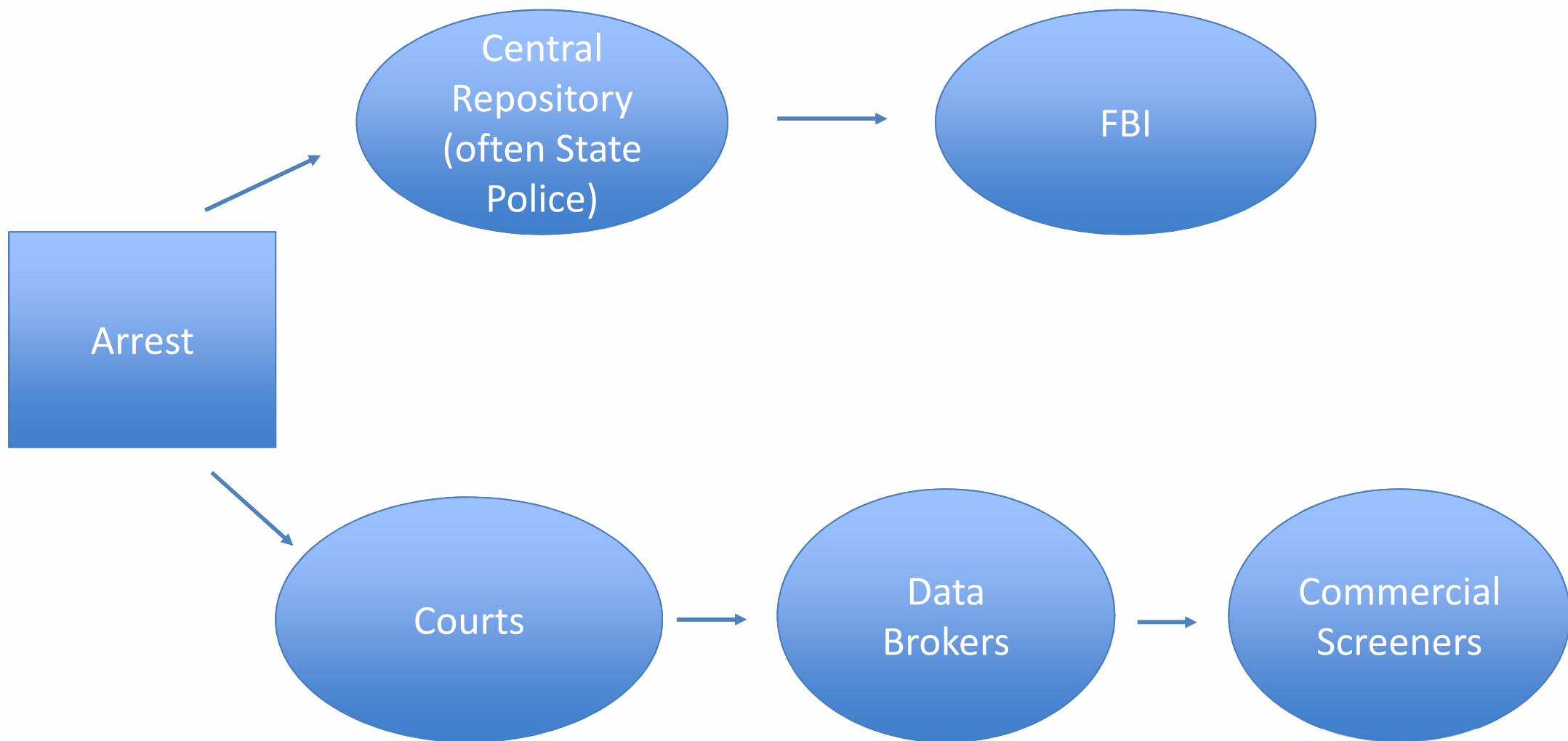
⁵ See S.B. 1159, 2013–2014 Leg. (Cal. 2014). See also Educators for Fair Consideration, *Career License Opportunities for ALL!*, http://www.e4fc.org/images/CareerLicense_Final.pdf.

Expungement “Aftercare”: What Comes Next Once the Record is Cleared?

Sharon Dietrich & Seth Lyons
May 8, 2019



Life Cycle of a Criminal Case: Arrest/Disposition/Expungement



Commercial Screeners

- **The industry is huge**, but dominated by a few big companies (Sterling, First Advantage, etc.). It's impossible to deal with all of them.
- **They tend not to refresh their data** and thus will report the expunged case (they won't know it's gone!). They claim they would remove sealed cases, if ONLY they knew!
- **Submit expungement order to**
ExpungementClearinghouse.org?



Policy Solutions for Screeners

- **PA – LifeCycle File**
 - Bulk purchasers and downstream users are required to run this computer file monthly, to eliminate expunged/sealed cases.
 - Required by contract.
- **Utah – contractual requirement that data be refreshed before being used.**



Fair Credit Reporting Act

- **Commercial screeners' legal obligations**
 - Follow “reasonable procedures to assure maximum possible accuracy” (15 USC § 1681e(b)).
 - For employment, “strict procedures” to ensure information is “complete and up to date”, unless they provide contemporaneous notice instead (15 USC § 1681k).
 - For employment, right to pre-adverse action notice (15 USC § 1681b(b)(3)).
 - Right to dispute (15 USC § 1681i).
 - Right to “full file disclosure” (15 USC § 1681g).



FCRA-based Tactics

- **Dispute a bad report.**
- **Order a “full file disclosure.”**
- **Send screeners an expungement order?**
- **FILE A LAWSUIT!** (or connect with one of the lawyers who will).



FBI Records

- **Certain types of jobs can require FBI background checks**
 - E.g. direct contact w/ children, older adult care, law enforcement, banks, airports, insurance, casinos etc.
 - Can also be used for foster care/adoption
- **Notoriously inaccurate**
 - NELP's report:
<https://www.nelp.org/publication/faulty-fbi-background-checks-for-employment/>



Challenging FBI Records

- **Common problems**
 - Missing dispositions
 - Expunged cases still showing up
- **Technically, there are 3 ways to correct errors**
 - 1) Ask state central repository to correct record with FBI (**best way!**)
 - 2) Submit challenge directly with FBI online at www.edo.cjis.gov
 - 3) Submit a written request to FBI's CJIS Division



Sealing FBI Records

- **FBI can expunge/delete information, but cannot seal records in its own database**
 - Problem for people with sealed records who need FBI background checks
- **Solutions?**
 - State controlled data (Compact Council, NFF, Purpose Codes)



Third-Party Repositories

- **E.g. mugshots.com, whosarrested.com, gotchamugshot.com, etc.**
 - Report expunged/sealed cases
 - Pay to remove
 - Probably not covered by FCRA
- **Regulating these sites**
 - Legislation → As of 2017, 18 states had laws
 - Problems with enforcement
 - Litigation → e.g. Taha
- **Problem for your clients?**
 - What are you seeing/doing?



Post-Expungement Client Education

- **Client must know:**
 - What, if anything remains on the record.
 - How s/he can answer application questions.
- **Discuss any limited access, tailored to the person's circumstances.**
- **Discuss any likely “ants under the refrigerator” problems (e.g. FBI).**





When a criminal record is “sealed,” that means that most people can’t see it.

A sealed record cannot be seen or considered by:

- The general public
- Landlords
- Schools
- Licensing boards
- Most employers -- Employers who do not use FBI background checks won't see a sealed criminal record. That means the vast majority of employers won't see a sealed record.

When a criminal record is “sealed,” you can deny it ever happened.

You are allowed to deny your sealed cases if you are asked by someone listed above. *See below for important exceptions to this rule.*

You still have access to your own full criminal record, so you can see what cases were sealed.

- The easiest way to get a record of your *sealed* cases is to visit the clerk of courts in a Pennsylvania courthouse and ask for your complete record, including sealed cases.
- You can also order your entire record – called an “Access and Review” – from the Pennsylvania State Police, but currently that can take months.
- To see the criminal history information that is available to the general public (your *unsealed* record), visit The Unified Judicial System of Pennsylvania at <https://ujportal.pacourts.us> and search by your name.

In these limited situations, your sealed record can be seen and used:

- Law enforcement purposes (police, prosecutors and criminal courts)
- Gun ownership and use applications (including permits to carry and Act 235)
- Immigration
- International travel
- Other court cases, sometimes (dependency, custody, or protection from abuse cases)
- Admission to the bar to be a lawyer
- Limited situations where federal law requires a background check for employment
- **FBI records will show sealed cases**, but they may be considered only where required by federal law (**see reverse side for types of jobs affected and more information**)

If you are asked about your sealed record by someone listed here, you should *not* deny your record. You should explain you have a record that has been sealed.

For new developments or more information about sealing, see www.MyCleanSlatePA.com.

Some jobs require FBI background checks, which currently include sealed records. Examples include:

- Schools
- Police departments
- Jobs requiring regular contact with children
- Caring for older adults, if you moved to PA in the last 2 years
- Banks
- Airports and seaports, if working as a screener or with access to secured areas
- Casinos
- Insurance and securities industries
- HAZMAT-endorsed commercial driver's licenses
- Any job requiring a fingerprint-based FBI background check.
- Foster care and adoption require FBI background checks.

You will know that you are getting an FBI check because you will have to provide fingerprints. You will usually get the check through the State's vendor, IDEMIA. For more information, see <https://bit.ly/2ttuOkz>.

If you are asked by someone listed above, you should not deny your sealed record. **However, most of the time your sealed record should *not* cause you to lose your job** because most employers are not allowed to make decisions based on sealed records.

- You should prepare to prove to the employer that your case is sealed by showing your sealing order or by getting an "Access and Review" from the State Police.
- Banks, airports, seaports and jobs requiring HAZMAT-endorsed commercial driver's licenses *can* consider a sealed record when deciding whether to hire or fire.
- If you have a problem with an employer and an FBI check, seek legal assistance.

If your sealed record continues to cause problems for you, or if you know your job requires FBI background checks, you may want to seek expungement.

Your sealed record may be eligible for expungement if:

- Charges were dismissed or withdrawn by the judge or prosecutor
- Charges were dismissed after completing a diversion program
- You were found not guilty by a judge or jury
- You were convicted of a summary offense and have not been arrested for 5 years
- You are 70 years of age or older and have not been arrested for 10 years

For new developments or more information about sealing, see www.MyCleanSlatePA.com.

FBI Records: Main things to remember

- Sealed cases are currently reported on FBI records.
- Most employers are not allowed to get your FBI record.
- You will know if you are getting an FBI check because you will have to provide fingerprints.
- If you have a problem with an FBI check, or if a sealed record is used against you by an employer, seek legal help.
- If your job requires a FBI background check, look into expungement.

CRIMINAL JUSTICE

AMERICAN BAR ASSOCIATION

SECTION OF CRIMINAL JUSTICE

WINTER 2016

VOLUME 30, NUMBER 4



Technology Symposium

ALSO IN THIS ISSUE

- Crime Fighting Machines
- Challenges in International Cybercrime Investigations
- Data Technology and the Fourth Amendment
- Removing Expunged Cases from Commercial Background Checks



AMERICAN BAR ASSOCIATION

Criminal Justice Section

Criminal Justice Section Spring Meeting

Co-sponsored by The New Mexico Bar Association

April 28- May 1, 2016 | Albuquerque, New Mexico

Neuroscience: Paving the Way for Criminal Justice Reform!

Keynote Luncheon Speaker:



Justice Charles W. Daniels
New Mexico Supreme Court

Schedule At-A-Glance

Thursday, April 28

- CJS Committee Meetings
- Town Hall: Reversing the School to Prison Pipeline

Friday, April 29

- CLE: Neuroscience: Paving the Way for Criminal Justice Reform!

Saturday, April 30

- CJS Council & Committee Meetings

Sunday, May 1

- CJS Council Meeting

ABA
Criminal Justice Section

1050 Connecticut
Avenue, NW, Suite 400
Washington, DC 20036

Main Tel:
(202) 662-1500

Fax:
(202) 662-1501

Email:
crimjustice@
americanbar.org

Web:
americanbar.org/
crimjust

Topics Include:

- The Neuroscience of Hate
- Neuroscience and Environmental Factors
- Neuroscience and Solitary Confinement

To register visit: <http://ambar.org/cjs2016spring>



Effectively Addressing Collateral Consequences of Criminal Convictions on Individuals and Communities

BY HON. BERNICE B. DONALD

Once labeled a felon, the badge of inferiority remains with you for the rest of your life, relegating you to a permanent second-class status. . . . Even if the defendant manages to avoid prison time by accepting a “generous” plea deal, he may discover that the punishment that awaits him outside the courthouse doors is far more severe and debilitating than what he might have encountered in prison.

—Michelle Alexander, *The New Jim Crow* (2010)

Collateral consequences are the deprivations of various rights and freedoms as applied to individuals who were either found guilty or decided to plead guilty to a crime. Sometimes they are applied automatically under the law, while other times they are applied as a result of a court’s or a regulatory agency’s discretion. Various restrictions apply to felonies, misdemeanors, and even lesser offenses. Collateral consequences often originate from various sources, and this uncoordinated development has resulted in thousands of negative consequences or barriers that affect numerous facets of life.

With a grant from the Department of Justice’s National Institute of Justice, the American Bar Association Criminal Justice Section has compiled a national inventory of federal and state collateral consequences of criminal convictions. Currently, there are more than 47,000 such collateral consequences in the database. With concerns over mass incarceration mounting, it is important to consider how collateral consequences impact an individual’s ability to become a productive member of the

BERNICE B. DONALD is a judge on the United States Court of Appeals for the Sixth Circuit and the 2015–2016 Chair of the Criminal Justice Section.

community. It compels policymakers, legislatures, courts, and society to reexamine the rationality of these ubiquitous consequences.

The application of collateral consequences to criminal convictions is not a new phenomenon. Their origins date back to ancient Greece, the Roman Republic, and Medieval England. (Danielle R. Jones, *When the Fallout of a Criminal Conviction Goes Too Far: Challenging Collateral Consequences*, 11 STAN. J. C.R. & C.L. 237, 244–45 (2015).) Today, however, with over 65 million individuals in the United States having some sort of criminal history, collateral consequences are pervasive and stringent. (*Id.* at 241.) They often affect not only those who

Extensive collateral consequences disproportionately affect the poor and minorities.

were previously imprisoned, but also families, dependents, communities, and society itself. Understanding who is affected by these consequences, how the consequences interact with each other, the link to recidivism, and the cumulative effect on society are crucial to understanding why reform is necessary. As this phenomenon is now at epic proportion, the United States Congress and many states have begun to focus on this issue and consider whether there is a rational

relationship between these consequences and traditional penal objectives.

Stories such as the following graphically and powerfully demonstrate the magnitude of the problem. Consider Maurice Alexander, who, at 61 years old, was convicted of a misdemeanor. His conviction prevented him from obtaining affordable housing, which eventually left him homeless for a number of months. (Monica Haymond, *Should a Criminal Record Come with Collateral Consequences?*, NPR (Dec. 9, 2014), <http://tinyurl.com/pp2jwnr>.) Then there is Markeisha Brown, who had to drop out of school to take care of her children when her boyfriend, who took care of

(continued on page 33)

FEATURES



10

4 **Federal Indigent Defense: How to Stop Worrying and Love the Digital Age**

By Sean Broderick and Russell M. Aoki

“Techno-strategizing” is not just for complex cases any longer. Even so-called “simple” prosecutions require that the defense understand the digital evidence hidden in government e-discovery.

10 **Machines as Crime Fighters—Are You Ready?**

By Michael L. Rich

Picture a future in which machines will be able to isolate and predict likely criminal candidates using ASA—automated suspicion algorithms. If it all sounds a little too much like the Tom Cruise sci-fi film, *Minority Report*, take notice: it’s just around the corner. Will the law be prepared?

15 **Cases without Borders**

THE CHALLENGE OF INTERNATIONAL CYBERCRIME INVESTIGATIONS

By Jason P. Gonzalez, Matthew A.S. Esworthy, and Neal J. Gauger

In the year 2000, a single computer virus did \$8 billion in damage worldwide. It wasn’t long before law enforcement agencies knew exactly who had written the code and spread the bug. But blocked by a tangle of international roadblocks, the culprits were never arrested or prosecuted.

19 **Location! Location! Location!**

DATA TECHNOLOGIES AND THE FOURTH AMENDMENT

By Rodolfo Ramirez, Kelly King, and Lori Ding

Post a picture on social media of you and your dog in the front yard and you may unwittingly be telling viewers precisely where you are through technology called geotagging. Use a Wi-Fi connection, and your movements can be tracked through your smartphone. Such unintentional exposure of information is usually harmless, but what are the Fourth (and Fifth) Amendment consequences when such data becomes evidence?



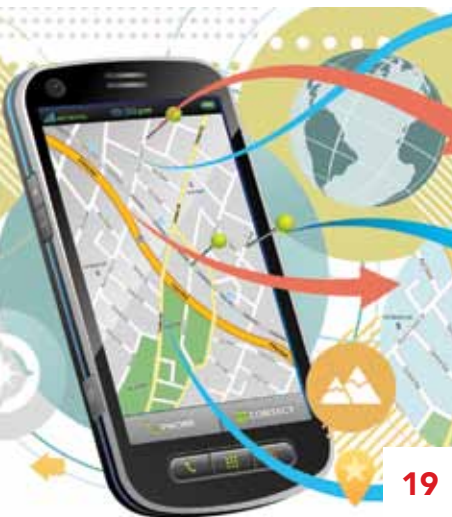
15

26 **Ants Under the Refrigerator?**

REMOVING EXPUNGED CASES FROM COMMERCIAL BACKGROUND CHECKS

By Sharon M. Dietrich

Like the proverbial bad penny, in today’s digital universe, a conviction or arrest can continue to resurface long after the court has sealed or erased the records, thanks to privately held databases that are in the business of selling information. Like the pesky ant in your kitchen, just when you think you’ve killed the last one, another emerges from under the fridge.



19

DEPARTMENTS

- 1 Chair's Counsel**
EFFECTIVELY ADDRESSING COLLATERAL CONSEQUENCES OF
CRIMINAL CONVICTIONS ON INDIVIDUALS AND COMMUNITIES
- 30 Federal Sentencing**
RESIDENTIAL DRUG ABUSE TREATMENT PROGRAM (RDAP)
- 35 Trial Tactics**
RULE 413 AND CHARGED PROPENSITY EVIDENCE
- 38 Indigent Defense**
THE SLOW JUSTICE MOVEMENT
- 40 Federal Rules Alert**
FEDERAL RULES PUBLISHED FOR PUBLIC COMMENT
- 41 Cert Alert**
SUPREME COURT CASES OF INTEREST
- 44 Juvenile Justice**
ABA MODEL ACT ADDRESSES MYTH OF "CLEAN SLATE"
- 46 Scientific Evidence**
DEFENSE EXPERTS AND THE MYTH OF CROSS-EXAMINATION
- 48 Ethics**
MISUSE OF LETTERHEAD BY PROSECUTORS AND ATTORNEYS
GENERAL
- 52 Criminal Justice Matters**
PROTECTING CONFIDENTIALITY OF A CRIMINAL DEFENDANT'S
LITIGATION FILE
- 55 Section News**
EIGHTH ANNUAL FALL INSTITUTE AND CJS FALL MEETINGS

Criminal Justice (ISSN 0887-7785) is published quarterly as a service to its members by the American Bar Association Section of Criminal Justice. Copyright © 2016 American Bar Association. Editorial, advertising, circulation, subscription offices: 321 N. Clark Street, Chicago, IL 60654-7598. Section offices: ABA, 1050 Connecticut Ave., NW, 4th Floor, Washington, DC 20036.

Any member of the ABA may join the Section of Criminal Justice by sending annual dues of \$40 to the Section (\$20 of which funds *Criminal Justice* magazine and is nondeductible); ABA membership is a prerequisite to Section membership. Individuals and institutions not eligible to join the ABA may subscribe to *Criminal Justice* for \$48 per year, \$57 for subscriptions addressed outside the United States and its possessions. Single copies are \$10 plus postage and handling. For information on subscriptions and back issues, contact the ABA Service Center at (800) 285-2221.

To write for us, contact the editor or go to http://www.americanbar.org/publications/criminal_justice_magazine_home.html. Opinions expressed in the magazine do not necessarily reflect the policies of the editorial board, the Section, or the American Bar Association.

Periodicals postage paid at Chicago, Illinois, and at additional mailing offices. **POSTMASTER:** Send address changes to *Criminal Justice* Member Records, American Bar Association, ABA Service Center, 321 North Clark St., Chicago, IL 60654-7598.

Members: Go online at www.abanet.org and click on "Membership" and "Update Your Profile."

Advertising: Sales & Business Manager, Anne Bitting, 312/988-6115. Address advertising material to ABA Publishing Advertising Sales, 321 N. Clark Street, Chicago, IL 60654-7598.

Reprint Permission: Contact ABA Publishing Contract & Copyrights at copyright@americanbar.org.

Published in *Criminal Justice*, Volume 30, Number 4, Winter 2016. © 2016 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

EDITORIAL BOARD

Chair

Justin P. Murphy

Vice Chair

Richard A. Ginkowski

Members

J. Vincent Aprile II
Alexander Bunin
Hon. Arthur L. Burnett, Sr.
Michael D. Dean
Donna Lee Elm
Janet Fink
Andrew Kim
Matthew F. Redle
Susan D. Rozelle
Mara V. Senn

Columnists

J. Vincent Aprile II
Geoff Burkhardt
Rebiah Burks
Todd A. Bussert
Bernice B. Donald
Alan Ellis
Carol Garfiel Freeman
Paul C. Gianellei
Peter A. Joy
Kevin C. McMunigal
Stephen A. Saltzburg
David A. Schlueter
Robert Schwartz
Kyo Suh

ABA PUBLISHING

Director, ABA Publishing

Bryan Kay

Editor

Erin Remotigue
erin.remotigue@americanbar.org

Director, Design/Production

Nick Panos

Art Director

Mary Anne Kulchawik
maryanne.kulchawik@americanbar.org

Production Coordinator

Karrie Dowling

Cover Image

istock





Federal Indigent Defense

How to Stop Worrying and Love the Digital Age

BY SEAN BRODERICK AND RUSSELL M. AOKI

Today, technology impacts every attorney defending an indigent client against a federal criminal prosecution. Public defenders and private court-appointed counsel increasingly need practical strategies to manage and review valuable evidence hidden like needles within the haystacks of discovery. No longer just a consideration for complex multiple-defendant cases, technology strategies must be considered and effectively employed to address government discovery productions even in “simple” single-defendant prosecutions.

Technology’s impact is most felt in the realm of electronic discovery, referred to as “e-discovery” or “ESI” (electronically stored information). Lawyers in large firms with experienced e-discovery staff know how to develop and implement discovery management plans. They understand the importance of usable formats, software tools, and processes specifically designed for the digital age. But the challenges of ESI may be especially daunting for private court-appointed counsel, who are predominantly solo or small-firm lawyers with little exposure to complex e-discovery. Because nearly 90 percent of all defendants in federal criminal cases have court-appointed counsel (either an attorney from the local federal public or community defender office, or a private attorney who accepts Criminal Justice Act (CJA) appointments), it’s vital for the integrity of the judicial system that counsel for indigent defendants adapt to the digital era. Broadly stated, the key to adequately addressing e-discovery challenges is understanding the technology and how to strategically use software and resources to efficiently review and manage e-discovery.

The days of paper investigative reports are long gone. Discovery productions now include e-discovery extracted from client computers and mobile devices. Agents look at social media sites like Facebook, Instagram, and Twitter to capture possible incriminating materials. Videos are common and include months of pole-camera recordings, business security videos, and even concealed camera footage. Add in government-created evidence using technology such as cell phone wiretaps, body wires, and GPS tracking devices, and it becomes clear technology is more than the form of discovery: it’s the tool to gather evidence, the means to manage evidence, and frequently the evidence itself.

Although tempting, hitting the print button will not solve discovery management problems. Hard copies will not address the mixed-media discovery—the volume is

too substantial to print, and critical information will not appear on the paper. Counsel for indigent defendants will lose out on the speed, efficiency, and quality of information that e-discovery can provide when done thoughtfully and produced in reasonably usable formats.

There are several critical issues indigent defense counsel must address to adequately manage and review e-discovery:

- Large volumes of information even in “small cases”;
- A variety of sources (from a multitude of digital devices and locations);
- Proprietary formats;
- Hidden information (metadata and embedded data);
- Differing formats for production; and
- Software and hardware limitations.

Regardless of the size of the firm and the availability of support staff, the challenges of technology and the management of e-discovery can be a time-consuming and distressing distraction, and are compounded by the ticking speedy-trial clock, impatient judges wanting to move the case along, and anxious in-custody clients seeking to review the materials that will be used to prosecute them. To meet these litigation demands and effectively represent their clients, defense counsel must leverage technology support tools for end-to-end discovery management. The solution to e-discovery’s challenges starts with making a plan then implementing it.

Make a Plan

Because public defenders and private court-appointed counsel are rarely appointed pre-indictment, they typically are not aware of specifics of the discovery such as volume and type. It can be particularly challenging to learn how to manage various forms of e-discovery while learning the case. The first step to making a plan is to meet and confer with the government about the nature and volume of e-discovery and the mechanics of producing it, specifically addressing the form of discovery production.

Historically, one of the challenges for all federal criminal practitioners has been the lack of established rules and procedures regarding how to manage e-discovery in criminal cases. Unlike the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure are largely silent on how to conduct e-discovery and do not address the form of production. In the absence of rules, an excellent road map for managing post-indictment e-discovery is the *Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases* (<http://www.fd.org/docs/litigation-support/final-esi-protocol.pdf>), also known as the ESI Protocol. This document was produced by the Joint Electronic Technology Working Group (JETWG) with representatives of the Administrative Office of the US Courts’ (AOUSC’s) Office of Defender Services (now called the Defender Services Office, or DSO), the Department of Justice (DOJ), federal public and community defender organizations, private attorneys who accept CJA appointments, and liaisons from the United States judiciary and other AOUSC offices.

SEAN BRODERICK is the national litigation support administrator for the Defender Services Office in Oakland, California. He provides guidance and recommendations in federal criminal cases to courts, federal defender offices, and court-appointed attorneys on e-discovery in complex cases. He can be reached at sean_broderick@fd.org.

RUSSELL M. AOKI is a Criminal Justice Act panel attorney in Seattle, Washington, and former member of the state’s Office of Public Defense Advisory Committee. He is also a coordinating discovery attorney for Defender Services, providing litigation and technology support to court-appointed counsel across the country, and can be reached at russ@aokilaw.com.

Published in 2012 with the support and encouragement of then Deputy Attorney General James Cole on behalf of DOJ, the ESI Protocol outlines 10 principles for managing post-indictment e-discovery. The ESI Protocol is familiar to federal prosecutors, as DOJ trains them in the use of the ESI Protocol in cases involving complex e-discovery, as well as to many federal public defenders, community defenders, and CJA panel attorneys. The document sets forth a collaborative approach to ESI discovery involving mutual and interdependent responsibilities. The goal is to benefit all parties by making ESI discovery more efficient, secure, and less costly.

Considering the guidance of the ESI Protocol and each lawyer's ethical responsibilities, every criminal defense lawyer's analysis of how to strategize e-discovery management should begin with four fundamental principles.

Learn technology. Many criminal practitioners should increase their understanding of e-discovery issues and litigation technology. Without sufficient knowledge in the constantly changing world of technology, counsel may miss potentially beneficial evidence by making critical mistakes early in the case, such as inadvertently choosing production formats they cannot use or that will not help find the evidence they need. The wrong format could cause valuable metadata in electronic records to be missed because counsel was entrenched in printing their discovery.

Ethics opinions and the interpretations of the Rules of Professional Conduct are evolving, requiring a lawyer to have an adequate understanding of e-discovery and technology needs. For example, the State Bar of California issued a formal ethics opinion on this subject in the summer of 2015. (*See* State Bar of Cal. Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. 2015-193 (2015).) Though focused on civil litigation, some of the points explicitly mentioned are directly relevant to counsel for indigent clients in federal criminal cases: the ability to initially assess e-discovery needs and issues; identifying custodians of potentially relevant ESI; engaging in competent and meaningful meet-and-confer with opposing counsel concerning an e-discovery plan; and performing data searches. This development follows the 2012 American Bar Association amendment to its Model Rule 1.1, stating that lawyers must "keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology.*" (MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 8 (emphasis added).) Lawyers unfamiliar with e-discovery are encouraged to associate or consult with others who have the expertise. Ultimately, however, lawyers remain responsible for e-discovery decisions whether made by staff or third-party vendors. By staying current with technology trends, lawyers can confidently oversee nonlawyer technical assistance.

With state bars emphasizing the ethical issues relating to technology competence, CLE sessions on e-discovery management have become prevalent. Local and national seminars offer educational opportunities from hour-long sessions to multiple-day in-person trainings. Most lawyers know of litigation support specialists, paralegals with

experience working e-discovery, or technology consultants who can also give advice.

Develop an early discovery plan based on volume and format. The temptation to dive into a haystack of discovery can be powerful but often proves to be an inefficient strategy for review. Sketching out even a basic plan to address discovery helps to stay focused on the greater and immediate objective of discovery management. A discovery plan typically starts with assessing the volume of materials and the format in which ESI is gathered for production before addressing case-specific issues.

E-discovery volume poses a serious challenge due to the variety of devices on which ESI can be created and stored, the ease of various forms of telecommunication (such as texting and social media), and the declining cost of storage. ESI can come from many sources, such as mobile phones, smartphones, tablets, laptops, desktops, computer network servers, external ESI storage devices (e.g., flash drives or external hard drives), cloud storage, GPS tracking devices, and social media. The growth of ESI in criminal cases is expected to continue, significantly complicating organization and review of evidence. The presence of e-discovery is not limited to computer and white-collar fraud cases. What once were "straightforward" gun or drug cases may now have smartphones and computers as evidence, with gigabytes or even terabytes of data on the device. Without technological assistance, attorneys cannot review so much data. The greater the volume, the greater the need to identify the necessary technology tools for management and review.

The format in which ESI is gathered affects how the data can be used. E-mail messages collected as PDF or text-only files can be searched for particular words or combinations of words. It can be cumbersome to review, sort, and filter the information. But if in the process of collecting the e-mail messages, the metadata is also gathered and produced, then thousands or millions of messages can not only be searched for particular words, but they can also be sorted and filtered in a number of combinations, including by date, custodian, and author or addressee, and software can be utilized to visually demonstrate who communicated with whom and how frequently.

To benefit from the information available in e-discovery, attorneys must know what format the original data was in, what formatting options are available, and how those options affect their potential review of the data. Attorneys who do not understand the various formats should consult with a litigation support expert before receiving or processing their e-discovery.

Meet and confer with the government. The ESI Protocol promotes early conferences with the government to ensure discovery is produced in a usable format. An early meet-and-confer is a valuable opportunity, because voluminous e-discovery cases present difficult challenges for both prosecutors and defense counsel. Missteps at the outset are costly to unwind or correct, and waste time and money. To get the parties to address e-discovery issues early, the ESI Protocol recommends three steps: (1) at the outset, the parties should meet and confer about the nature, volume, and

mechanics of producing e-discovery; (2) at the meet-and-confer, the parties should address what is being produced, a table of contents of the discovery, the forms of production, discovery volume, software and hardware limitations, inspection of seized hardware, and a reasonable schedule for producing and reviewing e-discovery; and (3) the producing party should transmit its e-discovery in sufficient time to permit reasonable management and review, and the receiving party should be proactive about testing the accessibility of the ESI when it is received.

Become familiar with litigation support tools. There are numerous software tools available for managing all of the stages of electronic discovery: preserving, collecting, and harvesting data; processing and/or converting ESI; searching and retrieving information; reviewing ESI; and presenting evidence. It can be daunting to determine what tools to use, especially since many can be used for similar tasks. Often, companies name the tasks differently in their computer program, or the program completes the task in a somewhat different way. At this point no single software tool does everything needed for e-discovery. Some tools specialize in processing raw ESI into formats that another tool can then use, while other tools specialize in a discrete function such as document review, strategic analysis, case organization, production of discovery, or trial presentation in the courtroom.

For the solo and small-firm lawyers, litigation software is necessary to work with ESI in its many formats. Most document review programs allow parties to view hundreds of different file types. DOJ and most civil law firms have managed their own discovery materials with software programs and technical personnel for years. However, many private court-appointed attorneys do not have litigation support software that can view and organize TIFF or native-file productions. (TIFF is a common file format for storing images; “native” refers to a file produced in the format in which it was originally created.) Similarly, most do not have tools to take advantage of a “load file” (a cross-reference file used to import images or data into litigation support databases), extracted metadata, or files in native or near-native ESI format. DOJ may produce discovery in a reasonably usable format, but court-appointed counsel may not utilize the most robust litigation software available to take advantage of the form of production. An important strategy is for computer-challenged defense counsel to seek reasonably useable e-discovery. US attorney’s offices can provide e-discovery on disks that contain software for viewing, searching, and tagging documents. For more sophisticated defense counsel, DOJ typically creates load files or otherwise configures its e-discovery productions in industry standard formats. There are instances where typical practices do not work well, such as cases that involve predominantly surveillance materials. Those instances are excellent topics for a meet-and-confer.

Implement Your Plan

Initial review of data. Upon receipt, the discovery should be cataloged by the date received and the contents produced. A second working copy should be made with the original put

away for safekeeping. A review of the composition of the data will confirm the volume and format of the discovery to ensure the production is complete and no files became corrupt during the collection or copying process.

The discovery should also be reviewed to determine if documents have been provided in a searchable format, or if they will need to be made searchable prior to loading into a discovery management tool. PDFs in the production should be reviewed to determine if they comprise many documents combined into one PDF, and if so, whether they should be separated into single-document PDFs. The types of documents must also be determined to identify the best method for organizing the data. Defense counsel may want investigative reports to be gathered and prioritized for immediate production and review to address pretrial motions and possible detention issues. Forensic images of computers should be handled separately as they take longer to produce and could take weeks from the time of receipt to analyze. Analysis of forensic computer data requires specialized tools to view while in their forensic state or to unlock for application of keyword searches. Which keywords to use may depend on information revealed in documents such as the investigative reports.

Selection of discovery management tools. Discovery management tools need not be expensive or complicated. The most effective tools are the ones counsel will use. Common business software programs provide features that will allow discovery to be cataloged, searched, and sorted, and are already available in every law firm, big or small. Programs such as Word and Excel all include the ability to create charts and tables, add and search comments, and hyperlink discovery items. Excel includes the ability to filter large quantities of materials to smaller collections. Even loading all the documents into a folder and using Windows Explorer or Apple’s Finder for simple keyword searches is an easy and effective method to locate materials in a small collection of searchable documents.

More sophisticated desktop programs provide cost-effective review. Programs like Adobe Acrobat Pro that are designed to create, edit, convert, encrypt, and publish PDF files are excellent tools for managing electronically scanned paper, and provide basic organization, search, and annotation features. Besides providing an easy-to-use PDF-based desktop tool, the program can add Bates numbers or separate documents by page or by bookmarks.

CaseMap is another desktop software application specifically designed for case management and analysis of legal and factual issues. It connects case facts, legal issues, key players, and key documents. Defense counsel can store important case information of many file types and generate relational spreadsheets for ready access and analysis. Through searching and flexible filtering, CaseMap enables end users to see how any person, fact, document, or issue relates to other elements in the case. Besides being a database and useful for discovery analysis, it can also create trial notebooks and prepare reports focused on any combination of issues, witnesses, or cross-examination material.

Stand-alone sophisticated desktop search engines such

as dtSearch can apply sophisticated multiword searches with results ranked based on relevance to the inquiry. Counsel merely assembles the discovery into a folder and points the search engine to index the materials for search capability. The program provides great functionality in searching both electronic documents and paper documents subsequently scanned and converted to a text-searchable format, especially since it can search and retrieve information in many file types.

The next step up in both sophistication and cost are web-hosted document review platforms. They have powerful databases with sophisticated search capabilities and enormous data capacity. Most are linked to multiple servers and can provide complex keyword search strings against millions of documents. The cost can be expensive, but considering the attorney time that would otherwise be spent conducting linear page-by-page review, a web-hosted document review platform can reduce the cost of searching and reviewing huge volumes of discovery. An outside service frees counsel from ensuring the program works properly, is kept secure, and is properly maintained with program updates.

Typically, web-hosted document review platforms entail two major costs. The first is processing, which is the loading of the discovery. Processing includes removing computer and system files that contain no probative evidence and indexing the material to be searchable. The second cost is hosting. Hosting fees are typically charged per month and based on how many gigabytes of data are being hosted. Often associated with monthly hosting are user fees where each end user is assessed a monthly charge.

Web-hosted document review platforms are well suited for multiple-defendant prosecutions, involving huge amounts of discovery and defense teams that include support staff, investigators, and experts. These platforms use a database and tools to capture, organize, analyze, and review e-discovery. They enable multiple individuals to access discovery and other case materials through a secure online portal, much like accessing bank account information online. The e-discovery can be searched, retrieved, viewed, and/or printed. Each individual can work collaboratively from his or her respective offices or any location that allows Internet access and privately code or comment on documents for only fellow team members. For multiple-defendant cases, the cost per defense team makes the expense worthwhile.

Selection of outside vendors. Many cases require technical assistance from vendors. The services could vary from converting proprietary audio and video files into formats for PC and Apple Mac computers, making huge volumes of discovery searchable, or enlisting a web-based database company to process and host discovery.

The most effective way to obtain court funding is to comparison shop for services and prices. One service provider may claim potential costs of \$10,000 for a particular service, yet another vendor may do the same work for under \$1,000. The cost difference often depends on the skill and experience of the vendor. By obtaining three

or four proposals, the court develops greater confidence that the service is cost-effective and a competitive price was obtained. Counsel gains a better sense of the options available, and is more likely to choose tools and services that fit specific needs for the case.

To assist in being able to compare proposals and to get better pricing in complex cases, consider using requests for proposal (RFPs). By developing an RFP, you will better understand the scope of work and increase the likelihood you will get what you want from the system and vendor selected. By providing a customized RFP to prospective vendors, you will be able to compare bids among vendors so that you are not comparing apples to oranges, as many employ different pricing models, charging differently for various services (or not telling you about hidden costs with their proposed solution). In the best-case scenario, the RFP identifies the features and functions counsel believes will help them efficiently and effectively review, search, organize, and analyze the voluminous discovery in a case, while at the same time reducing overall costs. For federal court-appointed lawyers, the National Litigation Support Team (NLST), which is part of the DSO, is available to help attorneys for indigent defendants struggling with extensive e-discovery and can assist in this process.

When planning, technology and outside assistance can come together. For illustrations of how thoughtful planning by counsel, use of appropriate technology, and outside assistance can help overcome e-discovery challenges and provide a solution, consider the following two example cases where counsel for indigent clients (one state, one federal) were able to assist their clients and turn e-discovery from a challenge into an asset.

Wiretap cases can be frustrating and time-consuming for defense counsel. Often they will receive unorganized collections of tens of thousands of captured telephone conversations and a similar amount of linesheets, which are documents memorializing each recorded call. In one recent multidefendant wiretap, the discovery included more than 20,000 recorded calls. Though the discovery was initially produced by the government in proprietary formats, after a meet-and-confer the government was willing to provide the discovery in industry standard formats (computer-generated CSV and PDF files). Defense counsel worked with an outside technology company to create sortable spreadsheets that used an automated process to extract linesheet information (the target number, date, time, duration, and number dialed), break up or “unitize” the multiple-document PDFs that were produced into PDFs each containing only a single recording session, then associate the information to the audio. Though the volume of wiretaps was over 20,000 calls, the work was completed in a few weeks. Using the sort and filter functions of the spreadsheet, counsel could then quickly locate pertinent calls by the target phone number, specific days, particular number dialed, or any combination of these criteria, and display the relevant linesheets hyperlinked to the associated audio. Such a review, performed manually

by counsel and/or paralegals, would have taken hundreds of hours and cost many times over the expense of the vendor's automated program.

In another recent case, defense counsel was presented with a hard drive of discovery that included not only the investigative reports, but also forensically preserved file folders. These folders had to be unlocked to process the data. Counsel forwarded the hard drive to a small technology company and requested a file-type report describing the various files found on the device: e-mail, PDFs, picture files, system files, etc. Besides the file-type report, counsel could obtain a file-path report that showed not only the file types, but also the folder path revealing where the materials were on the hard drive. From this report it was determined that most of the 386 gigabytes of data—primarily program and system files, or iTunes music files—were irrelevant. The file-path report revealed there were only three gigabytes of documents. The technology company then created a sortable, hyperlinked spreadsheet with three worksheets. The first contained documents, the second the audiovisual files, and the third the remaining discovery data. The cost was substantially less than other solutions that a large technology company may have charged for processing the discovery, and much, much less (and more effective) than if counsel had resorted to hitting “print” and attempting to review the materials with eyes on paper.

The solutions described above were case-dependent, and in many instances the solutions required for complex e-discovery cases will take more time and/or resources than described above. But they illustrate the possibilities that exist when counsel representing indigent clients obtain e-discovery in reasonably usable format, leverage the appropriate technology, and strategically use outside resources to efficiently manage e-discovery and better defend their clients.

Defendant's Access to E-Discovery When Incarcerated

Providing in-custody defendants meaningful access to e-discovery is a significant issue for criminal defense practitioners. As counsel for indigent defendants know, it is important to facilitate access for their defendants as they often can help locate critical evidence much more quickly than defense team members. Importantly, defendant access to e-discovery allows them to assist in their own defense, facilitates attorney-defendant communication, and improves overall advocacy on the defendant's behalf.

In 2013, DOJ reported that in recent years 76 percent of federal court defendants were in pretrial custody. With much of the discovery and potential evidence starting in digital form, developing ways for defendants to review e-discovery in digital form is a priority for all involved in the criminal justice system.

There is no easy answer on how to make the many formats of ESI accessible in a facility. Few in-custody defendants are housed in Bureau of Prisons (BOP) pretrial detention facilities. The BOP operates only seven dedicated detention centers. This means most defendants are

in one of the approximately 1,800 state, county, or private facilities nationwide—each with varying discovery review policies. Some do not allow discovery in even paper form. Some facilities lack funding to provide discovery computers, lack staff to maintain equipment and monitor its use, or disallow computers due to their concerns regarding security for their particular facility. Yet others are considering tablet devices, but those devices cannot handle the many file types common with e-discovery.

Even if equipment were available to review more file types, many facilities do not allow executable files (files that load software applications) to be added to inmate-accessible computers. This causes problems when defendants attempt to view many of the common surveillance audio and video files provided in discovery that can only be viewed by using proprietary viewers. Another variation on this problem is a defendant's inability to view files that require an IPRO runtime viewer. DOJ commonly produces TIFF images (a frequent file format for large e-discovery cases) in this manner. However, the IPRO viewer's self-executing feature means it is not allowed in many detention facilities. The files must be converted into a format the facility will allow, which is a time-consuming task defense counsel rarely know how to perform.

In addition, some of the discovery provided consists of unsearchable PDF documents. This causes significant delay in reviewing the discovery, because even the best PDF viewers cannot search PDF documents if the materials are not first made searchable. Defendants are left linearly reviewing discovery page by page. When facilities do allow computers, tablets, or other devices, they often require the attorney to be present with the defendant while he or she reviews the e-discovery. With large amounts of e-discovery, this can become quite time-consuming and costly for the CJA panel system.

JETWG is studying the risks and benefits of allowing inmates access to computers for e-discovery review. It hopes to produce practical recommendations soon, but with the wide variance in facilities and their respective policies, solutions will be difficult to identify. One thing is clear: there is no one-size-fits-all solution to this dilemma. In the interim, counsel working on behalf of indigent defendants should look to work with their local court, prosecution, defenders, CJA panel attorneys or representatives, and detention facility to find a workable solution.

Conclusion

Managing e-discovery is a critical component of today's criminal defense work and appears at first blush to be a daunting subject for most court-appointed counsel. However, taking the time to learn the technology will add a new skill to representing indigent defendants. If counsel is not sure what to do, they should ask those with experience. It may start with their local federal public or community defender office, CJA panel rep, or support staff experienced with managing e-discovery. The ability to manage e-discovery is an expectation of clients, the courts, and even the state bar associations. ■



MACHINES AS CRIME FIGHTERS ARE YOU READY?

BY MICHAEL L. RICH

A computer screen in a police dispatch office shows a live feed from a video camera trained on a public street corner, where people walk, linger, and interact. A beep sounds, and a figure on the screen is highlighted in red. A police dispatcher clicks on the figure, and a computer system reports that there is a 62 percent chance the highlighted individual is currently engaged in hand-to-hand cocaine transactions. The dispatcher contacts nearby officers so that they can intervene and make an arrest.

The computer system making the prediction has been trained to identify likely cocaine dealers using machine learning methods. Machine learning, a field of computer science, is the study of systems that improve their performance on a task with experience. In this case, the task is predicting whether an individual is involved in the targeted criminal conduct of cocaine selling. The system “learns” by looking at historical data and identifying patterns that correlate to cocaine sales. It then looks for those patterns in new data in real time and alerts police when it can, to a preset level of confidence, predict that an individual is selling cocaine.

Machine Learning and Automated Suspicion Algorithms

In a prior work, I have named technologies such as these, which use machine learning methods to find patterns in historical data that correlate to criminal activity and then analyze new data in real time to identify likely criminals, “automated suspicion algorithms” or ASAs. (See Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. (forthcoming 2016), available at <http://tinyurl.com/ofzq499>.)

As I write this, ASAs that target street crime like hand-to-hand drug transactions are hypothetical, but only just. Over the last several years, a convergence of machine learning applications and the real-time identification of street criminals has been creeping ever closer to reality. To see why that convergence is likely inevitable, it is helpful first to recognize that law enforcement has always been quick to adopt available technologies to detect crime and catch criminals.

For more than a century, police have used fingerprints at

a crime scene to identify perpetrators. And as technology has improved and become more ubiquitous, police have begun to gather all kinds of information with it. Radar guns tell how fast cars are driving. Matches in DNA databases reveal with greater accuracy than fingerprints who has (and who has not) been at the scene of a crime. GPS transponders track suspects' movements. Cell site simulators allow police to pinpoint cellphone locations.

Another reason machine learning will inevitably be used to detect street crime is that the capabilities of machine learning methods are well suited to crime detection. One of the primary uses of machine learning is, in computer science terms, the "classification" of "objects" based on "features." Here, the "object" is an individual, the "features" are any pieces of information about the individual that might be relevant, and the "classification" is whether or not the individual is engaged in the targeted criminal conduct. Machine learning methods are exceptional in their capacity at sifting through large quantities of data to find complex correlations among features and accurately predict a classification. In other words, machine learning can be used to analyze vast amounts of information about past criminals and noncriminals and isolate rules that describe when facts about an individual make it likely that he or she is engaged in criminal conduct. One additional technical note is important: often in order for a system trained by machine learning to be most effective at making predictions, it must operate as a "black box," where no one, even its programmers, understands exactly how it works.

Machine Learning Meets Crime Fighting

The first steps of the *pas de deux* between machine learning and crime fighting took place in private industry. eBay was a pioneer in the field when it announced more than a decade ago that it was using machine learning methods to uncover fraud. Since then, credit card companies and businesses in other data-driven industries have begun using machine learning to detect bad actors.

Unsurprisingly, the first attempts by law enforcement agencies to detect crime through machine learning have involved crimes that leave a digital footprint. For instance, the Securities and Exchange Commission operates a computer system that analyzes trading data in real time to detect insider trading and other criminal practices. While the precise workings of this system are unclear (an issue to which we will turn in a bit), machine learning almost certainly plays a role. Similarly, the Defense Advanced Research Projects Agency has entered into a multi-million-dollar contract with Carnegie Mellon University to develop tools through machine learning methods that can identify online ads connected to illegal sex trafficking.

While the move from obviously data-generating crimes like Internet sex trafficking and insider trading to

"ordinary" crimes like drug dealing or burglary will face practical challenges, it will happen, in large part because the data is there. Cameras are ubiquitous in many cities, and their video feeds are shared freely with law enforcement. License plate readers scan cars at toll booths, parking lots, and public roads. GPS data from cell phones reveal our every movement. Our daily actions inevitably generate troves of data: medical billing records, numbers dialed, text messages, airplane trips, web searches, stock trades, and credit card charges are just a sampling. The collection of this data raises serious concerns about privacy and autonomy that have justifiably garnered much attention from the popular media and academics. Law enforcement access to the data multiplies those fears. While I share many of these concerns, I am confident (if perhaps defeatist) that mass data gathering will continue, and I believe that we must be prepared to address how law enforcement uses the data it gathers.

An example helps further illustrate the potential of machine learning to help law enforcement. Police in East Orange, New Jersey, have adopted a computer system that analyzes information, including footage from public cameras and data from gunshot sensors, in real time to detect patterns believed to be consistent with criminal activity. For instance, the system can recognize when an individual takes repeated short trips into a home and back to the street, conduct thought to be like that of a corner drug dealer. When it detects suspect criminal activity, the system alerts police who are then sent to investigate. According to officials in East Orange, the system is at least partially responsible for a drastic reduction in violent crime in the city over the last several years.

Though details about the inner workings of the system are sketchy, it appears to rely on humans to tell it what patterns of conduct to look for. Machine learning methods could supplant that human input and allow the system to detect criminal conduct more effectively and efficiently. Machine learning would make the system more effective by identifying previously unknown indications of criminality, thus allowing police to catch dealers that otherwise might not have been caught. It would make policing more efficient by recognizing patterns of conduct thought to correlate to drug dealing that in fact are not strongly predictive of criminality, thus reducing the frequency of confrontational interactions between police and innocent civilians. These potential benefits will certainly prove hard for at least some law enforcement agencies to resist.

Moreover, applying machine learning to the identification of likely criminals has the potential, frequently trumpeted in relation to other machine learning applications, to scrub that decision of improper bias. An ASA can use only the information provided to it and must follow its programming. Thus, the argument goes, if the ASA never receives information that we do not want it to consider, such as an individual's race or religion, or is programmed to ignore that information, its prediction will be unbiased in that it cannot be based on that fact. Given how police

MICHAEL L. RICH is the Jennings Professor of Law at Elon University School of Law in Greensboro, North Carolina.

have long been dogged by accusations of improper bias, the possibility of eradicating such bias through technology is particularly attractive.

Doctrinal Challenges to ASAs

ASAs possess exciting potential to improve policing, but they also pose novel challenges. Some are doctrinal. Elsewhere, I explore in depth the unique challenge that ASAs are likely to pose to existing Fourth Amendment law. (See Rich, *supra*.) Some of the lessons from that analysis are useful here.

First, we should expect police and prosecutors to argue that an ASA's alert is sufficient to create individualized suspicion and thereby justify a search or seizure. Courts ought to reject this claim. ASAs are novel technologies in that they assist in a part of the Fourth Amendment's individualized suspicion analysis that has, at least until now, been the exclusive province of humans: the decision whether all the known relevant facts about an individual are sufficiently suggestive of criminality to give rise to probable cause or reasonable suspicion. (See Ornelas v. United States, 517 U.S. 690, 696 (1996).) Existing policing technologies merely provide a human decision maker with more or better facts to include in that decision.

Take DNA testing, for instance. A match between an individual's DNA and the DNA found at a crime scene is essentially conclusive evidence that the individual was at the crime scene, but it does not automatically mean that probable cause exists to arrest the individual. Instead, a human decision maker must take the fact of that match into consideration along with all other known facts to decide whether an arrest can be made. For instance, imagine a victim is stabbed at a party and no eyewitness could identify the perpetrator. A match between a suspect's DNA and DNA found under the victim's fingernails differs greatly in its importance to the individualized suspicion analysis from a match with DNA from a hair found nearby. A human's evaluation of the relative importance of various kinds of information is typically crucial to determining whether probable cause or reasonable suspicion exists in such a case.

On the other hand, an ASA's capacity to analyze a vast array of data and predict the existence of criminal conduct seems to mesh well with this second step in the individualized suspicion process that requires consideration of "the totality of the circumstances—the whole picture." (Navarette v. California, 134 S. Ct. 1683, 1687 (2014) (quoting United States v. Cortez, 449 U.S. 411, 417 (1981)).) But the fit between an ASA's capabilities and the Fourth Amendment's requirements is off in one important way. As explained earlier, an ASA can consider only the information that it is provided. The breadth of this information may be dizzying, but it cannot be all encompassing. There will always be the potential that a piece of information will exist that an ASA is not programmed to evaluate, but which matters in deciding whether individualized suspicion exists. The totality-of-the-circumstances analysis demands that this datum be considered. Yet, given

current technological constraints on machine learning algorithms, only a human is capable of incorporating such previously unrecognized facts that are relevant to an individual's criminality. Thus, a human must make the final call on the existence of individualized suspicion, and an ASA's prediction of criminality can be only a part of the totality-of-the-circumstances analysis undertaken by that person.

Second, an ASA is best analogized to drug dogs in the totality-of-the-circumstances analysis. Both are "black boxes," in that we cannot understand precisely how they translate the inputs they receive into the outputs they provide. Because we cannot interrogate the logic of how they produce their predictions, the only way to determine how much weight to give their output is to measure how often they are right. While the analogy is reasonably sound, a problem arises in that the Supreme Court has not been particularly rigorous in its approach to assessing drug dog reliability.

In *Florida v. Harris*, 133 S. Ct. 1050, 1056 (2013), the Court rejected the requirement of a "strict evidentiary checklist" before a drug dog's alert could support a finding of probable cause, favoring instead the traditional totality-of-the-circumstances approach. Nonetheless, the Court cautioned that greater weight should be placed on a dog's performance during training and any certifications it has received than on the dog's field performance. This is unsatisfying for two reasons. First, there are no accepted standards for the training and certification of drug dogs. Thus, the mere fact of training or certification tells us little about how well a dog performs. Second, field performance matters. It is the dog's performance on a given occasion that is the issue in a motion to suppress on Fourth Amendment grounds, and field conditions can differ substantially from those in training in ways that can affect the reliability of the dog's alert.

These problems are exacerbated for ASAs. Programming a machine learning algorithm is far more complex than training a drug dog. Teams of programmers will need to make hundreds or thousands of decisions in "training" an ASA. Any one decision could have a far-reaching and difficult-to-discover impact on the accuracy of the ASA. Robust and meaningful standards for the creation and testing of ASAs are therefore particularly important to ensure that only reliable ASAs are used in the field. Ad hoc standards like those that govern drug dogs are insufficient.

Moreover, field performance data are especially crucial to an accurate assessment of the proper weight to be given to an ASA's prediction. Unlike the residues left by drugs that make a dog alert, the patterns that correlate to criminal activity can change substantially over time, particularly as criminals adapt to law enforcement activities. Thus, an ASA's performance in training on historical data will become a less and less reliable indicator of the ASA's accuracy in the field over time. An analysis of an ASA's recent field performance is therefore an essential component of the totality of the circumstances for determining the existence of individualized suspicion.

To recap, then, an ASA's prediction of an individual's criminality cannot supplant a final assessment by a human being of all known facts relating to that individual to determine the existence of probable cause or reasonable suspicion. Rather, an ASA's prediction should be thought of like a drug dog's alert, though ASAs should be evaluated more rigorously than the Supreme Court has assessed drug dogs. Standards for the training and certification of ASAs must be rigorous and uniform, and meaningful weight must be given to the field performance of an ASA in addition to its performance in testing. Only then should courts find the Fourth Amendment's requirements satisfied.

Practical Challenges to ASAs

The challenges in implementing ASAs go far beyond just constitutional doctrine. A thorough catalog of all the problems that could arise in the creation and implementation of an ASA would require more space than is available here. Yet we must recognize that history has a long shadow, and ASAs, despite their potential, may ultimately reflect or even reinforce historical problems in policing. Two such problems in particular—the difficulty in fighting improper bias and the issue of transparency—are helpful to underscore my point here.

Improper bias. First, the potential for ASAs to remove improper bias from the individualized suspicion determination will face substantial practical obstacles. As suggested earlier, even if ASAs take humans out of one part of the law enforcement process, humans will continue to possess enormous discretion over any investigation or prosecution. Even when an ASA makes a strong prediction of criminality, a human officer must still make an independent assessment of whether individualized suspicion exists. If individualized suspicion exists, the officer must decide whether to investigate further. Then an actual person must engage in the investigation pursuant to the ASA's prediction. Human prosecutors will decide whether and how to prosecute an individual whose criminal conduct is uncovered. If that individual is found guilty, a human judge must render the sentence. Any of these decisions along the way could be infected by conscious and unconscious bias.

That all being said, there is no doubt that the initial decision of an officer to pay attention to a specific individual, to conceive of him or her as a suspect rather than a civilian, is vulnerable to improper bias. (See L. Song Richardson, *Police Efficiency and the Fourth Amendment*, 87 IND. L.J. 1143, 1154–55 (2012).) Thus, removing bias from that step would make meaningful progress, even if it would not be a panacea for bias throughout the criminal justice system.

But even removing bias from an ASA's predictions is much harder than it seems. Certainly an ASA, once trained, would analyze new data automatically and without any intentional bias. (ASAs, after all, are machines like any other and incapable of forming any intention.) Yet numerous human decisions go into the programming

and training of the ASA, and these decisions may well be colored by conscious or unconscious biases. For instance, a human programmer must decide, thinking again in machine learning terms, what “features” will be used to “classify” the “objects.” Or, in plain English, the programmer must decide what characteristics or actions of a person the ASA will look at to decide whether the individual is likely engaged in criminality. Obviously, teaching the ASA to look at a feature like “race” or “skin color” or “religion” is likely undesirable. But what about the color of a person's clothing, membership in a specific organization with a religious affiliation, or the possession of a lawful gun license? Are these pieces of data just proxies for facts we don't want ASAs to consider? Difficult questions like these must be answered, and the answers may be the result of improper biases.

Moreover, an ASA, like any machine learning algorithm, must be trained using historical data. Yet those historical data are likely to have been generated through whatever troubling policing practices we might hope that ASAs would ameliorate. As a result, ASAs have the potential merely to replicate old biases.

To see this, think again about an ASA targeting cocaine dealing. Imagine, if you can, that a police department historically targeted cocaine dealing in predominately poor, minority neighborhoods, where cocaine was sold on street corners, but did not target dealing that occurred in middle-class neighborhoods, where cocaine was sold in private. An ASA trained on the data gathered from these historical practices would learn patterns of cocaine dealing that predict future street dealers, not patterns that would identify those dealing out of their homes. Assuming little change in dealing patterns on the ground in the future, the ASA would alert police only to likely dealers in the same poor, minority neighborhoods, thus perpetuating earlier police decisions that may have been motivated by improper bias.

In addition, to detect future crimes, an ASA must have access to new data. Those data must be collected, and decisions about the sources of the data will impact who the ASA can identify as a potential criminal. For instance, if our ASA targeting cocaine dealing is trained on data that includes video of past dealers, the ASA may well need current video to identify future dealers. That ASA can therefore work only where video is available. To the extent that data-collection sources, such as public video cameras, are distributed unequally, so too will an ASA's alerts and the accompanying police attention.

Finally, and in a similar vein, someone must decide where and in what situations to deploy ASAs. Should they be used to find cookers of methamphetamines or importers of heroin? Terrorists or perpetrators of domestic violence? Insider traders or check kitters? These questions are exceedingly difficult, and involve issues of policing policy, the application of possibly scarce research dollars, practicality, and politics, among others. They also, like all other human decisions, can be infected by improper biases.

Lack of transparency. The preceding discussion also raises the question of who will know what about how

an ASA works. Specifically, will the public have access to information about what crimes are being targeted by ASAs, what facts are being used by ASAs to identify perpetrators, or information about how effective ASAs are? As explained above, this information is necessary to accurately weigh an ASA's prediction in the individualized suspicion analysis, to ensure that ASAs work effectively and efficiently, and to uncover improper bias in ASA predictions. Issues of transparency are thorny in any area of algorithmic decision making (*see generally* FRANK PASQUALE, *THE BLACK BOX SOCIETY* (2015)), and in the arena of criminal justice they are particularly knotty.

First off, an ASA can create the illusion of unbiased decision making that can be dispelled only by a thorough investigation and understanding of how the ASA works. Computers do not have feelings or personal preference or irrational beliefs, at least not yet. Algorithms do not hate, distrust, or fear. People therefore assume that automated decisions have been cleansed of improper bias. But as explained just above, human biases can potentially infect a criminal prosecution in many ways, even if an ASA had a substantial role in identifying the likely criminal.

There are two kinds of bias, however, and each impacts the question of ASA transparency differently. The bias may be extrinsic to the ASA, stemming from decisions by police, prosecutors, or judges after the ASA's alert. In cases where such bias exists, the fact that an ASA initially identified the suspect may extend a somewhat unearned patina of fairness to the entire prosecution. Nonetheless, a careful observer would still recognize that human beings are making important decisions in the process. That observer should not have substantially greater difficulty in raising red flags about biased decision making because of the ASA's involvement.

The more confounding problem is biases that are inherent in how the ASA works, arising from the programming, training, or operation of the ASA. The presumed impartiality of the ASA can mask these biases and obscure their sources. Think again of the ASA targeting cocaine dealing. A police department dogged by accusations of racism based on historical practices could decide to start using the ASA to initiate future drug interdiction efforts. As explained above, unless much thought is put into its programming, training, and use, the ASA is likely to perpetuate past police biases in the field of cocaine interdiction. The ASA, perceived to be an unbiased algorithm, will provide cover, but the disproportionate impact will continue. Observers may see the disparate treatment, but without computer science training, they may be unable to recognize that it is the result of programming decisions and bias reflected in the data used to train and operate the ASA. The observer may raise a red flag, but the presumption of algorithmic purity can be used to stymie efforts to publicize or fix the problem.

The problem of uncovering bias inherent in an ASA will be compounded by secrecy about how the ASA works. Such secrecy will likely be justified on three grounds. First, remember that the most effective ASA—in other words,

the one that will be best at identifying patterns that correlate to criminal conduct—will likely analyze data in a way that is incomprehensible to any human, including the ones who programmed it. To put it another way, the best ASA will likely be a “black box” that cannot be made transparent without diminishing its effectiveness.

Second, there is a strong presumption against compelling law enforcement agencies to disclose their methods. Evidence of this presumption can be found in so-called sunshine laws that provide exemptions from disclosure requirements to information compiled for law enforcement purposes. (*See, e.g.*, Freedom of Information Act, 5 U.S.C. § 552(b)(1).) Further evidence is found in the government's limited privilege to withhold from a criminal defendant the identity of an informant. (*Roviaro v. United States*, 353 U.S. 53, 60 (1957).) The presumption is justified by the public's weighty interest in effective law enforcement and the belief that criminals who know too much about how police work will be able to “game the system” in order to avoid capture. The same argument would support, with varying degrees of force, arguments against the public disclosure of information about the programming and training of an ASA, ASA performance in the field, and the sources of data analyzed by the ASA in real time to make its predictions.

Third, to the extent that ASAs are developed by private entities, those entities are likely to claim intellectual property protection for their work and to require language in their contracts with police departments forbidding disclosure about how the ASA works or even of its existence. The most well-known recent example of such efforts in the criminal justice arena involves “stingray” or cell-site simulator technologies, which remained largely secret for years due in part to nondisclosure contracts signed by law enforcement agencies. (*See* Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J. L. & TECH. 1, 34–40 (2014).) Claims of trade secrecy and nondisclosure provisions could prevent any oversight of ASAs at all.

Conclusion

The challenges posed by ASAs want for easy solutions. They raise hard questions that implicate the fields of law, computer science, criminology, and policing. These questions demand nuanced answers and thoughtful consideration of practicality, policy, and politics. Unfortunately, without a concerted effort, it is likely that such questions will not be addressed head-on; rather, they will be answered implicitly, through decisions made by computer scientists, programmers, police captains, lawyers, and policymakers, each working more or less independently within their narrow field, each hopefully well meaning, and each incapable of knowing what they do not know.

My goal here, then, is to give some sense of the complexity of the issues that this emerging technology will

(continued on page 45)



CASES WITHOUT BORDERS

The Challenge of International Cybercrime Investigations

BY JASON P. GONZALEZ, MATTHEW A.S. ESWORTHY, AND NEAL J. GAUGER

In the spring of 2000, the technology sector had never been so robust. The Y2K panic had been reduced to a false alarm, navigated by a combination of industrious preparation and luck. Business was booming as well, with the NASDAQ riding toward a record high on the backs of soaring dot-com companies. And so on the morning of May 4, 2000, computer experts and regular users alike gave little thought before opening an e-mail in their inboxes bearing a simple, affectionate salutation: “ILOVEYOU.”

What followed remains to this day one of the most far-reaching and catastrophic cyberattacks ever recorded. The ILOVEYOU e-mail contained a vicious computer worm—soon known as the “Love Bug”—designed to copy the user’s passwords, overwrite files, and redistribute itself to every person in the victim’s Microsoft Outlook address book. (David Kleinbard & Richard Richmyer, *U.S. Catches “Love” Virus*, CNNMONEY (May 5, 2000), <http://tinyurl.com/n5ebm7a>; see also Peter Knight, *ILOVEYOU: Viruses, Paranoia, and the Environment of*

Risk, 48 SOC. REV., no. S2, Oct. 2000, at 17.) By the time it was stopped, the Love Bug would cause over 45 million individual “infections,” crash nearly 10 percent of the world’s computer servers, and cause an estimated \$8 billion in damage. (Knight, *supra*, at 17; see also James Meek, *Love Bug Virus Creates Worldwide Chaos*, GUARDIAN, May 5, 2000; Lorenzo Franceschi-Bicchierai, *Love Bug: The Virus That Hit 50 Million People Turns 15*, MOTHERBOARD (May 4, 2015), <http://tinyurl.com/po8glte>.)

International investigators quickly identified a pattern, noting that the Love Bug’s infections had first appeared in the Philippines before ricocheting across the world. Soon thereafter, they fingered a Philippine hacker ring known as “GRAMMERSoft” and its leaders, Onel de Guzman and Reonel Ramones, as the likely culprits. (Franceschi-Bicchierai, *supra*.) What happened next? Surprisingly, nothing. Despite being able to trace the virus to an IP address in Ramones’s apartment, and despite de Guzman’s admitted experience with writing computer viruses, no Philippine law

at the time provided a mechanism to prosecute individuals for computer crimes. (*Id.*; see also Seth Mydans, *Philippine Prosecutors Release “Love Bug” Suspect*, N.Y. TIMES, May 10, 2000, <http://tinyurl.com/pft9m9s>.) Moreover, due to a lack of international cooperation and treaty limitations, no international law enforcement arm was successful in investigating and prosecuting the GRAMMERSoft ring. De Guzman and Ramones went free, and neither has ever paid a criminal or civil penalty related to the attack.

The Love Bug saga provides a prime example of both the devastating effect of international cybercrime and the frustrating legal roadblocks that prevent perpetrators from being brought to justice. This article provides a brief survey of three unique and significant challenges that exist in investigating and prosecuting international cybercrime, as well as a review of efforts by the international community to help develop more robust and effective methods of pursuing online crime around the world.

Issue 1: “Dual Criminality” and Jurisdictional Conflicts

“Dual criminality” is a principle of international criminal law under which an accused individual may be extradited “only if the alleged criminal conduct is considered criminal under the laws of both the surrendering and requesting nations.” (United States v. Saccoccia, 18 F.3d 795, 800 n.6 (9th Cir. 1994).) This principle often provides a direct roadblock to prosecution of international cybercrime, and it was a key factor in barring prosecution of the Love Bug attack—the extradition treaty between the Philippines and the United States demands dual criminality. (See Extradition Treaty between the Government of the United States of America and the Government of the Republic of the Philippines, Nov. 13, 1994, S. TREATY DOC. 104-16 (“Article 2(1) defines an extraditable offense as one punishable under the laws of both Contracting Parties by deprivation of liberty for a period of more than one year, or by a more severe penalty.”).) As a result of the Philippines’ lack of computer crime statutes, the actions of the GRAMMERSoft ring were not considered a punishable offense outside of its borders; thus, investigators from the United States were unable to extradite members of the GRAMMERSoft hacking ring to face prosecution.

More recently, the 2014 hack of Sony Pictures Entertainment has met similar investigatory roadblocks. Intelligence officials from the United States have concluded that the hack originated in North Korea, and may have been sponsored by the North Korean government. (David E. Sanger & Nicole Perlroth, *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, N.Y. TIMES, Dec. 17, 2014, <http://tinyurl.com/nmz7uhh>.) While the North Korean government has attempted to deny involvement (referring to the attack as “the righteous deed of supporters and

sympathizers”), it has unsurprisingly also failed to provide any assistance to international prosecution efforts. (*Id.*) The outcome is plainly evident—without the cooperation of the North Korean government, there is simply no mechanism for foreign governments to take effective legal action against the individuals who perpetrated the hack.

In response to these frequent dead ends, the international community has taken steps to help encourage greater cooperation between nations with respect to cybercrime, including passage of UN General Assembly Resolution 55/63, designed to combat international “criminal misuse of information technologies.” Resolution 55/63 specifically calls on all member states to “eliminate safe havens for those who criminally misuse information technologies,” and further establishes that “law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States.” (G.A. Res. 55/63, U.N. Doc. A/RES/55/63 (Jan. 22, 2001).) These global efforts have been echoed on the regional level as well, with groups such as the Organization of American States (OAS) calling upon its member states to “creat[e] a framework for enacting laws that protect information systems, prevent the use of computers to facilitate illegal activity, and punish cybercrime.” (Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, OAS Res. AG/RES 2004 (XXXIV-O/04) (June 8, 2004), <http://tinyurl.com/ns2uuyn>.)

Despite these efforts, there remains significant resistance to abandoning the “dual criminality” principle, as nations are loath to expose their citizens to international criminal liability when such acts are not illegal under (and sometimes condoned by) the accused’s native government. Moreover, as seen in the Sony hack, many nations (including the United States) recognize the utility of cyberwarfare as a key method of nonmilitary aggression, and they may be resistant to allowing foreign governments to extend jurisdiction over such actions. (See, e.g., David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks against Iran*, N.Y. TIMES, June 1, 2012, <http://tinyurl.com/d4tjk6j> (discussing the Stuxnet cyberattack launched by the United States and Israel against the computer systems operating Iran’s nuclear enrichment facilities); David Hancock, *Feds Out-Hack Russian Hackers*, CBS NEWS (May 12, 2002), <http://tinyurl.com/q8dq64m> (discussing the Invita operation, the FBI counterhacking sting of Russian nationals engaged in the theft of credit card information).)

At this time, jurisdictional and other issues related to “dual criminality” seem likely to persist into the future; insufficient incentives exist for governments to change current practices and allow greater international oversight over their online actions and the actions of their citizens. Despite this, countries may find themselves needing to weigh the advantages of jurisdictional sovereignty against their ability to effectively combat an ever-increasing number of cross-border cybercrime attacks.

JASON P. GONZALEZ is a partner with Nixon Peabody in Los Angeles and MATTHEW A.S. ESWORTHY is a partner with Shapiro Sher Guinot & Sandler in Baltimore. NEAL J. GAUGER is an associate at Nixon Peabody.

Issue 2: Challenges with Investigation Coordination and Consistency

Even where cooperation between nations can be achieved, significant roadblocks stand in the way of effective international cybercrime investigations. The mechanisms available to facilitate investigations are often inefficient and lack oversight as to the process by which cybercriminals are pursued.

An example of one such mechanism is the use of mutual legal assistance treaties, commonly known as MLATs. Under an MLAT, prosecutors in one country may request assistance from their counterparts in a foreign country in order to perform tasks such as the investigation of suspects and the collection of evidence. (T. MARKUS FUNK, *MUTUAL LEGAL ASSISTANCE TREATIES AND LETTERS ROGATORY: A GUIDE FOR JUDGES* 2–3 (Fed. Judicial Ctr. 2014), <http://tinyurl.com/o5kqpmo>.) Once provided by the foreign counterpart, the collected evidence may be used in a prosecution in the requesting attorney's country. (*Id.*)

While simple in concept, the MLAT process is often dif-

given low priority in light of domestic cases that implicate local victims. (*Id.*) In a 2013 study conducted by the United States executive branch, it was found that the average “turnaround” time for an MLAT request is 10 months, “with some requests taking considerably longer.” (RICHARD A. CLARKE ET AL., *LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT’S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES* 226–27 (2013), <http://tinyurl.com/o5x8cea>.) As discussed below in Issue 3, these delays can severely damage the effectiveness of a cybercrime investigation, wherein criminals often move quickly to erase traceable records of their actions online.

Despite these challenges, the MLAT process remains preferable to the use of “letters rogatory,” the predominant alternative method for gathering information across international borders. Under an MLAT, a request for information is made based on a binding treaty guaranteeing cooperation between the contracting nations; in comparison, a letter rogatory is merely an informal

Even where cooperation between nations can be achieved, significant roadblocks stand in the way of effective international cybercrime investigations.

ficult and time-consuming to accomplish. As an example, for an attorney from the United States to seek subpoena information, execute a search warrant, or gain compliance with a court order under an MLAT, the attorney must provide a specific request (which must be approved by the foreign nation's courts) identifying, among other information, the requesting agency, a description of the subject matter and nature of the investigation (including the specific criminal offenses suspected to have been committed), and a description of the evidence, information, or other assistance sought. (*Id.* at 7.) The detailed nature of this request and the requirement for international approval can often complicate and impede efforts at information gathering. This can be particularly true early in an investigation, when the theories driving a prosecution effort may still be in the process of development.

Even if a sufficient request can be drafted, prosecutors who use MLATs are often required to conduct their inquiry at arm's length; rather than traveling abroad to conduct a firsthand investigation, the prosecutors must rely on their counterparts in the foreign jurisdiction to execute the requested task. (Peter Swire & Justin D. Hemmings, *Re-Engineering the Mutual Legal Assistance Treaty Process*, 71 N.Y.U. ANN. SURV. AM. L. (forthcoming 2016).) This requirement can cause frequent miscommunications and delays: Because the foreign jurisdiction often has a full slate of domestic matters that require its attention, a requesting attorney may find that the request is

request that relies on the goodwill of foreign courts and law enforcement officials to be properly executed. (Pamela D. Pengelley, *A Compelling Situation: Enforcing American Letters Rogatory in Ontario*, 85 LA REVUE DU BARREAU CANADIEN 345, 346–47 (2006).)

In the face of these limitations, reforming MLAT procedures to allow a requesting attorney to have greater oversight and control (including direct participation in the foreign investigation) may lead to greater coordination, consistency, and outcomes. The efficacy of this proposal can be seen in investigations where nations have worked together to facilitate informal communications and cooperation in addition to their treaty obligations.

For example, in 2014, the US Department of Justice (DOJ) successfully led a multinational criminal investigation and prosecution against the Gameover Zeus botnet, a global network of criminals who caused over \$100 million dollars in losses to businesses and consumers worldwide. (Press Release, U.S. Dep't of Justice, U.S. Leads Multinational Action against “Gameover Zeus” Botnet and “Cryptolocker” Ransomware, Charges Botnet Administrator (June 2, 2014), <http://tinyurl.com/owgkfrw>.) By using a broad-spectrum, carefully coordinated approach, and by freely sharing information across public and private entities as varied as Italy's *Polizia Postale e delle Comunicazioni* (Postal and Communications Police), Ukraine's Ministry of Internal Affairs, Carnegie Mellon University, and Microsoft, investigators were able to efficiently and

effectively secure indictments against the leaders of the Gameover Zeus group.

While it is widely accepted that the formal MLAT procedures will require reform to be effective against cybercrime, the Gameover Zeus case provides a fantastic example of how informal international cooperation can and will help provide effective prosecutorial outcomes. In an area where technology consistently outpaces the laws that govern it, such collaborative action will likely be needed to ensure governments keep pace with cybercriminals going forward.

Issue 3: Difficulties with Identification and Disclosure of Traffic Data

Separate from intercountry inefficiencies, nearly all cybercrime investigations encounter a common impediment—the anonymity of the Internet, and the ability of criminals to cover their tracks. Since 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) has been responsible for, among other tasks, “coordinating the allocation and assignment of three unique identifies for the internet”: domain names, IP addresses, and protocol

for law enforcement, such actions would likely draw strong objections from lawful users who, beyond the scope of domain name registration, prize the option of keeping their real-life identifies separate from their nameless online interactions. (See, e.g., *Cheating Website Ashley Madison Hacked, Personal Info Posted*, BIG STORY (July 20, 2015), <http://tinyurl.com/phwagcp>.) As ICANN’s registration requirements evolve, the organization will have no choice but to weigh privacy concerns against the need for effectively tracing online criminal actions.

Apart from ICANN’s registration requirements, many other inefficiencies exist in pursuing the identities of cybercriminals. International cybercrime cases often involve tracing a hack through multiple IP addresses around the world, which can, in turn, mean digging through multiple layers of anonymity. Because speed is key to keeping online “trails” from growing cold, some intergovernmental organizations have recognized a special need to expedite disclosure of cyberspace traffic data across international borders. One such effort has been spearheaded by the Council of Europe, which requires (with few exceptions)

Intergovernmental organizations have recognized a special need to expedite disclosure of cyberspace traffic data across international borders.

port and parameter numbers. (*Bylaws for Internet Corporation for Assigned Names and Numbers*, ICANN (July 30, 2014), <http://tinyurl.com/pljjwh4>.) In plain English, this means that ICANN directly or indirectly oversees how and where individuals and their computers are identified on the Internet. Under current standards, ICANN effectively allows anonymous registration of domains, and does not appear to independently verify contact information provided to it by third-party registrar companies. (*Current Agreement*, ICANN (May 21, 2009), <http://tinyurl.com/p3mpgjr>; see also *Verifying Contact Information for ICANN Validation*, GoDaddy, <http://tinyurl.com/qxf3evg> (verifying only that a user has provided GoDaddy with an “active and accurate” e-mail account in order to confirm ICANN validation).)

Minor changes to the operation of ICANN could provide significant barriers to the use of computer networks for criminal purposes. For example, if ICANN were to require the submission and verification of a government-issued identification in order to register a domain name, the pool of individuals who submit false information would almost certainly shrink. A similar reduction in fraud would likely be seen by barring the use of prepaid credit cards or bitcoin to pay registration fees; a registration process that requires payment from authorized banks would undoubtedly provide more effective mechanisms for tracing individual actions online to the persons who committed them. Of course, while effective

that where a “tracing” request is made between council member states, “a sufficient amount of traffic data” must be “expeditiously disclose[d]” in order “to identify th[e] service provider and the path through which the communication was transmitted.” (Council of Europe, Convention on Cybercrime, art. 30, Nov. 23, 2001, Eur. T.S. No. 185.)

The open trade of “traffic data” between member states is a potentially fertile area for cooperation between governments. Because such data provides only the pathways through which a criminal act was allegedly taken, rather than the subject matter of the act itself, the scope of information provided does not require the more sophisticated analysis and approval of an MLAT request or other information-gathering mechanisms. While larger structural changes to international cooperation would likely be welcomed by many prosecutors, small changes like this can provide key advantages in combating fast-moving criminals online.

Ultimately, if the global community is able to meet the unique challenges presented by cybercrime, it will do so because sovereign nations band together, combine their resources, and recognize that cybercriminals rarely restrict themselves to the borders of a single nation. By embracing a policy of openness, and by placing an emphasis on efficient and effective collaboration, the world will be best able to beat back the ever-growing and increasingly sophisticated plague of hackers lurking online. ■

Location! Location! Location!

Data Technologies and the Fourth Amendment

BY RODOLFO RAMIREZ, KELLY KING, AND LORI DING



It appears that whenever you log on to Facebook or another social network site, you have a window into how everyone else lives their lives. Whether it is the friend who constantly travels or the person who keeps a daily photo journal of her cat's life, the Internet is full of information about others. So eager are people to publicly share their lives that you can follow in real time as they visit their favorite coffee shops or restaurants. Although they may want friends to see their photos, these individuals may not know that some of the photos they post online contain GPS coordinates that allow others to know precisely where those pictures were taken. This often uninformed sharing of so much information has its downside, something that Adam Savage, host of the popular television series *Myth-Busters*, ruefully discovered. When he posted on Twitter a photo of his vehicle parked on the street in front of his home, he was unintentionally letting some savvy viewers know exactly where he lived. How? The photo was geotagged. (Kate Murphy, *Web Photos That Reveal Secrets, Like Where You Live*, N.Y. TIMES, Aug. 11, 2010, [\[tinyurl.com/qx95sw5\]\(http://tinyurl.com/qx95sw5\).\) That he also mentioned he was “off to work” would have been an added bonus had anyone been looking to burglarize his empty house.](http://</p></div><div data-bbox=)

The Technology

Geotagging, which has become prevalent on social media websites and electronic devices such as smartphones, is a process that combines the Global Positioning System (GPS) with information technology by capturing location data in terms of longitude and latitude. Once captured, the information becomes a geotag that is embedded in the photo's metadata, which is then typically stored in the image as a digital file. Metadata is often referred to as “data about data” because it provides information such as when that data was last edited or what type of computer program was used to create it. (NAT'L INFO. STANDARDS ORG., UNDERSTANDING METADATA (2004), <http://tinyurl.com/y99olov>.) When location data is embedded in an image, that information is included in the metadata of the file as an exchangeable image file format (EXIF).

EXIF is a standard file format that allows images to be viewed across different digital devices. Each time a camera, whether a stand-alone or as part of a smartphone or laptop, is used to take a photograph, it records more than the image itself. It captures the time and date that the image was taken; more complex cameras also record the exposure time, aperture setting, and shutter speed. This information is collectively referred to as the EXIF header.

GPS data such as latitude, longitude, and altitude can now be automatically included in the EXIF header. Most of today's cameras and smartphones can determine where a device is located and automatically geotag a photograph or other file with that information. Electronic devices are able to detect their location in multiple ways. Many cameras and smartphones are equipped with built-in GPS capability. These devices also commonly employ triangulation in order to determine location coordinates. As long as the device is able to determine its proximity to three different known locations—typically using cell towers or Wi-Fi Internet hotspots for this purpose—it is able to determine its own location based on the strength of the signal it receives.

Viewing this geotagged information is relatively easy using various metadata access tools and editors, such as ExifTool, Opanda, EnCase, and AccessData FTK. While the latest models of digital cameras are no longer set to automatically geotag photographs, this function has only recently ceased to be a default setting for many smartphones with GPS capabilities and popular social media websites like Facebook and YouTube. Currently among the world's top social networking sites, Facebook, Instagram, and Twitter have begun to recognize the potential dangers of providing constant streams of location data about their users' daily lives.

Although geotagging is no longer an automatic feature, these social media sites continue to provide it as an optional but standard function on both their websites and on mobile devices through licensed third-party smartphone applications. With one click of a mouse or tap of a finger, users can choose to add their location each time they post content, making publicly available their specific GPS coordinates. Many users are unaware of the implications of this function and exercise little caution, which may threaten users' security by presenting opportunities for criminals to track unsuspecting users' movements and whereabouts.

However, law enforcement can just as easily use geotags to their advantage, as in the case of Higinio Ochoa, a criminal wanted for publicly posting the names and addresses of more than 100 law enforcement personnel. Ochoa taunted

the Federal Bureau of Investigation (FBI) by posting to his Twitter account a photo of his girlfriend's cleavage captioned with a message mocking law enforcement. The FBI was able to pull metadata off this photo, revealing that the image had been taken in Australia, a fact the FBI used to confirm the girlfriend's identity. Subsequent information then led to Ochoa's arrest in Galveston, Texas, where he was sentenced to 27 months in a federal prison.

As Ochoa's case demonstrates, metadata can be a powerful tool for law enforcement institutions. However, because geotags and other metadata are an emerging form of evidence in trials, many questions and concerns surround their admissibility.

Monitoring Software

When *New York Times* blogger David Pogue couldn't find his phone, he employed Find My iPhone, Twitter, and many online volunteers to track his phone down to a house in Maryland. The phone was eventually recovered by police in a backyard, but no one was charged because it was "unclear if the phone was actually stolen or misplaced." (Julianne Pepitone, *How the Internet Found David Pogue's Missing iPhone*, CNN MONEY (Aug. 3, 2012), <http://tinyurl.com/nn9vwb8>.) Thanks to the introduction of software like Find My iPhone and Computrace, digital devices are getting easier to recover if stolen or lost. Some people who have had their property stolen have even created blogs dedicated to tracking down the thief. These programs rely on Internet Protocol (IP) addresses and GPS coordinates to locate the lost or stolen property.

Some of these programs, like Absolute Software's LoJack for Laptops, do more than just track phones. LoJack uses GPS, Wi-Fi, or IP addresses to locate the property. As long as the laptop is connected, LoJack can track user activity by capturing keystrokes, thereby capturing information that may lead to recovery of the laptop. (See *State v. Galemore*, No. M2012-01783-CCA-R3-CD, 2013 WL 4679982, at *1 (Tenn. Crim. App. Aug. 29, 2013).) Even if the thief reinstalls the operating system, LoJack will still be able to monitor the computer because of a program hidden on the BIOS—the computer's basic "firmware." (Elinor Mills, *To Catch a Thief, with Monitoring Software*, CNET (Oct. 9, 2012), <http://tinyurl.com/pbv3cvo>.)

Wi-Fi. Smartphones can now be tracked through their connections to Wi-Fi wireless networks. One method is to track phones by their media access control (MAC) addresses. A MAC address is a unique code that is assigned to a phone when it is manufactured and is used to identify a specific device. Unlike IP addresses that can change when a device joins a different Wi-Fi network, MAC addresses remain constant. In order for a smartphone to locate and connect to nearby Wi-Fi networks, it sends out information, including its MAC address. Once the phone sends out its MAC address, that information can be collected and read by other parties. Many retailers are already making use of this technology to collect data about their customers.

RODOLFO RAMIREZ is a special assistant United States attorney in Houston, Texas. He also teaches a cybercrime class at Rice University. Contact him at rodolfo@rice.edu. **KELLY KING** is a student at Harvard Law School. **LORI DING** is a junior at Rice University. Cecilia Alvarez, Natalie Gow, Rachel Landsman, Cynthia Bau, and Gail McConnell assisted in the production of this article. The opinions expressed here are not those of the US Department of Justice, US Attorney's Office, or Texas Attorney General.

A phone's location history can also be determined because many smartphones collect and back up this data. For example, the Apple iPhone stores its location history in a data file called its Property List (also known as a plist). (TIM PROFFITT, SANS INST., FORENSIC ANALYSIS ON iOS DEVICES 4 (June 2012), <http://tinyurl.com/nnbbzro>.) The iPhone captures this data through iOS applications that access the phone's location data, which is in turn determined by GPS and Wi-Fi connections. Once the location of the phone has been determined, the data is stored in a plist file named "consolidated.db," which contains all Wi-Fi and stored map locations. (*Id.* at 19.) After this data has been collected, the iOS applications will interact with the Apple Core Location application programming interface (API) to interpret it. If a person were to use the phone during a crime, law enforcement would be able to seize the phone and track the individual's past movement by the location data saved on the phone.

Beacons. It is a simple task to place a tracking device or tracking software on real property, such as a laptop or phone, in case it is stolen. When the property is data, the proper precautions are less obvious. Major companies have fallen victim to security breaches in which various data from customer information to intellectual property were compromised. In 2013, Target suffered a massive and well-publicized breach, with many customers' credit and debit card information stolen. To prevent situations such as this, a beacon can be embedded in sensitive digital documents. A beacon sends out a signal to a server when the sensitive document is opened, indicating the IP address of the device being used to access that document. Law enforcement can use this information to track down the location of the document and obtain a warrant.

Social media. Social media sites like Facebook, Twitter, and Yelp allow users to manually include explicit location information on any of their content, often with time stamps, separate from any location metadata that may already be embedded on photos or videos that users post. These location tags and "check-ins" may be viewable on users' profiles as part of other posts or as discrete posts. For example, Facebook allows users to "add a location," such as cities or landmarks, to status updates, photographs, and videos, and the site now summarizes all of that data into a "Places" profile feature where others can view all of a profile owner's past locations on a map. (*Facebook Introduces Check-In Feature*, CNN (Aug. 18, 2010), <http://tinyurl.com/nt84e7k>.) On GPS-enabled devices, Facebook and Twitter applications also allow the user to add a precise current location or "check-in" from a list of nearby places based on the user's GPS coordinates. Similarly, Yelp users can check in to restaurants or other venues with specific addresses already listed, often with special offer incentives from businesses to do so. Though privacy settings may affect who is able to view the profile or even certain posts, these check-ins and location tags are generally viewable on users' profiles so that screenshots or printouts might be made. For example, the court in *Griffin v. State* acknowledged that printouts of profiles, which

include users' posts and check-ins, may be submitted as evidence. (19 A.3d 415 (Md. 2011).) The allowed use of metadata evidence gleaned from a photograph posted to the Internet in *United States v. Post* suggests that any metadata attached to social media posts would also be useable as evidence without violating Fourth Amendment rights, much like "fingerprints" unknowingly left behind by the user. (997 F. Supp. 2d 602 (S.D. Tex. 2014).)

These posts could be considered as being made through a third party, either the social media site or other users. A user can tag other users at some location or in a photograph at will that may not be reflective of reality. However, tagged users can easily remove those tags. There is also some debate as to whether social media sites can even be subpoenaed for further information. Some courts believe that social media sites fall under the protection afforded to electronic communication services, which is "any service which provides to users thereof the ability to send or receive wire or electronic communications." (*Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 972 (C.D. Cal. 2010) (quoting 18 U.S.C. § 2510(15)).) However, others state that content other than private chats or messages, such as photo or status posts, do not fall under this protection because they are immediately available and therefore allow subpoenas to social media sites.

Admissibility

All electronically stored information (ESI) must meet certain standards before it can be admitted as evidence. A framework for the admission of ESI was established by Judge Paul Grimm in *Lorraine v. Markel American Insurance Co.* that now serves as a guideline for the admission of ESI into evidence based on the Federal Rules of Evidence (FRE). (241 F.R.D. 534 (D. Md. 2007).)

The first predicate for the admission of any type of evidence, including ESI, is to establish relevancy. The ESI must be relevant, or related, to the case. As stated in the FRE, relevant evidence is evidence that, if admitted, "has any tendency to make a fact more or less probable than it would be without the evidence" when "the fact is of consequence in determining the action." (FED. R. EVID. 401.) Establishing relevance for ESI, including metadata and geotagging, is typically not an issue. (*Lorraine*, 241 F.R.D. at 541.)

Next, the ESI must be authenticated. In order for ESI to be authenticated, evidence must be offered that is "sufficient to support a finding that the item is what the proponent claims it is." (FED. R. EVID. 901(a).) However, the standard of authenticity for the proffered evidence is relatively low because the burden of proof is merely prima facie. (*Lorraine*, 241 F.R.D. at 542.) Authentication requirements are only meant to be "threshold preliminary standard[s] to test the reliability of evidence, subject to later review by an opponent's cross-examination." (*Id.* at 544.) Once this threshold has been met, the evidence has been authenticated.

The most common way to authenticate metadata, including geotagging, is by FRE 901(b)(9). (Linda L.

Listrom et al., *The Next Frontier: Admissibility of Electronic Evidence* 14 (2007) (unpublished ABA Annual Meeting program material.) Authentication occurs by introducing “[e]vidence describing a process or system and showing that it produces an accurate result.” (FED. R. EVID. 901(b)(9).) This can typically be done through the testimony of a person with knowledge of the relevant process or system. The Court of Criminal Appeals of Tennessee allowed “persons with special knowledge about the operation of the computer system [to give] evidence about the accuracy and reliability” of the system in order to authenticate the evidence. (*State v. Meeks*, 867 S.W.2d 361, 376 (Tenn. Crim. App. 1993); *see also* *State v. Hall*, 976 S.W.2d 121, 147 (Tenn. 1998) (finding a computer generated telephone bill was authenticated after an employee with knowledge about how the computer system operated testified to its reliability).) The Texas Court of Appeals has also held that the testimony from an employee who used and was familiar with the electronic monitoring system was sufficient to authenticate evidence. (*Ly v. State*, 908 S.W.2d 598 (Tex. App. 1995).) The evidence in question was a printout generated by the electronic monitoring computer. (*Id.* at 600.) After the employee testified to the “reliability and accuracy” of the system, the court determined that the printout was authentic. (*Id.* at 601.) Because geotags are also ESI generated by a computer, testimony from a person with knowledge about how the computer functions is sufficient to authenticate it.

However, when trying to admit profiles from social media sites, other factors must be considered. Because anyone can make a profile under any name on these sites, additional circumstantial information is necessary to authenticate social media messages. Simply being marked as sent from a particular profile is not enough, as profiles can be hacked into or used without permission. If the profile’s owner logs in to his or her computer and then leaves it unattended and logged in to the owner’s account on a social media site, no further verification is needed to create posts or messages. Testimony from a party to the conversation alone may be sufficient to authenticate the contents of message conversations, but not the identity of the other party. The Maryland Court of Appeals in *Griffin v. State* described three methods by which social media evidence—and by extension, their metadata—may be authenticated. (*Griffin*, 19 A.3d at 427–28.)

1. Provide witness testimony from the purported creator or noncreator as to whether the evidence accurately represents what the witness saw.
2. Search the personal computer of the purported creator, and then examine its Internet history and hard drive to determine whether the profile or posting originated from that computer.
3. Produce information from the social networking website that links the purported creator to the profile or posted content in question.

The Texas Court of Criminal Appeals in *Tienda v. State* noted that the *Griffin* methods of authentication are reliable, but that different combinations or amounts of identifying

or otherwise distinctive circumstantial evidence may also be sufficient. (*Tienda v. State*, 358 S.W.3d 633, (Tex. Crim. App. 2012).) While the three *Griffin* guidelines still require evidence of a social media profile to be proved, *Tienda* sets a slightly lower standard for authentication, requiring only that a jury could reasonably find the evidence to be authentic.

After the ESI has been authenticated, it must be determined not to be hearsay, which is “a statement,” not made by a testifying declarant, “offer[ed] in evidence to prove the truth of the matter asserted.” (FED. R. EVID. 801(c).) A statement is defined as “a person’s oral assertion, written assertion, or nonverbal conduct.” (FED. R. EVID. 801(a).) Therefore, metadata and geotagging cannot be hearsay because they are not statements made by a person. (*Lorraine*, 241 F.R.D. at 564.) Several courts have upheld this distinction, including the United States Tenth Circuit Court of Appeals, which held that a computer generated “header” was not hearsay because the information was automatically generated by a computer without any input from a person. (*United States v. Hamilton*, 413 F.3d 1138, 1142 (10th Cir. 2005); *see also* *United States v. Lamons*, 532 F.3d 1251, 1262–64 (11th Cir. 2008) (holding that because automatically generated data is not a statement by a person, it cannot be hearsay); *United States v. Washington*, 498 F.3d 225, 230–31 (4th Cir. 2007) (finding the data generated by machines did not receive any input from humans, so it could not be hearsay).)

Next, the ESI provided should either be an original or considered as an admissible duplicate based on FRE 1001–1008. This is often called the best evidence rule or original writing rule. (Jocelyn D. Larkin, *Getting It In: The Admissibility of Electronically Stored Information in Employment Litigation* 3 (2014), available at <http://tinyurl.com/q4k67aw> (unpublished program materials, 8th Annual ABA Section of Labor and Employment Law Conference).) When speaking of metadata and geotagging, any printout or duplicate of such information would be admissible “so long as it accurately reflects the data.” (*Lorraine*, 241 F.R.D. at 578.) Any computer printout of such information that has been certified is admissible. (*Norton v. State*, 502 So. 2d 393, 394 (Ala. Crim. App. 1987).)

Finally, the probative value of ESI must not be “substantially outweighed” by “unfair prejudice” or any other consideration embodied in FRE 403.

Fourth Amendment Issues

Right to privacy. Application of the Fourth Amendment to new technologies continues to present challenges. In order for a defendant to argue that Fourth Amendment rights have been violated, the individual must first prove that he or she has a “reasonable expectation of privacy.” (*United States v. Cardoza-Hinojosa*, 140 F.3d 610, 614 (5th Cir. 1998).) The question of whether one has a reasonable expectation of privacy is determined by whether it is “one which society would recognize as reasonable.” (*United States v. Kye Soo Lee*, 898 F.2d 1034, 1037–38 (5th Cir. 1990).)

One court has recently taken up this application

when looking at geotags. In *United States v. Post*, agents discovered a website used for the distribution of child pornography. (997 F. Supp. 2d 602, 602–03 (S.D. Tex. 2014).) Unfortunately, law enforcement personnel were not able to use the IP address of a user who had posted an image of child pornography because the IP address was masked. However, these agents were able to locate the user using a photo posted online by that user. They were able to pull metadata off of the image that contained the GPS coordinates of the location where the photo was taken, along with the type of phone used to take the photo. This information eventually led to the arrest of Donald Post in League City, Texas. (*Id.* at 603–04.)

At trial, Post claimed that the inclusion of the metadata and thus the geotag on the photo constituted a violation of his Fourth Amendment rights. Post conceded that he did not claim any privacy interest regarding the image he posted on the Internet. This is supported by *United States v. Dodson*, where the court held that the defendant did not have a reasonable expectation of privacy in contents of

files he made available for public download. (960 F. Supp. 2d 689 (W.D. Tex. 2013).) However, Post argued that he held a privacy interest in the metadata embedded in the image because he did not realize that he was releasing information such as his location, and his intent was to remain anonymous. (*Post*, 997 F. Supp. 2d at 604.)

The Fourth Amendment refers to “[t]he right of the people to be secure in their persons, houses, papers, and effects.” (U.S. CONST. amend. IV.) In this case, Post offered up the electronic image or his “effect” when he posted it online. The court held that “[t]here is no basis for divvying up the image Post uploaded into portions that are now public and portions in which he retains a privacy interest.” (*Post*, 997 F. Supp. 2d at 605.)

Whether Post knew he was releasing his location or not is irrelevant; he posted the information on the Internet, giving law enforcement the opportunity to find him. The court analogized this to leaving biological evidence behind at a crime scene before DNA analysis technology was fully developed. If Post was later identified because of

More Reading and Background Resources

Craig Valli & Peter Hannay, Sec. Research Ctr., *Geotagging Where Cyberspace Comes to Your Place* (2010), <http://tinyurl.com/okoewbc>.

Dave Roos, *How GPS Photo Taggers Work*, HOW STUFF WORKS TECH, <http://tinyurl.com/n99erf8> (last visited Nov. 13, 2015).

Karl Kruszelnicki, *Geotagging: How Much Do Your Photos Give Away?*, ABC SCI. (June 5, 2012), <http://tinyurl.com/pjnybxq>.

Brian Fung, *How Stores Use Your Phone's WiFi to Track Your Shopping Habits*, WASH. POST, Oct. 19, 2013, <http://tinyurl.com/p6rz7d4>.

Gerald Friedland & Robin Sommer, Int'l Computer Sci. Inst., *Cybercasing the Joint: On the Privacy Implications of Geo-Tagging* (May 3, 2010), <http://tinyurl.com/nvu4qcb>.

Latanya Sweeney, *My Phone at Your Service*, FED. TRADE COMM'N (Feb. 12, 2014), <http://tinyurl.com/nks9zcr>.

Twitter Location Search: A Complete Guide, THOUGHTFAUCET, <http://tinyurl.com/ov886ry> (last visited Nov. 13, 2015).

David Pogue, *Where Is David Pogue's iPhone?*, N.Y. TIMES POGUE'S POSTS (Aug. 2, 2012), <http://tinyurl.com/nac94rk>.

Joshua Kaufman, *This Guy Has My MacBook*, TUMBLR (Mar. 21, 2011), <http://tinyurl.com/3t5t7t8>.

Press Release, FBI San Antonio Div., U.S. Attorney's Office, *Galveston Man Sentenced to Federal Prison*

for Computer Hacking (Aug. 24, 2012), <http://tinyurl.com/oupz9n8>.

Jeffrey D. Bukowski, *E-Discovery without Admissibility Is Useless: Lorraine v. Markel and Authentication*, 17 PROOF (ABA), no. 1, Fall 2008, <http://tinyurl.com/ore6g99>.

MATS ENGMAN, HALMSTAD UNIV., *FORENSIC INVESTIGATIONS OF APPLE'S IPHONE 8* (2013), <http://tinyurl.com/pzyhkqu>.

Linda L. Listrom et al., *The Next Frontier: Admissibility of Electronic Evidence 14* (2007) (unpublished 2007 ABA Annual Meeting program material).

Brooks Threatened with Contempt, HARNESS EDGE (Apr. 6, 2010), <http://tinyurl.com/nvqat4e>.

Alex Levinson, *3 New Thoughts on Mobile Location—A Follow Up to Apple Location Tracking*, ALEX LEVINSON (Apr. 23, 2011), <http://tinyurl.com/ojck39z>.

Brian M. Bowen et al., Columbia Univ. Dep't of Computer Sci., *Baiting Inside Attackers Using Decoy Documents* (2009), <http://tinyurl.com/pc4rvoe>.

Keith Lee, *Social Media Subpoena Guide 2015 Edition*, ASSOCIATE'S MIND (Jan. 26, 2015), <http://tinyurl.com/lk6b5da>.

CAMERA & IMAGING PRODS. ASS'N, *CIPA DC-010-2012, EXIF 2.3 METADATA FOR XMP* (2012), <http://tinyurl.com/njf78yx>.

View and Remove Exif Online, VEREXIF, <http://www.verexif.com/en/> (last visited Nov. 13, 2015).

hairs he had inadvertently left behind, he would not be able to suppress the results of the DNA analysis. He made his photograph viewable to the public and, “once it was left in a public place, he no longer had a Fourth Amendment privacy interest in it.” (*Id.* at 606.) Therefore, his Fourth Amendment rights were not violated.

When monitoring software is being used to track a stolen computer, there are two hurdles for a defendant to overcome to claim any privacy rights. First, courts have ruled that there is no expectation of privacy in a computer that has been stolen. (*United States v. Wong*, 334 F.3d 831, 839 (9th Cir. 2003).) An important consideration in this determination is whether a defendant had a legitimate

the Electronic Communications Privacy Act (ECPA) and the Stored Communications Act (SCA). (*Id.* at 864.) The court found that the officers also had qualified immunity under these acts. (*Id.* at 877–79.) This is likely a very common situation, as there are many theft recovery services that directly handle the tracking process and data prior to handing information over to the police. Less commonly however, in this case the company also intercepted photographs and messages sent between the possessor of the stolen laptop and her boyfriend. The *Clements-Jeffrey* court firmly asserted that this constituted wiretapping and therefore violated the ECPA. The court stated that there is a clear distinction between intercepting commu-

Because tracking technologies are simple to use and accessible online, law enforcement is no longer restricted to more expensive, specialized software.

expectation of privacy in the area searched. (*See United States v. Salvucci*, 448 U.S. 83, 91 (1980); *United States v. Lyons*, 992 F.2d 1029 (10th Cir. 1993).) However, this only extends to a person who knowingly possesses stolen property. (*United States v. Tropiano*, 50 F.3d 157, 161 (2d Cir. 1995).)

In *Clements-Jeffrey v. City of Springfield*, the plaintiff purchased a laptop that was stolen from a school. (810 F. Supp. 2d 857, 861 (S.D. Ohio 2011).) The school district had installed software that allowed the software company to track the laptop. The company obtained the IP address, electronic communications, screenshots, and all keystrokes. (*Id.* at 861–62.) In one instance, “while monitoring webcam communications between [the plaintiff and her boyfriend] in ‘real time,’ [the company] took three screen shots of images appearing on the monitor,” which contained sexually explicit images of the plaintiff and her boyfriend. (*Id.* at 862.) Using the aggregated information, police were able to find the plaintiff and obtain the laptop. The plaintiff filed suit after the theft case was dismissed. (*Id.* at 863.) The court ruled that the plaintiff did not know nor should have known the computer was stolen. (*Id.* at 866.)

The court then turned to the issue of qualified immunity for the police officers. The plaintiff argued that law enforcement only needed her IP address and not the sexually explicit communications. (*Id.* at 867–68.) The court determined that the officers had qualified immunity. “[T] here is simply no legal basis for holding [the officers] liable under § 1983 for their ‘use’ of the sexually explicit communications allegedly illegally intercepted by [the software company].” (*Id.* at 868.) The court concluded that the company was not acting on behalf of a government agent. (*Id.* at 869.)

The plaintiff also alleged other privacy violations under

communications on a laptop and simply determining its location; the former is much more intrusive than the latter. Because the ECPA does not state that wiretapping becomes lawful when attempting to find and recover stolen property, the court implied that, stolen or not, the possessor of the laptop has a privacy interest in the communications made with it.

The second hurdle is that the Fourth Amendment’s search and seizure provision does not apply to private actors. (*See United States v. Jacobsen*, 466 U.S. 109 (1984).) However, there is a case that has ruled otherwise depending on the government involvement. (*See State v. Oliveras*, 65 So. 3d 1162 (Fla. Dist. Ct. App. 2011).)

Search warrants. Technologies that enable the use of GPS and IP addresses can narrow a location to a small area and make it easier to obtain warrants. However, what happens when these functions are not turned on or used? In *State v. Galemore*, the victim’s house was burglarized and her laptop was stolen. (No. M2012-01783-CCA-R3-CD, 2013 WL 4679982, at *1 (Tenn. Crim. App. Aug. 29, 2013).) Using computer tracing software, the detective learned that Galemore had used the laptop to log on to her Facebook account via her Yahoo! account. (*Id.* at *2.) Using this information, the detective found a home address for Galemore and visited the house. An unknown male answered the door and confirmed that a computer was inside, but refused to let the detective inside the house. Based on this information, the detective obtained a warrant to search the defendant’s house for the laptop.

Galemore complained that the evidence did not provide a sufficient nexus, arguing that she could have logged on to her Facebook account from anywhere, making the nexus stale. (*Id.* at *5.) Galemore also argued that two days had

passed between the time she most recently logged on and the search of the house, making it stale.

The court was not persuaded by Galemore's argument. (*Id.* at *7.) It noted that Galemore was in possession of stolen property at the time she logged on, and just because the computer was portable it was still "reasonable to infer that the Defendant retained possession of it." (*Id.*) The court also considered the fact that someone said the laptop was inside the house.

Fifth Amendment Issue

Location data can be very powerful evidence in a trial. However, is it evidence that the defendant has a right not to turn over because it would be self-incriminating? The Fifth Amendment affords protection against being "compelled in any criminal case to be a witness against himself." (U.S. CONST. amend. V.) Nevertheless, defendants can still be subpoenaed for evidence that may incriminate them. However, a privilege derived from the Fifth Amendment known as the "act of production doctrine" allows a defendant to refuse to turn over incriminating evidence if "the act of producing the evidence would contain 'testimonial' features." (*United States v. Hubbell*, 530 U.S. 27, 49 (2000).) The evidence is considered testimonial if and only if it, "explicitly or implicitly, relate[s] a factual assertion or disclose[s] information." (*Doe v. United States*, 487 U.S. 201, 210 (1988).)

In *United States v. Hatfield*, the defendant, David Brooks, was ordered to produce metadata to determine the authenticity of an e-mail that his attorney submitted in order to discredit a witness for the government. Brooks refused to do so, citing the act of production privilege. (Order to Produce Metadata, *United States v. Hatfield*, No. 06-CR-0550 (E.D.N.Y. Apr. 7, 2010).) However, the

court found that the doctrine did not apply. The judge determined that the doctrine would apply "only (1) 'if the existence and location of the subpoenaed papers are unknown to the government'; or (2) where production would 'implicitly authenticate' the documents." (*Id.*, slip op. at 1 (quoting *In re Grand Jury Subpoena Duces Tecum* Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir.1993)).)

First, Brooks's attorney already admitted in front of the court and the government that the metadata existed and that the defense was in possession of it. Therefore, the government already knew of the metadata's existence and location. Second, implicit authentication does not occur unless the individual subpoenaed to turn over the documents complies with the subpoena and "thereby implicitly testifies that he owns or at least possesses the documents." (*United States v. Fox*, 721 F.2d 32, 38 (2d Cir. 1983).) Again, since Brooks's attorney already admitted to Brooks's owning the metadata, producing the metadata would not have any "testimonial quality." (*Hatfield*, No. 06-CR-0550, slip op. at 2.)

Conclusion

Due to the prevalence of location sharing and the widespread availability of location technologies, it is becoming increasingly easier to track users' whereabouts. Because many of these tracking technologies are simple to use and accessible online, law enforcement is no longer restricted to more expensive, specialized software. This has taken metadata forensics out of its niche and brought it into law enforcement's basic repertoire. With all of the different technologies allowing both law enforcement and the layperson access to location data, obtaining evidence has become easier and acquiring technological savvy has become simpler. ■

CRIMINAL JUSTICE EDITORIAL POLICY STATEMENT

Criminal Justice is a magazine for everyone who cares about the quality of our justice system. Its focus is on practice and policy. Our readers are private and public defense attorneys, prosecutors, judges, law professors, and others who recognize that society is itself ultimately judged by its system for judging others. The magazine is published by the Section of Criminal Justice of the American Bar Association with the assistance of ABA Publishing.

The membership of the Section is diverse. Some members preside over or practice in state courts, others primarily in federal courts. Some specialize in white collar crimes, others prosecute or defend street crimes, and still others specialize in juvenile cases. Articles in *Criminal Justice* thus cover a wide variety of subjects, addressing areas of importance to all segments of the Section.

Those who prosecute and defend, regardless of their level of experience, constantly seek information on how to enhance their practice skills. *Criminal Justice* is also a forum for airing significant issues of interest to everyone concerned with the administration of justice. Accordingly, critical policy questions and recent trends are routinely covered. In doing so, *Criminal Justice* does not avoid controversy or unpopular viewpoints. Although a serious journal, *Criminal Justice* aims to be lively, provocative, and always highly readable.

Readers are cordially invited to submit manuscripts and letters for publication. Final decisions concerning publication are made by the Editorial Board of *Criminal Justice*, but are not to be taken as expressions of official policy of the Section or the ABA unless so stated.

Ants Under the Refrigerator?



Removing Expunged Cases from Commercial Background Checks

BY SHARON M. DIETRICH

After years of avoiding getting into trouble again (or after having charges dropped), your client is thrilled to get a court order “clearing” a criminal case by expungement or sealing or whatever name your state uses. Newly confident, he or she applies for a job, an apartment, a place in a college class. But despite the court order, the expunged case comes to light in a background check, and the opportunity for work, a home, and an education is denied. Your client is back to square one.

Such individuals are not alone because removing a criminal case from the public records is no insurance that it has been removed from privately held databases that are used by commercial background checkers. As I advise clients, hopefully they will no longer be affected by the expunged case, but they should think of expungement like ants in their kitchen: you may think you’ve got them all only to later discover that one or two have escaped under the refrigerator. (See Joe Palazzolo & Gary Fields, *Fight Grows to Stop Expunged Criminal Records Living On in Background Checks*, WALL ST. J., May 7, 2015.)

Commercial background checks that report expunged cases thwart public policy, judicial orders, and an individual’s attempts to move forward. But it doesn’t have to be this way. In fact, when commercial background checkers report expunged cases, their conduct implicates the federal Fair Credit Reporting Act. (15 U.S.C. §§ 1681 *et seq.*) This article looks at why expungements are so important, why commercial background screeners sometimes report expunged cases, and how this problem can be corrected.

Expungements: A Critical Reentry Tool

About one in three Americans has a criminal record of some kind. (Jo Craven McGinty, *How Many Americans*

Have a Police Record? Probably More Than You Think, WALL ST. J., Aug. 7, 2015.) Coinciding with the increase in numbers of people with criminal records is a growth in background screening. Eighty-seven percent of employers, 80 percent of landlords, and 66 percent of colleges screen for criminal records. (Rebecca Vallas & Sharon Dietrich, *One Strike and You’re Out: How We Can Eliminate Barriers to Economic Security and Mobility for People with Criminal Records*, CENTER FOR AM. PROGRESS (Dec. 2, 2014), <http://tinyurl.com/p5nd95m>.) Because criminal records have constituted an increasingly serious barrier to these and many other critical needs of life, they have become a significant cause of poverty in this country. (*Id.*)

These civil consequences of criminal records are very keenly felt by the clients of civil legal aid programs. In the Community Legal Services Inc. program serving low-income Philadelphians, 941 of 1,389 new employment law clients in 2014—or 68 percent—sought help related to their criminal records, which was by far the most common single type of employment law service requested. Typically, the clients asked for representation in an “expungement” of their criminal records. They knew that eliminating a record that has been repeatedly hampering them is their best chance at moving forward in their lives.

The demand for expungements and other record-clearing remedies has been clearly heard by state policymakers nationwide, who have been willing to give former offenders a fresh start. Between 2009 and 2014, at least 23 states, as diverse as Mississippi, Indiana, and California, expanded their expungement or sealing laws. (Ram Subramanian, Rebecca Moreno & Sophia Gebreselassie, *Relief in Sight? States Rethink the Collateral Consequences of Criminal Conviction, 2009–2014*, VERA INST. FOR JUST. (Dec. 22,

2014), <http://tinyurl.com/oxksywx>.) The trend is to permit even convictions—felonies as well as misdemeanors—to be expunged after a period of desistance from crime.

These expanded record-clearing laws are consistent with the findings of relatively new criminology research into “redemption”—the point at which a former offender is no more likely than a member of the general population to commit a crime. This research finds that recidivism risk declines steadily with time free from reoffending, and that a criminal record does not predict future criminality after three to four years for a single conviction, and 10 years for multiple convictions. (Alfred Blumstein & Kiminori Nakamura, *Redemption in the Presence of Widespread Criminal Background Checks*, 47 *CRIMINOLOGY* 327, 331 (2009).)

Expanded state expungement laws, therefore, serve the strong public policy purpose of eliminating collateral consequences for people who no longer present heightened risk of crime. Unlike “ban the box” and other laws that maintain criminal records but ask that they be considered fairly, expungement laws do not require employers and others obtaining background checks to follow the law; instead, the case is not presented for consideration at all. This remedy is not only popular with people with criminal records; in my experience, countless employers tell people that they will consider the candidate if a case has been expunged. And perhaps best of all, the elimination of a criminal case from the public records is a way to broadly address collateral consequences, not just a single type such as employment. Simply put, record clearing is one of the best tools in the growing fight to return people with criminal records into the mainstream in this country. (See Jenny Roberts, *Expunging America’s Rap Sheet in the Information Age*, 2015 *WIS. LAW R.* 321, available at <http://tinyurl.com/qg4nkwx>.)

The next wave in expanded record-clearing remedies is a concept known as “Clean Slate.” This model statute would provide for the sealing of misdemeanor convictions after 10 years for an individual without another felony or misdemeanor conviction. Infractions would be sealed after five years, and nonconvictions shortly after the disposition becomes final. The key to the Clean Slate concept, though, is that the sealing would be done automatically, without the filing, adjudication, and implementation of many thousands of petitions for all eligible persons. This automatic implementation is the innovative path that will make clearing a criminal case a reality for large numbers of people. No longer will qualified individuals need to obtain a lawyer to file and then wait for court consideration and implementation; indeed, they need not even be cognizant of the right to having their record cleared. And resources are saved for

courts, district attorneys, and law enforcement staff who no longer will need to handle the ever-increasing numbers of petitions. (Vallas & Dietrich, *supra*.)

But despite this encouraging trend, a major stumbling block remains. Simply put, no one can assure a client that an expunged case will never reappear—even when public record keepers, such as the courts and the central repository (often the state police), have removed it. Any one of the hundreds of commercial background screeners may still report the case. Hence my advice to clients: Always be on alert for those stray ants under the refrigerator. The key for both policymakers and individuals is to identify available methods to root out these cases from the private databases, as well as public ones.

Background Screeners’ Reporting of Expunged Cases

While criminal justice professionals are accustomed to working with public sources of criminal records, the same is not true for most civil users. Theoretically, employers, landlords, and others can check the large number of court websites that make criminal case information readily available for free, but generally they do not. Unless required by law, they tend not to obtain criminal records from their state’s central repository, nor do they typically “Google” the individuals they are screening. Because they are not experts in criminal law, civil users choose to buy reports from commercial background screeners. Such services provide a broad check prepared by professionals with criminal record expertise that they can comfortably rely upon when deciding whether to exclude someone as a risk based on his or her criminal history.

Although relatively little information is publicly available about the commercial background screening industry, it is known to be huge and growing. The industry’s revenues were recently estimated at \$2 billion. (*Background Check Services in the US: Market Research Report*, IBIS-WORLD (Aug. 2015), <http://tinyurl.com/pt5ralk>.) The three largest providers (First Advantage, SterlingBackCheck, and HireRight) alone produced 56 million background checks in a recent 12-month period. (Max Mihelich, *Special Report: More “Background” Noise*, *WORKFORCE* (Sept. 5, 2014), <http://tinyurl.com/ppjguac>.) Unlike the credit reporting industry, with its three companies, the criminal record screening industry includes hundreds of companies, many of them small. The industry is virtually unmapped, and a potential employer could buy a background check on a job applicant from any of these hundreds of companies.

Commercial background checkers almost never begin a report by directly checking public data, such as court records. Instead, virtually every commercial background screener begins by running a query of a database maintained by one of a handful of middlemen that obtain data in bulk directly from public sources, usually the courts. If there is no match between the person whose record is being checked and the database, the report indicates that the person has no criminal cases.

SHARON M. DIETRICH is the litigation director of Community Legal Services Inc., the civil legal aid program serving the employment law needs of low-income Philadelphians. She can be contacted at sdietrich@clsphila.org. This article is based on an article published on the website povertylaw.org, April 14, 2015, by the Sargent Shriver National Center on Poverty Law.

But what happens once there appears to be a “hit” depends on the commercial screener preparing the report. Many companies, especially the larger ones, conduct little verification of that match before issuing a background check reporting the case. Others view the database as a “pointer file,” a starting point rather than the end. They verify the results against courthouse records, often sending court runners to review files. About 200 of these companies have signed on as members of a loose affiliation called “Concerned CRAs” (consumer reporting agencies), certifying that they verify the results of a database search before reporting a case (www.concernedcras.org). This verification has critical implications for removing cases that may still be in the privately held database but that have been removed from public records because of expungement.

At this point, it is well accepted that commercial background screeners are “consumer reporting agencies” within the meaning of the Fair Credit Reporting Act (FCRA). Two accuracy-related provisions of that statute are implicated by the reporting of expunged cases. First, consumer reporting agencies must “follow reasonable procedures to assure maximum possible accuracy.” (15 U.S.C. § 1681e(b).) Second, in the employment context, unless a consumer reporting agency provides contemporaneous notice to the person being screened that it is providing a background check to the employer, it must use “strict procedures” to ensure that the information is “complete and up to date.” (15 U.S.C. § 1681k.) There are no regulations interpreting these broad terms. However, the background screening industry is regulated by two federal agencies, the Federal Trade Commission (FTC) and the relatively new Consumer Financial Protection Bureau (CFPB).

Despite the commands of the FCRA and the federal oversight, many commercial background reports are far from accurate, presenting a host of problems. (See PERSIS S. YU & SHARON M. DIETRICH, NAT’L CONSUMER LAW CTR., *BROKEN RECORDS: HOW ERRORS BY CRIMINAL BACKGROUND CHECKING COMPANIES HARM WORKERS AND BUSINESSES* (2012), <http://tinyurl.com/c6pjac6>.) One of the most notable, and prejudicial, accuracy issues is the reporting of expunged or sealed cases. Some delay for commercial databases to remove expunged cases is understandable; it takes some time for them to learn of the expungement and eliminate the case. But expunged cases are often reported long after they have been removed from public records. In one instance, the expunged case was reported by a national screening company 20 months after it had been removed by the Pennsylvania courts from their publicly available website.

There are numerous reasons that commercial background screeners sometimes report expunged cases. From a technical perspective, when databases are updated, the combination of new and old data may not reveal the absence, because of expungement, of a case that previously was reported. This technical flaw is exacerbated by many companies having no procedure whatsoever to learn of expunged cases, short of waiting to hear from a wronged subject of a background check through an internal “dispute” procedure required by the FCRA that a case had been expunged. Because many do not

verify database hits (and discover that expunged cases no longer exist in public records), expunged cases will be reported.

The failure of many commercial background checkers to employ any mechanism to identify and remove expunged cases appears on its face to contravene the FCRA’s accuracy provisions. At least five class actions have challenged this error as a violation of the FCRA. All but one settled, with practice changes, and the remaining case is still pending. (See *FCRA Class Actions*.)

Avoid Reporting Expunged or Sealed Cases

Fortunately, there are steps that can be taken to protect persons whose cases have been expunged from having the cases reappear in commercial background checks. Some of these steps can be taken by and for individuals; others, by courts seeking to ensure that their expungement orders are enforced or by policymakers looking to protect their expungement initiatives.

Warn clients they may see expunged or sealed cases again. Give them the example of the ants that escape under the refrigerator. Help them understand that criminal case data goes into many databases, and rooting it all out may be a challenge. Encourage your clients to keep copies of their expungement orders in a safe place (in case they need them later to prove that the cases were expunged) and to contact you for follow up if an expunged case reemerges.

Take steps to remove clients’ expunged or sealed cases from commercial databases. You can try (or recommend that your clients try) to register an expungement with the Expungement Clearinghouse (www.expungementclearinghouse.org). This clearinghouse collects and transmits expungement orders to its members in the background screening industry for free. Beware of a competitor of this website that charges for the same service. The Foundation for Continuing Justice, which operates the clearinghouse, indicates that its updates reach 500 background screening companies. Alternatively, you can send the expungement orders to the dominant companies in the industry or ask for a “full file disclosure” to determine whether your client’s expunged cases are still in their databases. A list of these larger companies may include ADP, Backgroundchecks.com, EmployeeScreenIQ, First Advantage, General Information Services, HireRight, Kroll Background America, IntelliCorp, and SterlingBackCheck.

Similar to the better-known right to a “free credit report,” people have the right to see their “specialty credit reports,” such as criminal background checks. (Dan Rutherford, *You Have a Right to See Specialty Consumer Reports Too*, CFPB (Nov. 29, 2012), <http://tinyurl.com/bp6ytnu>.) To try to obtain data that is in a database but may not yet have been reported to an employer or other customer, be sure to request the “file” rather than the “reports” made by the screener. The CFPB offers a list of contacts. (See CFPB, *LIST OF CONSUMER REPORTING AGENCIES* (2015), <http://tinyurl.com/7cyz8jw>.) If the expunged cases are still reported, the client should file a “dispute” in response to the disclosure and submit a copy of the expungement order; doing so is likely to result in the case

being removed. Such disputes are much better done in the full file-disclosure process, rather than after an employer gets an erroneous report that may cost the client a job.

Public sellers of bulk data should provide lists of expunged cases to the industry. The Administrative Office of Pennsylvania Courts (AOPC) has devised an elegantly simple solution to the problem of commercial background screeners that have not removed expunged cases from their databases. After fielding phone calls from Pennsylvanians complaining that their expunged cases were showing up in background checks, AOPC created a data file provided on a monthly basis that it calls a “LifeCycle file,” which lists expunged cases to be removed from private databases. AOPC contractually requires that this file be used by bulk purchasers of their data and any and all downstream users to remove expunged cases.

This LifeCycle file has not eliminated the problem in its entirety in Pennsylvania, as some in the industry have not used it or applied it properly. However, when faced with class action litigation, these companies have quickly rectified their practices. And certainly Pennsylvanians with expungements have much greater expectations that their expunged cases will be removed than people in states without such an innovation. Yet, Pennsylvania is virtually alone in providing the industry with affirmative notice of cases that should no longer be reported.

All bulk sellers of criminal record data to the background screening industry (often the administrative offices of state courts) should develop a procedure similar to the Pennsylvania courts’ LifeCycle file that specifically identifies expunged or sealed cases that should be removed from privately held data. The data purchasers and their downstream users should be required to use this list to remove expunged cases as a term of the purchase agreement. The seller should periodically audit the bulk purchasers to ensure that the file is being used and should check on any complaints that indicate that the file is not being used. AOPC can be contacted for more information about the Pennsylvania courts’ LifeCycle file.

Make complaints to the CFPB or the FTC. Both the CFPB (<http://tinyurl.com/7ljv2tl>) and the FTC (<http://tinyurl.com/nptahxp>) provide an online complaint mechanism for the industries that they regulate. The filing of a complaint to the CFPB results in an interaction between the client and the screener that is brokered by the agency and that could resolve a background check issue not remediated in a dispute. Moreover, the federal agencies track patterns identified by complaints that may result in enforcement action against background screeners with substandard practices. Recently, the CFPB obtained a notable consent order from General Information Services and e-Backgroundchecks.com, two of the largest background screeners, requiring improvements to their screening practices. The order included a requirement that the screeners use proprietary software in their possession to identify and remove expunged cases. (USA, CFPB, Admin. Proceedings File No. 2015-CFPB-0028 (Oct. 29, 2015), at 6–7, 12, <http://tinyurl.com/nczpjqu>.)

FCRA Class Actions

Reporting of expunged cases was challenged in at least five class actions brought under the Fair Credit Reporting Act:

- *Henderson v. HireRight Solutions, Inc.*, No. 10-459 (E.D. Pa. 2010).
- *Robinson v. General Information Services, Inc.*, No. 11-7782 (E.D. Pa. 2011).
- *Roe v. Intellicorp Records, Inc.*, No. 1:12-cv-2288 (N.D. Ohio 2012).
- *Giddiens v. LexisNexis Risk Solutions, Inc.*, No. 2:12-cv-02624-LDD (E.D. Pa. 2012).
- *Stokes v. RealPage, Inc.*, No. 2:15-cv-01520-JP (E.D. Pa. 2015).

The first four of these cases were settled; the fifth remains in active litigation. The settlements in these cases typically discontinued the use of stale data or required the screener to change its practice to verify data.

Pursue litigation under the FCRA. This approach should bring relief for a client who has sustained lost wages or other damages because of the reporting of an expunged or sealed case. Individual cases are not overly complicated and have some deterrent effect if the client recovers a monetary award. Practice changes by the screener are not likely to be obtained in response to an individual case, although one would like to think that having been put on notice of a deficiency by the lawsuit would prompt a background screener to examine its practices. At the least, individual cases will set up a “willfulness” claim for compensatory and punitive damages if there is a subsequent class action for this practice.

Practice changes regularly are negotiated as a component of settlements of FCRA class actions, even though most circuits have ruled that private parties cannot obtain injunctions under the statute. Moreover, the likely monetary damages in a class action should be a deterrent.

Encourage purchasers to use background screeners that verify their data. Employers and other purchasers of background checks often express exasperation that the reports provided by their screeners are not accurate. The answer? Get a better screener! By pledging to verify the results of a database query, the members of Concerned CRAs deserve consideration. When a commercial screener verifies potential “hits” at the courthouse before reporting them to a purchaser, expunged cases are not likely to be reported. (See Thomas Ahearn, *Expunged Criminal Records Appearing in Background Checks Unnecessarily*, EMP. SCREENING RESOURCES (May 7, 2015), <http://tinyurl.com/o674t6t>.)

Conclusion

When commercial background checks report criminal cases that have long been expunged, a great deal of frustration ensues. Policymakers are frustrated that their efforts to expand expungement have been thwarted. Courts

(continued on page 54)

Residential Drug Abuse Treatment Program (RDAP)

BY ALAN ELLIS AND TODD A. BUSSERT

The Federal Bureau of Prisons (BOP) estimates that 40 percent of federal inmates have diagnosable, moderate to severe substance abuse problems. The BOP operates three drug abuse programs. The first program is the 12- to 15-hour voluntary Drug Abuse Education Course offered at all institutions, designed to teach inmates about the consequences of drug/alcohol abuse and addiction by reviewing their personal drug use and the cycle of drug use and crime. The second program is the 12- to 24-week (90–120 minutes per week) Non-Residential Drug Abuse Treatment Program (NRDAP), which is targeted to, *inter alia*, those awaiting RDAP, those who do not meet RDAP admission criteria, and those found guilty of an incident report for use of drugs or alcohol. In addition to paying NRDAP graduates \$30, BOP policy encourages wardens to consider them for maximum pre-release (halfway house and/or home confinement) placement. The third program is the nine-plus-month, 500-hour Residential Drug Abuse Treatment Program (RDAP) for inmates with a diagnosable and verifiable substance abuse disorder.

RDAP has been in existence since 1989 and employs cognitive behavioral therapy (CBT) to treat substance abuse. The “in-patient” component is followed by an aftercare component, which is administered in the community during the final six months of an inmate’s sentence. Male inmates who successfully complete RDAP are 16 percent less likely to be rearrested or revoked than cohorts who went untreated, and 15 percent less likely to use drugs. Female graduates are 18 percent less likely to reoffend or use drugs.

Through the 1994 Crime Bill, Congress also

incentivized RDAP participation: *nonviolent* offenders who successfully complete the program while incarcerated (and who have not previously received early release via RDAP) are eligible for release up to one year before the expiration of their sentence. (18 U.S.C. § 3621(e).) Importantly, prisoners ineligible for a reduction in sentence under § 3621(e) are not precluded from participating in RDAP; the two are not mutually exclusive.

Congress’s action had its desired result, especially since RDAP is the only BOP program through which federal prisoners can earn a sentence reduction.

Admission to RDAP

RDAP participation is voluntary. Interested prisoners within 36 months of release may apply by requesting an eligibility interview via a “cop-out” (informal request from a staff member) or a BP-8 (formal request for resolution). The written request serves to initiate the RDAP application and should prompt an interview with either the institution’s RDAP coordinator or a drug treatment specialist (DTS), or, if a prisoner is housed at a facility that does not offer the RDAP, a member of the psychology services staff.

To qualify for RDAP, one must, *inter alia*, have at least 24 months or more remaining to serve; present a verifiable, documented pattern of substance abuse or dependence within the 12-month period preceding arrest on the underlying offense; have no serious mental or cognitive impairment precluding full program participation; be halfway house eligible (which precludes participation by removable non-US citizens); and sign an acknowledgment of program responsibilities.

Section 3621 is silent with respect to how determinations about whether a prisoner has “a substance abuse problem” are made. And, while 28 C.F.R. § 550.53(b) establishes criteria, in practice Program Statement 5330.11 controls. (*See* FED. BUREAU OF PRISONS, P5330.11, U.S. DEP’T OF JUSTICE, PSYCHOLOGY TREATMENT PROGRAMS (2009) [hereinafter P.S. 5330.11].) Staff review each program applicant’s presentence investigation report (PSR) before scheduling an interview to ascertain whether the applicant meets the diagnostic criteria for abuse or dependence indicated in the *Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition (DSM-V)*. An RDAP applicant’s chemical dependency need not be linked to his or her offense conduct, nor is a judicial recommendation necessary. There is, however, debate over how much drug or alcohol use is enough. (*Compare* P.S. 5330.11, § 2.5.8(2) (noting that “recreational, social, or occasional use of alcohol and/or other drugs that does not rise to the level of excessive or abusive drinking does not provide the required verification of a substance abuse disorder”), *with* *Kuna v. Daniels*, 234 F. Supp. 2d 1168 (D. Or. 2002) (finding social use of alcohol sufficient



ALAN ELLIS is a regular columnist for *Criminal Justice* magazine and past president of the NACDL. He practices in the areas of federal sentencing, prison matters, postconviction remedies, and international criminal law, with offices in San Francisco and New York. Contact him at AELaw1@alanellis.com or go to www.alanellis.com.



TODD A. BUSSERT is a member of Frost Bussert LLC in New Haven, Connecticut. He is of counsel to the Law Offices of Alan Ellis and author of the Federal Prison & Post Conviction Blog (<http://thebopblog.blogspot.com>).

to warrant RDAP admission).)

In terms of assessing a prisoner's substance abuse history, the BOP places primary reliance on a prisoner's self-reporting to the PSR writer. Whatever is written in the PSR is presumptively valid, and any claim of a disorder that the PSR does not plainly substantiate is treated as suspect. Counsel must, therefore, be attuned to a client's substance abuse history. Counsel should meet with the client before the presentence interview to fully understand the nature and extent of the client's problem(s) (e.g., illegal drugs, prescribed pharmaceuticals, alcohol, etc.). Prudence also dictates that counsel encourage clients to be fully forthcoming with the PSR writer, that is, not to minimize for fear of embarrassment. Subject to client preapproval, counsel can foster this conversation by offering the PSR writer an overview during the interview, allowing the writer to follow up directly with the client as deemed appropriate. Counsel can also provide documentation (e.g., medical records and clinical assessments) from an independent professional (e.g., physician, mental health professional, or drug and alcohol counselor) concerning the existence and degree of a client's dependence. Barring that, it is useful to find records that demonstrate the nature and extent of the client's substance abuse difficulties, such as certified copies of DUI judgments, hospital records noting blood alcohol level, and/or a primary physician's treatment notes with entries that substantiate the existence of the problem.

Given the § 3621(e) incentive, and to ferret out malingering, RDAP eligibility interviews often entail difficult questions designed to determine whether admission is sought in good faith to obtain treatment or simply to secure a quicker return home. Applicants are routinely asked when they learned about the program and the § 3621(e) credit, whether attorneys advised them to exaggerate treatment needs when meeting with probation, and the details of their drug or alcohol use (e.g., when, how often, where, with whom, others' awareness, etc.). Counsel should thus advise clients not to mangle or to overstate their problems, either during the presentence interview or when seeking entrance into the program.

Should the BOP deem a PSR factually insufficient, an inmate might well be refused an interview or found ineligible for services. In that instance, counsel and/or the client may supply "collateral documentation." As set forth in P.S. 5330.11, this requires documentation "from a substance abuse treatment provider or medical provider who diagnosed and treated the inmate for a substance abuse disorder *within the 12-month period before the inmate's arrest on his or her current offense*" (emphasis added). This documentation must be sent to and received by the drug abuse treatment staff in the BOP institution. It is not to be given to

INELIGIBILITY FOR EARLY RELEASE

1. Inmates who have a prior felony or misdemeanor conviction for:
 - homicide (including deaths caused by recklessness, but not including deaths caused by negligence or justifiable homicide);
 - forcible rape;
 - robbery;
 - aggravated assault;
 - arson;
 - kidnapping; or
 - an offense that by its nature or conduct involves sexual abuse offenses committed upon minors.
2. Inmates who have a current felony conviction for:
 - an offense that has as an element the actual, attempted, or threatened use of physical force against the person or property of another;
 - an offense that involved the carrying, possession, or use of a firearm or other dangerous weapon or explosives (including any explosive material or explosive device);
 - an offense that by its nature or conduct presents a serious potential risk of physical force against the person or property of another; or
 - an offense that by its nature or conduct involves sexual abuse offense committed upon minors.
3. Inmates who have been convicted of an attempt, conspiracy, or other offense that involved an underlying offense listed in 1. and/or 2. above.
4. Inmates who previously received an early release under 18 U.S.C. § 3621.

Certain sex offenders, in particular individuals convicted of possession of child pornography, are *not* automatically disqualified from § 3621(e) eligibility.

Amount of Reduction

The BOP has implemented a sliding scale for the amount of a sentence reduction: those serving 30 months or less are ineligible for more than a six-month reduction; those serving 31 to 36 months are ineligible for more than a nine-month reduction; and those serving 37 months or longer are eligible for the full 12 months. (See P.S. 5331.02, § 10.)

RESIDENTIAL DRUG ABUSE TREATMENT PROGRAM LOCATIONS

RDAP is available at the following facilities:

Northeast Region

FCI Allenwood-Low (PA)
FCI Allenwood-Medium (PA)
FCI Berlin (NH)
USP Canaan (PA)
FCI Danbury (CT)*
FCI Elkton (OH)
FCI Fairton (NJ)
FCI Fort Dix 1 (NJ)
FCI Fort Dix 2 (NJ)
FPC Lewisburg (PA)
FPC McKean (PA)
FCI Schuylkill (PA)

North Central Region

FPC Duluth (MN)
FCI Englewood (CO)
FCI Florence (CO)
FPC Florence (CO)
FPC Greenville (IL)*
FPC Leavenworth (KS)
USP Leavenworth (KS)
USP Marion (IL)
FCI Milan (MI)
FCI Oxford (WI)
FPC Pekin (IL)
FCI Sandstone (MN)
MCFP Springfield (MO)
FCI Terre Haute (IN)

FCI Waseca (MN)*
FPC Yankton (SD)

Southeast Region

FCI Coleman (FL)
USP Coleman II (FL)
FPC Edgefield (SC)
FCI Jesup (GA)
FCI Marianna (FL)
FPC Miami (FL)
FCI Miami (FL)
FPC Montgomery (AL)
FPC Pensacola (FL)
FCI Talladega (AL)
FCI Tallahassee (FL)*
FCI Yazoo City (MS)

Mid-Atlantic Region

FPC Alderson (WV)*
FCI Beckley (WV)
FPC Beckley (WV)
USP Big Sandy (KY)
FCI Butner (NC)
FCI Cumberland (MD)
FPC Cumberland (MD)
SFF Hazelton (WV)*
FMC Lexington (KY)
FCI Memphis (TN)
FCI Morgantown (WV)
FCI Petersburg-Low (VA)
FCI Petersburg-Medium (VA)

South Central Region

FCI Bastrop (TX)
FCI Beaumont-Low (TX)
FCI Beaumont-Medium (TX)
FPC Beaumont (TX)
USP Beaumont (TX)
FPC Bryan (TX)*
FMC Carswell (TX)*
FCI El Reno (OK)
FCI Forrest City-Low (AK)
FCI Forrest City-Medium (AK)
FCI Fort Worth (TX)
FCI La Tuna (TX)
FCI Seagoville (TX)
FPC Texarkana (TX)

Western Region

FCI Dublin (CA)*
FPC Dublin (CA)*
FCI Herlong (CA)
FPC Lompoc (CA)
FCI Phoenix (AZ)
FPC Phoenix (AZ)*
FCI Safford (AZ)
FCI Sheridan (OR)
FPC Sheridan (OR)
FCI Terminal Island (CA)

Contract Facility

RCI Rivers (NC)

KEY

FCI = Federal Correctional Institution
FMC = Federal Medical Center
FPC = Federal Prison Camp
MCFP = Medical Center for Federal Prisoners

USP = United States Penitentiary
RCI = Rivers Correctional Institution
SFF = Secure Female Facility
* = Female Facility

the inmate to provide to the drug abuse treatment staff. If the document is acceptable, the inmate will be referred to the Drug Abuse Program coordinator for a diagnostic interview. Multiple convictions (two or more) for driving under the influence (DUI) or driving while intoxicated (DWI) in the five years prior to the most recent arrest will suffice to show eligibility for the RDAP program.

Program Statement 5330.11 directs that otherwise eligible prisoners must “ordinarily” be within 24 months of release to qualify for admittance to RDAP. Accounting for customary good time credits, the 24-month cutoff means that a defendant with a diagnosable disorder and no pretrial jail credit must receive a sentence of 27.6

months or greater to even be considered for the program. Notably, BOP officials have stated publicly that the 24-month cutoff has shifted to 27 months, which means a sentence of at least 31 months (if the prisoner is ineligible for pretrial jail credit).

Ineligibility for RDAP

The following categories of inmates are not eligible for the RDAP program:

1. Immigration and Customs Enforcement detainees;
2. pretrial inmates;
3. contractual boarders (for example, state or military inmates); and

4. inmates with detainers that preclude halfway house placement.

The Sentence Reduction

The determination as to whether an inmate is ineligible for early release has been the subject of significant controversy. After much litigation, the BOP modified the criteria for eligibility for early release from a sentence for successful completion of RDAP. (See 28 C.F.R. § 550.55; FED. BUREAU OF PRISONS, U.S. DEP'T OF JUSTICE, P5331.02 (a pending revision to 28 C.F.R. § 550.55 will liberalize criteria for a §3621(e) reduction), EARLY RELEASE PROCEDURES UNDER 18 U.S.C. § 3621(E) (2009) [hereinafter P.S. 5331.02]; FED. BUREAU OF PRISONS, U.S. DEP'T OF JUSTICE, P5162.05, CATEGORIZATION OF OFFENSES (2009) [hereinafter P.S. 5162.05].) This change was intended to exclude violent offenders by the exercise of the implicit discretion placed in the BOP by the statute, 18 U.S.C. § 3621(e)(2)(B), rather than by definition of the statutory language "nonviolent offense." The authority for determining whether prior offense history or current offense characteristics preclude § 3621(e) credit has been moved to the BOP's Designation and Sentence Computation Center (DSCC) in Grand Prairie, Texas.

BOP policy, which the US Supreme Court has upheld, denies early release to persons who have been convicted of a crime of violence—homicide, forcible rape, robbery, aggravated assault, child sexual offense (but *not* possession of child pornography), arson, or kidnapping—or a felony offense (1) that has as an element the actual, attempted, or threatened use of physical force against the person or property of another; (2) that involved the carrying, possession, or use of a firearm or other dangerous weapon or explosives (including any explosive material or explosive device); (3) that by its nature or conduct presents a serious potential risk of physical force against the person or property of another; or (4) that by its nature or conduct involves sexual abuse offenses committed upon children. Inmates with firearm convictions and inmates who have received a two-level adjustment in their drug guideline offense severity score for possession of a dangerous weapon (including a firearm) pursuant to US Sentencing Guidelines Manual Section 2D1.1(b) (1) are also ineligible for early release. For information on the specific crimes that would preclude an inmate from an early release, see P.S. 5162.05. ■

CHAIR'S COUNSEL (continued from page 1)

her kids, could not afford bail for charges that were subsequently dropped. (Shaila Dewan, *The Collateral Victims of Criminal Justice*, N.Y. TIMES, Sept. 5, 2015, <http://tinyurl.com/pxp5kx6>.) Zachery Anderson, a 19-year-old, had consensual sex with a girl he met on a dating app, who claimed to be 17 but was actually 14. (Julie Bosman, *Teenager's Jailing Brings a Call to Fix Sex Offender Registries*, N.Y. TIMES, July 4, 2015, <http://tinyurl.com/pujhd7a>.) Zachery was sentenced to jail and now must register as a sex offender. He must submit to random searches of his home and belongings; he cannot reside near schools, parks, and other public places; and he must refrain from engaging in activities frequented by children. He also cannot access the Internet while on probation, which means that the computer science degree he was earning from a local community college will be put on hold.

Researchers are also concerned about the impact of collateral consequences on communities. They compare the effects of incarceration and collateral consequences to a patulous contagion. (Emily von Hoffmann, *How Incarceration Infects a Community*, ATLANTIC (Mar. 6, 2015), <http://tinyurl.com/mvk68al>.) Neighborhoods become infected by the incarcerated and become magnet communities. These communities often are places that are high density, high poverty, levels of high violence, and experience lower levels of social services.

The infected are handicapped due to collateral consequences, usually an inability to find employment and affordable housing. Children from infected families often have shorter life spans, and they eventually continue the epidemic and become incarcerated themselves. The serious social and health consequences of incarceration and collateral consequences necessitate consideration and awareness of how they affect the millions of individuals like Maurice, Markeisha, and Zachery, as well as local communities.

The breadth of the types of collateral consequences is as immense as the depth of their far-reaching effects. Individuals with criminal convictions often have difficulty gaining employment, getting job training, obtaining educational benefits, or receiving health benefits. They are often disqualified from receiving federal housing assistance, student loans, and other public benefits. Their parental rights may be affected, or they may be subject to deportation. They may not vote, hold public office, or serve on a jury. These extensive collateral consequences disproportionately affect the poor and minorities, entrenching them in a cycle of poverty, instability, and incarceration and often imposing a badge of inferiority.

Certain collateral consequences of criminal convictions are, of course, justified by various concerns for public safety or as a consequence of the loss of public trust. For example, courts have justifiably and

historically upheld laws denying felons the right to own or possess a firearm under the Second Amendment. (*See* *District of Columbia v. Heller*, 554 U.S. 570, 626 (2008) (acknowledging “longstanding prohibitions on the possession of firearms by felons”).) These valid restrictions are not the issue here. Instead, understanding the individual and societal impact of prevalent consequences is essential. Now, more than ever before, collateral consequences are increasingly numerous and severe. They affect more individuals than ever before, and there are few methods for relief. Furthermore, because multiple sources promulgate the restrictions, policymakers and criminal justice stakeholders are often left without a full picture of the net effects of collateral consequences.

The ABA and the Criminal Justice Section have confronted these somber facts and difficult problems head on. The National Inventory of the Collateral Consequences of Conviction (NICCC) (www.abacollateralconsequences.org) has organized over 47,000 collateral consequences. It compiles collateral consequences from the federal level, the state level, territorial statutes, regulations, and rules. This free and searchable database provides a crucial and useful tool for individual states and organizations to analyze the cumulative effect of disjointedly implemented collateral consequences. It is an informational stepping stone to ensuring that the collateral effects of incarceration are limited to those deemed necessary by society without causing undue harm.

Ensuring that the collateral consequences of criminal conviction are appropriately limited requires both education and engagement by the many stakeholders in the criminal justice system. While the Supreme Court has acknowledged the existence of collateral consequences, it has yet to distinguish between what is a collateral consequence and what is a direct and necessary consequence of incarceration. (*See* *Chidez v. United States*, 133 S. Ct. 1103, 1111–12 (2013) (noting that the Supreme Court avoided this question in *Padilla v. Kentucky*, 559 U.S. 356 (2010)).) Still, the Supreme Court found that an individual has the right to be advised of when a criminal proceeding may subject her to deportation because it is a uniquely harsh punishment. (*Padilla*, 559 U.S. at 369.) Which other collateral consequences fall into this category has yet to be determined. With an estimated 65 million people in the United States having some type of criminal record, failing to address the problem is not an option.

Even though this issue has not been fully fleshed out in the courts, the NICCC is an important informational tool for parties, lawmakers, policymakers, and courts. For example, the NICCC can aid the parties and the court during plea bargaining by helping the defendant understand the full ramifications of a guilty plea or a criminal conviction. Prosecutors can evaluate collateral consequences when deciding

how to charge. Defense attorneys can utilize collateral consequences to help explain the full impact of a criminal case resolution. Judges can search the database to broaden their understanding of the ramifications of pleading guilty as well and fully advise criminal defendants of the short and long term effects of their disposition option.

State and federal legislators must be aware of the complications of applying so many collateral consequences to criminal convictions. For example, a search of the NICCC indicates that over 75 percent of collateral consequences at the state level are related to employment. (NICCC, www.abacollateralconsequences.org/search/ (limiting a search of all 50 states to categories for “employment,” “occupational and professional license and certification,” “business license and other property rights,” and “government contracting and program participation”) (last visited Nov. 25, 2015).) While some of these restrictions may be necessary, it is also important to recognize that employment is a leading factor in reducing recidivism. (Steven D. Bell, *The Long Shadow: Decreasing Barriers to Employment, Housing, and Civic Participation for People with Criminal Records Will Improve Public Safety and Strengthen the Economy*, 42 W. ST. U. L. REV. 1, 10–11 (2014).) The NICCC allows states to identify which collateral consequences affect their constituents and target legislation to ameliorate any particularly harsh effects. It is an asset that should be utilized by legislators and policymakers alike.

In *The New Jim Crow*, Michelle Alexander states, “As a society, our decision to heap shame and contempt upon those who struggle and fail in a system designed to keep them locked up and locked out says far more about ourselves than it does about them.” I implore this Section and other ABA leaders, state and federal legislators, prosecution and defense attorneys, judges, policymakers, and other criminal justice stakeholders and community members to study collateral consequences and their effects on individuals and communities. The NICCC is an effective and advantageous tool that should be used by diverse groups within the criminal justice community to analyze these critical concerns. The literature addressing collateral consequences demonstrates the seriousness of this issue and how important it is that our Section continues to bring this issue to the forefront of the nation’s awareness. As Chair, I am honored by the dedication, passion, and commitment of our CJS members—prosecutors, defense attorneys, judges, academics, government lawyers, and students—to the cause of justice through information, advocacy, and action! I leave you with the words of Anne Frank: “How wonderful it is that nobody need wait a single moment before starting to improve the world!” ■

Rule 413 and Charged Propensity Evidence

BY STEPHEN A. SALTZBURG

Federal Rule of Evidence 413 was adopted by Act of Congress in 1995. Unlike Rule 404(b), which generally prohibits the use of uncharged misconduct evidence to prove propensity, Rule 413 provides that evidence of other sexual assaults is admissible to prove propensity in a sexual assault prosecution. The relevant portion of the rule is:

Rule 413. Similar Crimes in Sexual-Assault Cases
(a) Permitted Uses. In a criminal case in which a defendant is accused of a sexual assault, the court may admit evidence that the defendant committed any other sexual assault. The evidence may be considered on any matter to which it is relevant.

The language “any matter to which it is relevant” is intended to open the door to propensity use of sexual assault evidence. Because the rule was not drafted by the Advisory Committee on the Federal Rules of Evidence, there is no Advisory Committee Note explaining the purpose of the rule. But it is evident that Congress believed that propensity evidence was more probative in sexual assault cases and in child molestation (Rule 414) cases than in other criminal cases.

A Typical Case

The typical case in which Rule 413 applies is one in which the defendant is charged with a sexual assault and evidence of other uncharged assaultive conduct is offered to prove that the defendant is the kind of person who commits sexual assaults. The standard is that there must be sufficient evidence of the uncharged misconduct for a jury to find by a preponderance of the evidence that the misconduct occurred. (*Huddleston v. United States*, 485 U.S. 681 (1988).) The trial judge upon request from

the defense will conduct Rule 403 balancing before admitting the uncharged misconduct evidence.

Charged Propensity Evidence: A Sample Case

The case of *United States v. Barnes*, 74 M.J. 692 (Army Ct. Crim. App. 2015), dealt with a different issue: namely, what instruction the judge should give the jury when more than one sexual assault is charged against a defendant. Barnes was charged with raping two separate victims—one in 2006 and one in 2009. During a hearing on pretrial motions, the military judge and parties discussed the application of Military Rule of Evidence 413 to two issues. The first issue was a defense motion to exclude evidence of uncharged misconduct concerning a sexual assault offense that Barnes allegedly committed as a juvenile. The military judge ruled that the alleged juvenile misconduct was irrelevant unless the defense opened the door by presenting a claim that Barnes “had never been accused of such crimes before.” The second issue involved the possibility raised by the government that it might argue “propensity” during closing argument based solely on the two charged acts of misconduct. A decision by the judge as to whether this would be permissible was reserved for later in the case.

The 2006 incident. The first rape charge was that Barnes, while on temporary duty for training at Fort Huachuca, Arizona, invited a fellow soldier, KAS, and her female friend back to his hotel room after a night of drinking and raped KAS. The female soldiers went to sleep in the living room of Barnes’s hotel suite on a pull-out sofa while Barnes went to bed in a separate room with its own door. The government alleged that KAS woke up during the night when she felt a sharp pain caused by an unlubricated attempt at sexual intercourse, pushed the person off her, and told him to stop. He stopped, she went back to sleep, and she awoke with her pants around her ankles. KAS reported the rape to her military leadership and local civilian law enforcement the next morning. Although she could not identify her assailant, DNA testing of vaginal swabs from KAS revealed the presence of Barnes’s DNA. Barnes testified that he could not recall any events after going to bed that night.

The 2009 incident. The second rape charge was that Barnes, once again on temporary duty at the same military base in Arizona, went drinking with a male staff sergeant and a civilian, NB, and raped the civilian. The government alleged that the staff sergeant and NB were leaving Barnes to take a cab back to town, NB told the staff sergeant that she had left her purse upstairs and that she would take a separate cab, and NB actually intended to return to Barnes and have consensual sex. It was undisputed



STEPHEN A. SALTZBURG is the Wallace and Beverley Woodbury University Professor at the George Washington University Law School in Washington, D.C. He is a past chair of the Criminal Justice Section and a regular columnist for *Criminal Justice* magazine.

He is also author of the book *Trial Tactics*, Third Edition (American Bar Association 2013), an updated and expanded compilation of his columns.

that Barnes and NB had consensual sex. But the government alleged that NB complained when Barnes removed his condom and repeatedly told him to stop, and he forced himself on her. A military police officer discovered NB walking down the road crying and hysterical and transported her to a military police station where she subsequently reported the rape. Barnes testified that he put on another condom, had further consensual intercourse with NB, and parted from her amicably with her showing no indications of distress.

The judge's instruction. The military judge instructed the members (military jury) as follows:

Evidence that the accused committed the sexual assault alleged in each specification and charge may have no bearing on your deliberations in relation to the other specifications and charge, unless you first determine, by a preponderance of the evidence that it is more likely than not the offense alleged in one of these specifications occurred. For example, if you determine by a preponderance of the evidence, the offense alleged in one of the specifications occurred, even if you were not convinced beyond a reasonable doubt that the accused is guilty of that offense, you may nonetheless then consider the evidence of that offense for its bearing on any matter to which it is relevant in relation to the other charge. You may also consider the evidence of such other acts of sexual assault for its tendency, if any, to show the accused's propensity or predisposition to engage in sexual assault. You may not, however, convict the accused solely because you believe he committed this other offense or solely because you believe the accused has a propensity or predisposition to engage in sexual assault. In other words, you cannot use this evidence to overcome a failure of proof in the government's case, if you perceive any to exist. The accused may be convicted of an alleged offense only if the prosecution has proven each element beyond a reasonable doubt. Each offense must stand on its own and proof of one offense carries no inference that the accused is guilty of any other offense. In other words, proof of one sexual assault creates no inference that the accused is guilty of another sexual assault. However, it may demonstrate that the accused has a propensity to commit that type of offense. The prosecution's burden of proof to establish the accused's guilt beyond a reasonable doubt remains as to each and every element of each offense charged. Proof of one charged offense carries with it no inference that the accused is guilty of any other charged offense.

The instruction, when parsed, meant that the jury could only convict Barnes of a rape if it found beyond a reasonable doubt that he committed it, but that it could consider evidence of either charged rape as propensity evidence even if it did not believe beyond a reasonable doubt that the defendant committed that rape as long as it found by a preponderance of the evidence that he did.

It should be apparent that the instruction is internally inconsistent to the extent that it told the members "proof of one sexual assault creates no inference that the accused is guilty of another sexual assault" but such proof "may demonstrate that the accused has a propensity to commit that type of offense." The propensity *inference* is permissible, and therefore proof of a rape by a preponderance of the evidence may, in fact, create an inference that the accused is guilty of another rape.

Closing arguments. The defense repeated in its closing argument a portion of the judge's instruction by arguing that "each offense must stand on its own and proof of one offense carries no inference that the accused is guilty of the other offense." The government's rebuttal argument also focused on the judge's instruction:

I ask that you pay careful attention to all of the instructions in their entirety, not just certain portions of them, and know that the accused's propensity to commit these offenses can be evaluated if you find he has at least committed the offense by [a] preponderance of the evidence standard. . . . The defense would like you to believe that the rape in 2009 and the rape in 2006 were so different, but yet, they are so similar. Each time the accused took what he wanted, when he wanted, without the consent of the other parties, of the victim. Each time. They are actually very similar.

The verdict. The members found Barnes guilty of both rapes.

The appeal. The Army Court of Criminal Appeals found no error in the judge's instruction. It reasoned as follows:

The government's propensity argument was a permissible use of Mil. R. Evid. 413's exception allowing evidence of similar crimes in sexual assault cases. The error here is that the military judge did not make the predicate findings on the record regarding the permissibility of any inference of propensity to be drawn from evidence that was also properly admitted as proof of charged misconduct.

In a more routine Mil. R. Evid. 413 case, the

military judge is required to make findings before evidence of uncharged misconduct is admitted. When evidence of charged misconduct is to be argued for its tendency, if any, to show propensity, the military judge should make similar findings allowing a propensity argument by counsel prior to providing an instruction. Based on the government's initial intent to argue propensity, the military judge should have made specific findings regarding not the initial admissibility of the evidence, but the use of evidence already properly admitted, and its relevance to the other charged sexual assault.

Presumably, the court of appeals was saying no more than this: because a trial judge must determine that there is sufficient evidence of uncharged misconduct before admitting Rule 413 evidence, the judge must also determine that there is sufficient evidence for a jury to find by a preponderance of the evidence that both rapes occurred before telling the jury that it may use one rape as propensity evidence in determining guilt on the other rape charge. The court seemed critical that the judge did not make such an on-the-record finding. But in a typical case there will be a motion for judgment of acquittal at the close of the evidence, and a denial of the motion signifies that the military judge finds that there is sufficient evidence for the members to find guilt beyond a reasonable doubt (which means that there clearly is sufficient evidence to meet a preponderance standard). If the standard motion was made in this case and was denied, the judge made all the findings that were required.

The court of appeals also observed that the trial judge made no Rule 403 balancing analysis on the record. It proceeded to do the balancing itself and found that the probative value of each rape was not outweighed by the danger of unfair prejudice. The use of the balancing test to evaluate uncharged misconduct makes sense (because the decision is whether to permit the jury to hear evidence of acts not charged), but when the conduct is charged it is in the case and it has been fully litigated. Even if the judge were to instruct a jury that it could not use one rape charge as propensity evidence, it is doubtful that the jury would be capable of following the instruction. The court of appeals seemed to think that each charged rape somehow became "uncharged" rape if it were not proved beyond a reasonable doubt, but this is nonsensical. A rape is either charged or uncharged; as long as there is sufficient evidence for a jury to find by a preponderance of the evidence that it occurred, it may be used as propensity evidence. When it is charged, however, it is *in* the case, and no balancing under Rule 403 will take it *out* of the case.

The Strategic Question

The government raised the idea of a propensity instruction in *Barnes*. That meant it thought such an instruction would be beneficial to the government. The military judge was not required to give the instruction and might not have done so absent a government request.

So, if a prosecutor has a choice between having the trial judge instruct as the judge did in *Barnes*, or having the judge say nothing about propensity in a case in which all of the sexual offenses in evidence are charged, what is the right choice? I believe that the instruction is more likely to be unhelpful to the prosecution for three reasons.

First, the instruction encourages the jury (or members in the military) to focus on the difference between a preponderance of the evidence and proof beyond a reasonable doubt rather than simply asking it to decide whether the government has proved its case by the usual standard of proof required in a criminal case. The jury might think that the judge thinks the evidence falls short of proof beyond a reasonable doubt on one or all of the charged offenses. The jury could well find itself in deliberations wondering why the judge would give such an instruction and complicate deliberations. Telling a jury about two different standards of proof is more likely to be confusing than helpful.

Second, the instruction is unnecessary. Jurors know how to consider two criminal charges tried together in a case like *Barnes*. They know they can convict on both counts, on only one, or on neither. It would have been rational for the *Barnes* members, for example, to distinguish the two rape charges on the ground that the first was totally nonconsensual and the second began with consensual conduct. It would also have been rational to find them to be similar as the prosecution contended.

Third, the language of the instruction is inherently contradictory as pointed out earlier and actually misstates the law. The language "proof of one sexual assault creates no inference that the accused is guilty of another sexual assault" tends to undermine the propensity inference that Rule 413 was adopted to permit. In short, proof of one sexual assault can be used to infer that an accused committed another sexual assault because of his or her propensity to commit such assaults.

So, I maintain that the prosecution is better off without the instruction. That means, of course, that the defense should not object to such an instruction. Telling the jury about two standards of proof and instructing the jury that proof of one sexual assault creates no inference that the accused is guilty of another sexual assault is likely to work to the benefit of the defense. ■

The Slow Justice Movement

BY GEOFF BURKHART

When things happen too fast, nobody can be certain about anything, about anything at all, not even about himself.

—Milan Kundera, *Slowness* (1995)

Americans exalt efficiency. Rapid transit, high-speed Internet, speed dating, fast food—few would abandon these for buggies and snail mail. But, as those of us who have daily gorged ourselves on fast food can attest, speed carries a cost. Some things are better slow.

Nowhere is this truer than in criminal justice. A quick Google or Westlaw search for “McJustice” or “assembly line justice” yields impressive results:

With many counties at their breaking points, Michigan courts increasingly value speed over quality, leading many advocates in the Ottawa County criminal justice community to describe the system as providing “McJustice.”

(Press Release, NLADA, Michigan Ranks 44th in the Nation for Public Defense Spending; So-Called “McJustice” System Puts Communities at Risk (June 2008), <http://tinyurl.com/ovkzotn>.)

Quality is sacrificed for efficiency. . . . We are fast becoming the courts of McJustice.

(Jeff Severns Guntzel, *Minnesota’s Public Defender Shortage: “We Are Fast Becoming the Courts of McJustice,”* MINNPOST (Oct. 13, 2010).)

[T]he courtroom was more of a fast food process rather than the idealistic notions which television and movies place in our head. I saw the public defenders, assistant district attorneys and judges as providing a service where the goal is to dispose of the cases as quickly as possible while still effectuating justice. Every player has a role to help the business run efficiently.

(William P. Quigley, *Reflections from the Journals of Prosecution Clinic Students*, 74 MISS. L.J. 1147, 1167 (2005).)



GEOFF BURKHART is an attorney and project director for the American Bar Association's Standing Committee on Legal Aid and Indigent Defendants.

We’re seeing court systems that are run about like a fast food restaurant. A fast food restaurant may be a little better, because at least there [are] some choices and a menu there for the customers. But people are processed through court not understanding what’s happening to them, with no investigation by the lawyer, no understanding of who they are, when they’re sentenced. They’re just processed through the system.

(Mark C. Milton, *Why Fools Choose to Be Fools: A Look at What Compels Indigent Criminal Defendants to Choose Self-Representation*, 54 ST. LOUIS U. L.J. 385, 404 (2009).)

[The attorney] describes being a public defender as a cross between an air-traffic controller and working at a fast-food restaurant. There are a lot of moving parts that have to be dealt with quickly and with people’s lives hanging in the balance.

(Nick Mariano, *Public Defenders: The Fast Food Workers of Justice?*, S. ILLINOISAN (Apr. 19, 2015).)

Data backs this up. Last year, an ABA study of the Missouri Public Defender Office found that attorneys spent, on average, 2.3 hours on each misdemeanor, but should be spending 11.7 hours in order to deliver reasonably effective assistance of counsel. (THE MISSOURI PROJECT: A STUDY OF THE MISSOURI PUBLIC DEFENDER SYSTEM AND ATTORNEY WORKLOAD STANDARDS 24 (2014), <http://tinyurl.com/qgp4v5u>.) In 2009, a study by the National Association of Criminal Defense Lawyers (NACDL) found that, on average, attorneys in Chicago, Atlanta, and Miami handled more than 2,000 misdemeanors a year. (NACDL, MINOR CRIMES, MASSIVE WASTE: THE TERRIBLE TOLL OF AMERICA’S BROKEN MISDEMEANOR COURTS 21 (2009), available at www.nacdl.org/reports/misdemeanor/.) A separate NACDL report found that the average misdemeanor arraignment in Florida lasts less than *three minutes*, even while most misdemeanants plead guilty at arraignment. (NACDL, THREE-MINUTE JUSTICE: HASTE AND WASTE IN FLORIDA’S MISDEMEANOR COURTS 9 (2011), available at www.nacdl.org/reports/threeminutejustice/.)

The ABA has developed extensive standards regarding defense counsel’s duties. (STANDARDS FOR CRIMINAL JUSTICE: DEF. FUNCTION (4th ed. 2015).) Not one of those tasks—investigating the facts (Standard 4-4.1), researching the law (Standard 4-4.6), communicating with the client (Standards 4-3.1, 4-3.3, 4-3.9, 4-5.1), negotiating with prosecutors (Standards 4-6.1, 4-6.2, 4-6.3), filing appropriate motions (Standards 4-6.2, 4-7.11, 4-8.1)—could be completed in less than three minutes, much less all of them.

And while books and television aren't an accurate reflection of legal practice—the rules of evidence, for instance, don't seem to exist in Hollywood—the gap between practice and the stories that inspired many of us is often disturbing. The methodically crafted defense mounted by Atticus Finch (before his sequel-driven downfall) bears little resemblance to an attorney saddled with more than 2,000 cases a year. Given that more than 95 percent of defendants plead guilty, the diligence of the jurors in *12 Angry Men* is rarer still.

While assembly line justice burdens attorneys, its effect on clients is greater still. The National Registry of Exonerations, a joint program of the University of Michigan and Northwestern University, has documented over 1,300 exonerations since 1989. Because exonerations occur most often in homicide and rape cases, which constitute less than 2 percent of felony convictions, scholars believe that this is just the tip of the iceberg.

But justice isn't reserved for the innocent. We have a duty to provide competent and diligent representation to all clients. (See MODEL RULES OF PROF'L CONDUCT R. 1.1, 1.3; ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 06-441 (2006).) That's simply impossible when shouldering hundreds of cases. (See, e.g., Tina Peng, *I'm a Public Defender. It's Impossible for Me to Do a Good Job Representing My Clients*, WASH. POST, Sept. 3, 2015.)

We've prized efficiency over effectiveness for too long.

There's a movement afoot, across several disciplines, to slow down. The Slow Movement is an intentional shift toward more thoughtful, logical pacing. A central tenet is that faster is not always better—some things are worth doing *well* instead of *quickly*. The time is ripe to apply this simple principle to criminal justice.

Carl Honoré's *In Praise of Slowness* (2004) is a call to arms for slow-minded folks (pun unavoidable). Honoré argues that "some things cannot, should not, be sped up. They take time; they need slowness. When you accelerate things that should not be accelerated, when you forget how to slow down, there is a price to pay." (*Id.* at 4–5.) As described above, we've paid a price for assembly line justice many times over in attorneys neglecting their ethical and constitutional obligations, clients being processed like cattle, and money being spent on imprisonment, relitigation, and compensation for innocent clients.

But what would a Slow Justice Movement look

like? The image shouldn't be too foreign. Simply put, it would look a great deal like ABA standards. Instead of three-minute justice, an attorney could meet with his or her client before court, research the law, investigate the facts, explore collateral consequences, strategize with other attorneys, develop mitigation, and give informed advice as to whether to proceed by way of trial or plea.

That last part warrants consideration. To be sure, a utopian system devoid of pleas isn't desirable. Guilty pleas are an excellent tool when attorneys have sufficient time to investigate, research, and communicate. But meet-and-pleads have no place in criminal justice. If guilty pleas are to exist, attorneys should stick closely to ABA standards, which require full investigation and research prior to entering a plea. (See, e.g., STANDARDS FOR CRIMINAL JUSTICE: DEF. FUNCTION Standard 4-6.1(b) ("In every criminal matter, defense counsel . . . should not recommend to a client acceptance of a disposition offer unless and until appropriate investigation and study of the matter has been completed. Such study should include discussion with the client and an analysis of relevant law, the prosecution's evidence, and potential dispositions and relevant collateral consequences.")) Thus, while a Slow Justice Movement would have fewer guilty pleas, it would certainly have some.

Nor is a Slow Justice Movement contrary to the right to a speedy trial. Despite its name and snail logo, the Slow Movement does not seek to do everything at a snail's pace. Rather, it seeks the right pace. As Honoré writes, "The paradox is that Slow does not always mean slow." Rather, the Slow Movement is about *balance*. The aim is the right speed: not too fast, not too slow, but control the pace, maximizing both efficiency and effectiveness.

How, then, should we pursue a Slow Justice Movement? There are several ways to slow criminal justice: lowering caseloads through decriminalization, reclassification, caseload limits, or prosecutorial discretion; increasing funding through education, lobbying, or litigation; using the private bar as a release valve when caseloads are too high. Whatever the approach, quality must precede quantity.

Like a drive-thru burger, American criminal justice is often fast, cheap, and unhealthy, while maintaining a nourishing guise. But we have seen the actual effects of speed—both in food and justice—for too many years to be complacent. The time to slow down is now. ■

Federal Rules Published for Public Comment

BY DAVID A. SCHLUETER

Under the Rules Enabling Act, 28 U.S.C. §§ 2071–77, amendments to the Federal Rules of Procedure and Evidence are initially considered by the respective advisory committees, who draft the rules, circulate them for public comment, and forward the rules for approval to the Judicial Conference's Standing Committee on the Rules. If the rules are approved by the Judicial Conference of the United States, they are forwarded to the Supreme Court of the United States, which reviews the rules, makes any appropriate changes, and in turn forwards them to Congress. If Congress makes no further changes to the rules, they become effective on December 1. That process—from initial drafting by the advisory committee to effective date—typically takes three years. In August 2015, the Standing Committee approved the publication of proposed amendments to two Federal Rules of Evidence—Rules 803(16) and 902. The public comment period for those proposals closes on February 16, 2016. The text of the proposed amendments is available at <http://www.uscourts.gov/rules-policies/proposed-amendments-published-public-comment> [hereinafter Proposed Amendments]. Comments may be submitted electronically at that same web address or e-mailed to rules_comments@ao.uscourts.gov.

Federal Rule of Evidence 803(16). Statements in Ancient Documents. The hearsay exception in Rule 803(16) provides that statements in an “ancient document” are admissible if the document is more than 20 years old and is shown to be authentic. The Advisory Committee on the Federal Rules of Evidence has proposed that the exception in Rule 803(16) be abrogated. The proposed committee note for the amendment explains that the exception “could once have been thought tolerable out of necessity (unavailability of other proof for old disputes) and by the fact that the exception has been so rarely invoked.” The drafters continue by noting, however, that “[g]iven the development and growth of

electronically stored information, the exception has become even less justifiable and more subject to abuse.” The committee note also states that counsel should be able to use other “reliability-based” hearsay exceptions, such as the business records exception in Rule 803(6) and the residual hearsay exception in Rule 807. Although the committee note does not reflect the point, the Advisory Committee's report to the Judicial Conference's Standing Committee indicates that it considered three other alternatives to dealing with Rule 803(16): limiting this hearsay exception to hardcopy documents, adding a necessity requirement similar to what appears in Rule 807, and adding a requirement that the document be found to be trustworthy. That report also indicates that the committee voted unanimously to abrogate the exception.

Federal Rule of Evidence 902. Evidence That Is Self-Authenticating. There are two proposed amendments to Rule 902, which would add Rule 902(13) and (14). Both amendments would permit counsel to authenticate records generated by an electronic process or system and evidence copied from an electronic device, storage medium, or file. Although the proposed committee notes to the new provisions are silent on the issue, the Advisory Committee discussed potential confrontation clause issues in its report to the Judicial Conference's Standing Committee on the Rules. The committee believed that no confrontation clause issue is raised if the certifications are used only to authenticate another piece of evidence, such as a document. (See Proposed Amendments, *supra*, at 20–21 (citing *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 322 (2009)).)

The first amendment to Rule 902 would add Rule 902(13), which would provide for self-authentication of records generated by an electronic process or system. The new provision would generally track with Rule 902(11) (Certified Domestic Records of a Regularly Conducted Activity) and Rule 902(12) (Certified Foreign Records of a Regularly Conducted Activity). The proposed note explains that the committee concluded that the expense and inconvenience of producing a witness to authenticate electronic evidence is often unnecessary; the opponent either stipulates to the evidence or fails to object. The committee note recognizes that the amendment addresses only the authenticity issue. Opposing counsel may make any other objections to the evidence, e.g., that the contents of a web page are hearsay, or that the notice requirements of 902(11) were not met.

The second proposed amendment to Rule 902 is a new provision in 902(14) that parallels the proposed new provision in Rule 902(13). Rule 902(14) would permit counsel to authenticate evidence that has been copied from an electronic database

(continued on page 43)



DAVID A. SCHLUETER is the Hardy Professor of Law and Director of Advocacy Programs at St. Mary's University Law School in San Antonio, Texas. He served as the reporter for the Advisory Committee on the Federal Rules of Criminal Procedure

from 1988 to 2005. He is a regular columnist for *Criminal Justice* magazine.

Supreme Court Cases of Interest

BY CAROL GARFIEL FREEMAN

During the first weeks of the October 2015 Term, the Court heard arguments in 11 of the 32 criminal justice cases pending at the end of June, including one challenging Florida's system of imposing capital sentences and another involving a life-without-parole sentence imposed on a 17-year-old in 1963. Several additional cases of interest were added to the docket. Arguments scheduled through December are listed below.

The only order of unusual interest issued during the summer was that staying the mandate of the Court of Appeals for the Fourth Circuit pending the filing and decision on a petition for cert to be filed by the former governor of Virginia, Robert McDonnell, No. 15A218 (Aug. 31, 2015). The petition was filed on October 13 (No. 15-474).

The decisions themselves and other information about the cases are available on the Court's website, www.supremecourt.gov.

CERT GRANTED

Note: *Questions presented are quoted as drafted by the parties, or, in some instances, by the Court.*

Capital Case

Williams v. Pennsylvania, No. 15-5040, *cert. granted*, Oct. 1, 2015, decision below at 105 A.3d 1234 (Pa. 2014), *reh'g denied*, Feb. 18, 2015.

1. In *Caperton v. A.T. Massey Coal Co.*, 556 U.S. 868, 881 (2009), this Court held that due process requires an "objective" inquiry into judicial bias. The question presented is:

Are the Eighth and Fourteenth Amendments violated where the presiding Chief Justice of a State Supreme Court declines to recuse himself in a capital case where he had personally approved the decision to pursue capital punishment against Petitioner in his prior



CAROL GARFIEL FREEMAN has been a staff lawyer with the US District Court for the District of Columbia, a deputy district public defender in Maryland, and an assistant US attorney for the District of Columbia. She is a regular columnist for Criminal Justice magazine and has been a Section vice-chair for publications, chair of the Book Board, and chair and member of the editorial board of the magazine.

capacity as elected District Attorney and continued to head the District Attorney's Office that defended the death verdict on appeal; where, in his State Supreme Court election campaign, the Chief Justice expressed strong support for capital punishment, with reference to the number of defendants he had "sent" to death row, including Petitioner; and where he then, as Chief Justice, reviewed a ruling by the state post-conviction court that his office committed prosecutorial misconduct under *Brady v. Maryland*, 373 U.S. 83 (1963), when it prosecuted and sought death against Petitioner?

In *Aetna Life Insurance Co. v. Lavoie*, 475 U.S. 813 (1986), this Court left open the question whether the Constitution is violated by the bias, appearance of bias, or potential bias of one member of a multimember tribunal where that member did not cast the deciding vote. The circuits and states remain split on that question. The question presented is:

Are the Eighth and Fourteenth Amendments violated by the participation of a potentially biased jurist on a multimember tribunal deciding a capital case, regardless of whether his vote is ultimately decisive?

Crimes and Offenses

Taylor v. United States, No. 14-6166, *cert. granted*, Oct. 1, 2015, decision below at 754 F.3d 217 (4th Cir. 2014).

Whether, in a federal criminal prosecution under the Hobbs Act, 18 U.S.C. § 1951, the Government is relieved of proving beyond a reasonable doubt the interstate commerce element by relying exclusively on evidence that the robbery or attempted robbery of a drug dealer is an inherent economic enterprise that satisfies, as a matter of law, the interstate commerce element of the offense.

Voisine v. United States, No. 14-10154, *cert. granted limited to Question 1 presented by the petition*, Oct. 30, 2015, decision below at 778 F.3d 176 (1st Cir. 2015), *reh'g denied*, Mar. 31, 2015.

1. Does a misdemeanor crime with the *mens rea* of recklessness qualify as a "misdemeanor crime of domestic violence" as defined by 18 U.S.C. §§ 921(a)(33)(A) and 922(g)(9)?

Double Jeopardy

Puerto Rico v. Valle, No. 15-108, *cert. granted*, Oct. 1, 2015, decision below at 192 D.P.R. 594 (2015).

Whether the Commonwealth of Puerto Rico and the Federal Government are separate sovereigns for purposes of the Double Jeopardy Clause of the United States Constitution.

Fourth Amendment

Utah v. Strieff, No. 14-1373, *cert. granted*, Oct. 1, 2015, decision below at 357 P.3d 532 (Utah 2015).

Should evidence seized incident to a lawful arrest on an outstanding warrant be suppressed because the warrant was discovered during an investigatory stop later found to be unlawful?

Habeas

Duncan v. Owens, No. 14-1516, *cert. granted*, Oct. 1, 2015, decision below at 781 F.3d 360 (7th Cir. 2015).

No clearly established precedent of this Court holds that it violates the Constitution for a finder of fact to infer a criminal defendant's motive when the motive is a non-element of the offense and is not directly established by the evidence at trial. Respondent claimed that the judge at his bench trial made improper "extrajudicial" findings regarding his motive and thus found him guilty based on evidence not produced at trial. The state appellate court upheld respondent's conviction, holding that the trial court's speculation regarding motive was harmless. The Seventh Circuit overturned respondent's conviction on habeas corpus review, finding that the trial court's inference about motive violated respondent's right to have his guilt adjudicated solely on the evidence introduced at trial, and that the error was not harmless.

Did the Seventh Circuit violate 28 U.S.C. § 2254 and a long line of this Court's decisions by awarding habeas relief in the absence of clearly established precedent from this Court?

Plain Error—Sentencing

Molina-Martinez v. United States, No. 14-8913, *cert. granted*, Oct. 1, 2015, decision below at 588 F. App'x 333 (5th Cir. 2014).

In *United States v. Olano*, 507 U.S. 725 (1993), the Court held that, in order to secure relief under plain-error review pursuant to Federal Rule of Criminal Procedure 52(b), a defendant must show that the error affected his substantial rights, which "in most cases [] means that the error must have been prejudicial[, i.e.,] [i]t must have affected the outcome of the district court proceedings." *Id.* at 734 (citations omitted). The Court, however, declined to "decide

whether the phrase 'affecting substantial rights' is always synonymous with 'prejudicial,'" *id.* at 735 (citations omitted); and the Court suggested that "[some] errors [] should be presumed prejudicial [even] if the defendant cannot make a specific showing of prejudice." *Id.*

Since that time, at least two circuits have, in connection with errors in the application of the United States Sentencing Guidelines, adopted the very sort of presumption suggested in *Olano*: that is, they presume an effect on substantial rights when an error results in the application of an erroneous Guideline range to a criminal defendant. See *United States v. Sabillon-Umana*, 772 F.3d 1328, 1333–34 (10th Cir. 2014); *United States v. Knight*, 266 F.3d 203, 207–10 (3d Cir. 2001). In this case, however, the Fifth Circuit rejected such a presumption as foreclosed by its prior decisions. See *United States v. Molina-Martinez*, 588 Fed. Appx. 333, 334 n.1 (5th Cir. 2014) (unpublished).

In light of the foregoing, the question presented is as follows:

Where an error in the application of the United States Sentencing Guidelines results in the application of the wrong Guideline range to a criminal defendant, should an appellate court presume, for purposes of plain-error review under Federal Rule of Criminal Procedure 52(b), that the error affected the defendant's substantial rights?

DECIDED CASE

Maryland v. Kulbicki, No. 14-848, *cert. granted and judgment of Maryland Court of Appeals reversed*, Oct. 5, 2015. Kulbicki was convicted of murder in 1995 on evidence including testimony of a state expert on comparative bullet lead analysis (CBLA). For many years, expert witnesses had testified that elements in the lead of bullet fragments could be used to identify the package from which the bullet had come. By 2006, the CBLA theory had been debunked and such testimony was no longer admissible. Kulbicki had a pending post-conviction petition that he amended to include a claim that his lawyers were constitutionally ineffective by not challenging the testimony of the state expert. The lower courts rejected his petition. Although he abandoned his CBLA claim in the court of appeals, that court reversed on the sole basis that counsel should have found an obscure report coauthored by the state expert in 1991 that presaged the later rejection of CBLA. The Court, per curiam, reversed, concluding that the lawyers' failure to find the report and challenge the

then-accepted CBLA testimony was reasonable and did not constitute ineffective assistance under *Strickland v. Washington*, 466 U.S. 668 (1984).

ARGUMENTS

Tuesday, October 6, 2015:

Ocasio v. United States, No. 14-361, *Cert. Alert*, 30:2 CRIM. JUST. at 50 (Summer 2015) (Does conspiracy to extort require the conspirators to agree to obtain property from someone outside the conspiracy?).

Wednesday, October 7, 2015:

Kansas v. Gleason, No. 14-452, *Cert. Alert*, 30:2 CRIM. JUST. at 50 (Summer 2015), joined for one-hour argument with *Kansas v. Carr*, Nos. 14-449 & 14-450, *Cert. Alert*, 30:2 CRIM. JUST. at 50 (Summer 2015) (Must capital sentencing jury be affirmatively instructed that mitigating circumstances need not be proven beyond a reasonable doubt, or is it sufficient if instructions make clear that each juror must individually assess any mitigating circumstances?).

Kansas v. Carr, *supra* (One hour for argument on question whether decision not to sever sentencing phase of brothers' trials violated their Eighth Amendment rights and was not harmless.).

Tuesday, October 13, 2015:

Montgomery v. Louisiana, No. 14-280, *Cert. Alert*, 30:2 CRIM. JUST. at 51 (Summer 2015) (Is *Miller v. Alabama*, 132 S. Ct. 2455 (2012), applicable to a 17-year-old sentenced to life without parole in 1963, and does the Court have jurisdiction to review state court's decision to deny *Miller* retroactive effect?).

Hurst v. Florida, No. 14-7505, *Cert. Alert*, 30:2 CRIM. JUST. at 50 (Summer 2015) (Does Florida's death sentencing system violate the Sixth or Eighth Amendment, in light of the decision in *Ring v. Arizona*, 536 U.S. 584 (2002)?).

Monday, November 2, 2015:

Foster v. Chatman, No. 14-8349, *Cert. Alert*, 30:3 CRIM. JUST. at 50 (Fall 2015) (Capital case, *Batson* issue (*Batson v. Kentucky*, 476 U.S. 79 (1986))).

Tuesday, November 3, 2015:

Lockhart v. United States, No. 14-8358, *Cert. Alert*, 30:3 CRIM. JUST. at 51 (Fall 2015) (Interpretation of sentencing provision on conviction of possessing child pornography for a person with a prior conviction of sexual abuse.).

Torres v. Lynch, No. 14-1096, *Cert. Alert*, 30:3 CRIM. JUST. at 50 (Fall 2015) (Immigration issue, whether a state offense that does not include an interstate

commerce element constitutes an aggravated felony because it is described in a specific federal statute.).

Wednesday, November 4, 2015:

Bruce v. Samuels, No. 14-844, *Cert. Alert*, 30:3 CRIM. JUST. at 50 (Fall 2015) (Application of Prison Litigation Reform Act provision requiring prisoners proceeding *in forma pauperis* to pay a portion of their income to the filing fees.).

Tuesday, November 10, 2015:

Luis v. United States, No. 14-419, *Cert. Alert*, 30:3 CRIM. JUST. at 51 (Fall 2015) (Does the pretrial restraint of a defendant's assets, not traceable to a criminal offense, needed to retain counsel of choice, violate the Fifth and Sixth Amendments?).

Monday, November 30, 2015:

Musacchio v. United States, No. 14-1095, *Cert. Alert*, 30:3 CRIM. JUST. at 50 (Fall 2015) (Appellate procedure when instructions, without objection, required proof of elements not specified in statute or indictment, and whether a statute of limitations defense not raised before or at trial can be reviewed on appeal.). ■

FEDERAL RULES ALERT

(continued from page 40)

through a certification from a qualified person who can show that the information was authenticated by a "process of digital identification." The certification must comply with the requirements of Rule 902(11) (domestic records) or Rule 902(12) (foreign records). The proposed committee note recognizes that a typical method of authenticating electronic files is through use of a "hash value," which in turn requires a witness to verify that he or she checked the hash value of a particular item and that it is identical to the original. The note indicates that the language of the new provision permits counsel to authenticate evidence through other technology and that the new language only addresses the question of the authenticity of the evidence, not other potential objections, such as a hearsay objection to the contents. ■

ABA Model Act Addresses Myth of “Clean Slate”

BY ROBERT SCHWARTZ

The American Bar Association has moved to address harm to children caused by one of the great myths of juvenile justice: that juvenile records are confidential, or automatically expunged, because of the system’s goal of protecting children from the consequences of criminal behavior.

In truth, as Juvenile Law Center noted in its 2014 report, *Juvenile Records: A National Review of State Laws on Confidentiality, Sealing and Expungement*, many states disclose information about youth involvement with the juvenile justice system and fail to provide opportunities for expungement.

This is a serious problem. Young people are routinely denied jobs, housing, access to the military, and admission to college because their juvenile records are open to the public. Youth who expect to have “second chances” encounter high barriers from juvenile records that they incorrectly believed would be expunged.

To respond to these problems, the ABA House of Delegates at the August 2015 Annual Meeting adopted a Model Act Governing the Confidentiality and Expungement of Juvenile Delinquency Records. The model act builds on long-standing ABA policy that directs states to enact statutes to protect youth from the adverse consequences of juvenile delinquency records. The Criminal Justice Section cosponsored the recommendation, which was introduced by the Section of Litigation through its Children’s Rights Litigation Committee. The model act provides legislators with language they can use to tighten the confidentiality of delinquency records and provide for faster and easier expungement once youths’ cases are closed.

The model act implements policy that is as old as the IJA-ABA Juvenile Justice Standards that the association adopted in 1980. It also operationalizes the 2010 ABA policy on collateral consequences, which called upon government entities to limit “the collateral consequences of juvenile arrests, adjudications, and convictions.” The 2010 policy, for example, would prohibit employers or educational institutions from considering juvenile records “if such records have been sealed or expunged by the court.”

Juvenile records are addressed in the volume

entitled *Standards Relating to Juvenile Records and Information Systems* (IJA-ABA JR-IS). These standards direct each state to enact laws that:

- protect juveniles from the adverse consequences of disclosure of juvenile records;
- establish safeguards to protect against the misuse, misinterpretation, and improper dissemination of juvenile records;
- limit the collection and retention of juvenile records so that unnecessary and improper information is not collected or retained;
- restrict the information and juvenile records that may be disseminated to and used by third persons;
- afford juveniles and their parents with maximum access to juvenile records pertaining to them; and
- provide for the timely destruction of juvenile records.

Under the IJA-ABA JR-IS Standards, the term “juvenile records” encompasses juvenile delinquency court records, which include the “case file” (formal documents such as the complaint or petition, summonses, warrants, motions, legal memoranda, and judicial orders or decrees), “summary records” (the equivalent of the docket maintained by most juvenile courts), and “probation records” (which include social histories). (IJA-ABA JR-IS Standards 13.1, 13.3, 14.1–.3.) The term also includes “law enforcement records.” (IJA-ABA JR-IS § IV.) The model act definitions track the definitions in the Standards.

The model act addresses two core aspects of juvenile records: (1) confidentiality, i.e., who has access to juvenile records that are maintained by juvenile courts, juvenile probation, and law enforcement; and (2) expungement or sealing of records of cases that have been closed.

Confidentiality. The model act first defines records that should be covered by confidentiality provisions. These include pleadings in juvenile court cases, as well as social records in those files, such as medical records, psychological records, service plans, education records, and demographics about the child or family.

The model act then prohibits “public inspection” of those records and lists to whom and under what circumstances those records can be made available. These include court personnel, such as prosecutors and defense attorneys, as well as agencies that have custody of a child pursuant to a court order. Courts also have discretion to make records available to others, upon petition, subject to restrictions in federal law. When a court makes records available, it “may include in its order restrictions on the use and re-disclosure of the released information.”

Expungement. The model act prescribes automatic

ROBERT SCHWARTZ is the cofounder and executive director emeritus of Juvenile Law Center in Philadelphia. He is a regular columnist to *Criminal Justice* magazine.

expungement for certain kinds of records. These include records of dismissed cases, or cases in which a juvenile has successfully completed a program of diversion. There are exceptions. For example, automatic expungement would be delayed if the chief law enforcement officer can certify that certain information is needed for a pending investigation.

In some situations, the model act directs the juvenile court after specified periods of time to order the expungement of records, noting that “this requires no application or action” on the part of the juvenile. The model act also allows juveniles, in cases in which expungement is not automatic, to petition the court for expungement.

The model act requires the juvenile’s defense attorney “to inform the juvenile of the consequences of being adjudicated delinquent, the definition of expungement, and the timeline for expungement that is automatic and that which is available upon application.”

The model act directs the juvenile court, “at the time of dismissal or disposition of the case,” to inform the juvenile “of his or her expungement rights.”

Once a person’s record is expunged, it is as though it never existed. The model act gives persons whose records are expunged the right to respond, when asked, “that no record exists.”

The model act is a thoughtful action by the ABA to balance the needs of juvenile courts and law enforcement with society’s interest in giving juveniles second chances. As Attorney General Loretta Lynch recently blogged about “second chances”:

The long-term—sometimes lifetime—impact of a criminal record will keep many of these people from obtaining employment, accessing housing, higher education, loans, and credit—even if they have paid their debt to society, turned their lives around, and demonstrated that they are unlikely to reoffend. At the same time, research sponsored by the National Institute of Justice (NIJ) shows that individuals who stay out of trouble for just a few years after an arrest are largely indistinguishable from the general population in terms of their likelihood of committing a crime. Further, participation in pro-social behaviors like employment, education and civic engagement—the very things that people with criminal records are often barred from participating in—actually reduce recidivism. (Loretta Lynch, *Second Chances Vital to Criminal Justice Reform*, HUFFPOST BLOG (July 30, 2015), <http://tinyurl.com/pl3csfy>.) ■

MACHINES AS CRIME FIGHTERS (continued from page 14)

create and to call for experts in these different fields to come together to begin addressing them. Traditionally, police tactics are governed by the courts, which, facing issues on a case-by-case basis, are not experts in the fields at issue and do not have the information, perspective, or jurisdiction to create broadly applicable guidelines for the use of new technology.

That’s not to say I do not have my perspective on how ASAs should be handled. There should be meaningful standards to govern the creation and training of ASAs to ensure their effectiveness and minimize the continuing impact of historical biases and some body to oversee their implementation. There also should be guidelines for the disclosure of how ASAs work, so that civilians can meaningfully understand how they are being evaluated by the

police, while law enforcement is not unduly hindered and valid business interests are protected. Criminal defendants must be able to exercise their due process rights and challenge searches and seizures based on an ASA’s alert. Finally, judges must be able to issue informed rulings when an ASA’s prediction comes before them.

Of course, if I am an expert at all, it is only in criminal procedure. My perspective on these issues is blinkered by my experience in the field in which I work. Other perspectives must be part of the conversation in order to achieve the best answer to any of the problems I have identified, before ASAs are put into place more broadly and answers to these questions come piecemeal and from the limited capabilities of the courts. ■

Defense Experts and the Myth of Cross-Examination

BY PAUL C. GIANNELLI

Recent Supreme Court cases concerning ineffective assistance of counsel have emphasized the need for defense experts. In *Harrington v. Richter*, 131 S. Ct. 770, 788 (2011), the Court wrote: “Criminal cases will arise where the only reasonable and available defense strategy requires consultation with experts or introduction of expert evidence.” In *Hinton v. Alabama*, 134 S. Ct. 1081 (2014), the Court found the defense counsel ineffective for failing to understand the statutory procedure for retaining a defense firearms identification expert. The Court commented:

Prosecution experts, of course, can sometimes make mistakes. Indeed, we have recognized the threat to fair criminal trials posed by the potential for incompetent or fraudulent prosecution forensics experts, noting that “[s]erious deficiencies have been found in the forensic evidence used in criminal trials. . . . One study of cases in which exonerating evidence resulted in the overturning of criminal convictions concluded that invalid forensic testimony contributed to the convictions in 60% of the cases.” This threat is minimized when the defense retains a competent expert to counter the testimony of the prosecution’s expert witnesses; it is maximized when the defense instead fails to understand the resources available to it by law.

(*Id.* at 1090 (quoting *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 319 (2009) (citing Brandon L. Garrett & Peter J. Neufeld, *Invalid Forensic Science Testimony and Wrongful Convictions*, 95 VA. L. REV. 1, 14 (2009))).)

When *Hinton* was remanded for a retrial, the prosecutor moved for a dismissal after the prosecutor’s new experts reexamined the bullets. “After a new round of analysis, prosecutors wrote, the

state experts ‘found that they could not conclusively determine that any of the six bullets were or were not fired through the same firearm or that they were fired through the firearm recovered from the defendant’s home.’” (Alan Blinder, *Alabama Man on Death Row for Three Decades Is Freed as State’s Case Erodes*, N.Y. TIMES, Apr. 4, 2015, at A11.) Hinton had spent 30 years on death row.

The Right to a Defense Expert

In *Ake v. Oklahoma*, 470 U.S. 68, 76 (1985), the Supreme Court recognized a due process right to a defense expert: “[W]hen a State brings its judicial power to bear on an indigent defendant in a criminal proceeding, it must take steps to assure that the defendant has a fair opportunity to present his defense.” This fair opportunity mandates that an accused be provided with the “basic tools of an adequate defense.” While the *Ake* decision settled the core issue by recognizing a right to expert assistance, it left a number of important issues unresolved. (See generally Paul C. Giannelli, *Ake v. Oklahoma: The Right to Expert Assistance in a Post-Daubert, Post-DNA World*, 89 CORNELL L. REV. 1305 (2004).) Because some courts have been reluctant to give *Ake* a broad reading, problems persist—in particular, the standard for appointment of a defense expert is often too demanding. If the threshold standard is set too high, the defendant is placed in a “catch-22” situation, in which the standard “demand[s] that the defendant possess already the expertise of the witness sought.” (*State v. Moore*, 364 S.E.2d 648, 657 (N.C. 1988).)

The Limits of Cross-Examination

One rationale used to justify the failure to appoint a defense expert focuses on the right of cross-examination. It is not uncommon to find appellate courts that cite cross-examination of the prosecution expert as a substitute for the appointment of a defense expert. For example, in *Plunkett v. State*, 719 P.2d 834, 839 (Okla. Crim. App. 1986), the court rejected a request for a blood stain expert. In limiting *Ake* to psychiatric expertise, the court wrote that the risk of an inaccurate resolution in other areas of scientific evidence “is not necessarily present because the scientific expert is often able to explain to the jury how a conclusion was reached, the defense counsel can attack that conclusion, and the jury can then decide whether the conclusion had a sound basis.” (*Id.*)

Another court declared:

[W]e disagree with [the defendant’s] contention that the average attorney is ill-equipped to defend against [DNA] evidence. To the contrary, law libraries—i.e., law journals, practitioners’ guides, annotated law reports, CLE



PAUL C. GIANNELLI is a Distinguished University Professor and Weatherhead Professor of Law at Case Western Reserve University in Cleveland, Ohio, and the coauthor of *Scientific Evidence* (Lexis 5th ed. 2012). He is also a regular columnist for *Criminal Justice* magazine.

materials, etc.—are teeming with information and advice for lawyers preparing to deal with DNA evidence in trial. Even a cursory perusal of the literature in this area reveals copious lists of questions for defense attorneys to use in cross-examinations and other strategies for undermining the weight of DNA evidence. (State v. Huchting, 927 S.W.2d 411, 420 (Mo. Ct. App. 1996).)

This statement borders on the incredulous. First, the same reasoning applies to prosecutors seeking a psychiatric evaluation of an accused who raises an insanity defense. There are numerous texts and CLE materials on this subject, and yet virtually every jurisdiction has procedures recognizing the prosecution's right to have the accused *examined* by a state psychiatrist—i.e., a prosecution expert. (See FED. R. CRIM. P. 12.2(c).) The rationale for this procedure is obvious—the adversary system would be undermined if the prosecution was deprived of its own expert. The same is true when the defense is deprived of the right to a defense expert.

Second, effective cross-examination of a prosecution expert frequently depends on the advice of a defense expert. In a British DNA study, “94 per cent of defence lawyers who consulted an expert felt that they had been assisted by that expert, either in their evaluation of the case and the advice they gave to their client or in presenting their case in court.” (BEVERLEY STEVENTON, ROYAL COMM’N ON CRIMINAL JUSTICE, THE ABILITY TO CHALLENGE DNA EVIDENCE, RESEARCH STUDY NO. 9, at 43 (1993).)

Third, there is a significant difference between attacking the opinion of an opponent's expert through cross-examination and attacking that opinion through the testimony of your own expert. In *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), the Supreme Court did not cite cross-examination by itself; it noted that “[v]igorous cross-examination, *presentation of contrary evidence*, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence.” (*Id.* at 596 (emphasis added) (citing *Rock v. Arkansas*, 483 U.S. 44, 61 (1987)).) In *Barefoot v. Estelle*, 463 U.S. 880, 898–99 (1983), the Court wrote that the “jurors should not be barred from hearing the views of the State's psychiatrists *along with opposing views of the defendant's doctors*” (emphasis added).

Similarly, the National Academy of Sciences 1992 report observed that “[m]ere cross examination by a defense attorney inexperienced in the science of DNA testing will not be sufficient.” (NAT’L

RESEARCH COUNCIL, DNA TECHNOLOGY IN FORENSIC SCIENCE 160 (1992).) A noted forensic scientist agrees: “If cross-examination is to be the only way to discover misleading or inadequate testimony by forensic scientists, then too much is being expected from it.” (Douglas M. Lucas, *The Ethical Responsibilities of the Forensic Scientist: Exploring the Limits*, 34 J. FORENSIC SCI. 719, 724 (1989).) Another commentator rejected, almost out of hand, the argument that the “searing test of a rigorous cross-examination” is a sufficient safeguard in this context. He wrote: “All that one can say to such an argument is that the lawyers who make it should know better, and, if they do know better, as they must if they are experienced trial lawyers, they should have more conscience than to perpetuate such a myth.” (Barton L. Ingraham, *The Ethics of Testimony: Conflicting Views on the Role of the Criminologist as Expert Witness*, in *EXPERT WITNESSES: CRIMINOLOGISTS IN THE COURTROOM* 178, 183 (Patrick R. Anderson & L. Thomas Winfree Jr. eds., 1987).)

Several courts have also recognized this point. For instance, in *De Freece v. State*, 848 S.W.2d 150, 160 (Tex. Crim. App. 1993), the Texas Court of Criminal Appeals rejected the notion that an “admirable” cross-examination of the prosecution expert justified the failure to appoint a defense expert. (*Accord Williamson v. Reynolds*, 904 F. Supp. 1529, 1562 (E.D. Okla. 1995) (“This court disagrees that cross-examination of the State's experts was an acceptable substitute for Petitioner's own experts.”), *rev'd on other grounds*, *Williamson v. Ward*, 110 F.3d 1508, 1522 (10th Cir. 1997) (noting that due process, not *Daubert*, standard applies in habeas proceedings); *People v. Lawson*, 644 N.E.2d 1172, 1191 (Ill. 1994) (finding defense counsel's cross-examination not sufficient).)

Conclusion

Even after *Ake* and *Daubert*, securing the services of a defense expert often remains a challenge. A well-known federal judge has written: “Courts, as gatekeepers, must be aware of how difficult it can be for some parties—particularly indigent criminal defendants—to obtain an expert to testify. The fact that one side may lack adequate resources with which to fully develop its case is a constant problem.” (Jack B. Weinstein, *Science, and the Challenges of Expert Testimony in the Courtroom*, 77 OR. L. REV. 1005, 1008 (1998); see also ROGER A. HANSON, *INDIGENT DEFENDERS: GET THE JOB DONE AND DONE WELL* 100 (1992) (the “greatest disparities occur in the areas of investigators and expert witnesses, with the prosecutors possessing more resources”).) ■

Misuse of Letterhead by Prosecutors and Attorneys General

BY PETER A. JOY AND KEVIN C. McMUNIGAL

In the past few years, some prosecutors and attorneys general have lent the authority of their offices to others through use of their letterhead. There have been several news reports of prosecutor offices and attorneys general selling (sometimes also referred to as “renting”) official letterhead and the seals of their offices to debt collectors for use in demand letters. In return for use of the letterhead, prosecutors and attorney general offices receive a portion of the money collected. (See, e.g., Jessica Silver-Greenberg, *In Prosecutors, Debt Collectors Find a Partner*, N.Y. TIMES, Sept. 15, 2012, <http://tinyurl.com/9ststnj>; Debra Cassens Weiss, *Debt Collectors Use DA Letterhead, with Permission, to Threaten Bad Check Writers*, A.B.A. J., Sept. 17, 2012, <http://tinyurl.com/nco477c>.) The letters prominently display the prosecutor’s or attorney general’s official seal and proclaim “Official Notice.” The body of the letter typically spells out the potential prison sentence for an offense such as bouncing a bad check.

In a similar and no less disturbing misuse of office, some attorneys general have sent letters on official letterhead substantially written by lobbyists or lawyers for corporations that have made campaign contributions to the attorney general. An exposé in the *New York Times* revealed how the attorney general of Oklahoma let lawyers for an energy company draft a letter denouncing federal pollution regulation of energy companies that the attorney general then sent on state government stationery with only

a few word changes. (Eric Lipton, *Energy Firms in Secretive Alliance with Attorney General*, N.Y. TIMES, Dec. 6, 2014, <http://tinyurl.com/lzj7d6z>.) The *New York Times* reported that “[a]ttorneys general in at least a dozen states are working with energy companies and other corporate interests, which in turn are providing them with record amounts of money for their political campaigns, including at least \$16 million this year [2014].” (*Id.*)

The *New York Times* broke another story about a law firm representing the Motion Picture Association of America (MPAA) drafting a letter that Mississippi’s attorney general sent with only minor changes to Google threatening an investigation and possible criminal action if Google did not cease practices that the MPAA had complained about to state attorneys general. The attorney general followed up the letter by serving Google with a 79-page subpoena, based on work by a team of lawyers from the MPAA, which asked for an extensive list of records. (Nick Wingfield & Eric Lipton, *Google’s Detractors Take Their Fight to the States*, N.Y. TIMES, Dec. 16, 2014, <http://tinyurl.com/qy955ay>.)

Following public revelation of prosecutors and state attorneys general selling their letterhead to debt collectors, the ABA Standing Committee on Ethics and Professional Responsibility issued an advisory ethics opinion explaining that this practice is unethical and must stop. In Formal Opinion 469, available at <http://tinyurl.com/pfsk3jb>, the standing committee explained that prosecutors engaging in such arrangements with debt collectors violate Model Rules 8.4(c) (conduct involving dishonesty, fraud, deceit, or misrepresentation) and 5.5(a) (assisting in the unauthorized practice of law).

There is not an ethics opinion specifically addressing the practice of attorneys general permitting lobbyists and lawyers for campaign contributors to draft letters and direct their actions without disclosing it to the recipients of the letters. But this practice raises several ethical issues. In this column, we examine both practices.



PETER A. JOY is the Henry Hitchcock Professor of Law and director of the Criminal Justice Clinic at Washington University School of Law in St. Louis, Missouri; he can be reached at joy@wustl.edu.



KEVIN C. McMUNIGAL is a professor of law at Case Western Reserve University School of Law in Cleveland, Ohio; he can be reached at kcm4@case.edu. Both authors are regular columnists for Criminal Justice magazine and are coauthors of *Do No Wrong: Ethics for Prosecutors and*

Defenders (2009), as well as the chapter “Basic Ethics: Criminal Practice and the Media” in *Media Coverage in Criminal Justice Cases* (Andrew E. Taslitz ed., 2013).

The Problems

More than 300 prosecutors and attorneys general across the United States have partnered with debt collection agencies. Some consumer lawyers estimate that more than one million collection letters a year are being sent on prosecutor letterhead without any oversight by prosecutor offices receiving payment for the use of their letterhead. Class action lawsuits seeking to ban this practice have been filed in California and Washington alleging violations of the federal Fair Debt Collection Practices Act (FDCPA) and state laws. Recently the Sixth Circuit Court of Appeals, in *Gillie v. Law Office of Eric A. Jones, LLC*, 785 F.3d 1091 (6th Cir. 2015), cert. filed, No.

15-620 (Nov. 13, 2015), decided that lawyers designated as special counsel by Ohio's attorney general to collect state debts using the Ohio Attorney General's letterhead are not "officers" of the State of Ohio and thus not exempt from the FDCPA.

The demand letters usually cite criminal statutes and state that the recipient has been accused of violating the law by, for example, passing a bad check or incurring a debt. The demand letters also advise the debtor that to avoid the possibility of further action from the prosecutor's office the debtor must pay the amount of the debt, collection fees, and, in many cases, a substantial additional fee to attend a mandatory debtor education course. The prosecutor's office whose stationary is used receives a portion of the collection fees and fees from the debtor education course. Typically, no lawyer in the prosecutor's office reviews the case file to determine if a crime has been committed, if prosecution is warranted, or if the demand letter complies with the ethics rules. In many of the agreements, merchants refer bounced checks directly to debt collection agencies and the prosecutor offices are never involved.

It is much harder to estimate the frequency of state attorneys general permitting lobbyists and lawyers for campaign contributors to draft letters and direct their actions. In the cases involving the attorneys general of Oklahoma and Mississippi, both maintained that the letters they used reflected their own positions and that there was nothing wrong with using drafts provided to them by campaign contributors. Unlike the debt collection letters that no one from a prosecutor's or attorney general's office reviews, when attorneys general have taken letters drafted by lobbyists or lawyers for campaign contributors in the reported instances they have reviewed the letters and, , made some changes.

Both practices, though, raise additional issues. In debt collection matters, the recipient is likely to think that the prosecutor's or attorney general's office is involved in the debt collection, when it is not. In the matters involving attorneys general stating positions or threatening legal action in letters prepared by others, there is a lack of candor by concealing the lobbyists' or campaign contributors' involvement. If the identities of the drafters were known, the targets of the letters and the general public would be able to evaluate whether the attorneys general are motivated or influenced by outside contributors. For example, once Google uncovered that the Mississippi attorney general was working in concert with the MPAA, Google filed a lawsuit alleging that the attorney general was conspiring with the MPAA to engage in a smear campaign against Google and to violate Google's First Amendment rights. It also alleged that the investigation was improperly influenced. (See Hayley Tsukayama, *Google Files Lawsuit*

against Mississippi Attorney General, WASH. POST, Dec. 19, 2014, <http://tinyurl.com/oquaklm>.) The federal district court granted Google's preliminary injunction to quash the subpoena and granted an injunction against the Mississippi attorney general. Although the court's order is still under seal, a posting on Google's Public Policy Blog states that the court's ruling "recognizes that the MPAA's long-running campaign to censor the web . . . is contrary to federal law." (Kent Walker, *The MPAA's Attempt to Revive SOPA through a State Attorney General* (Dec. 18, 2014), <http://tinyurl.com/lwnfeuv>.)

Debt Collection Letters on Prosecutor Letterhead

Dishonesty and misrepresentation. Model Rule 8.4(c) states: "It is professional misconduct for a lawyer to . . . engage in conduct involving dishonesty, fraud, deceit or misrepresentation." In stating that a prosecutor violates this ethics rule by entering into agreements with debt collection agencies such as those described above, the ABA Standing Committee on Ethics and Professional Responsibility, in Opinion 469, relied on both ABA and state ethics opinions that previously held that it is unethical for a lawyer to allow a client to use the lawyer's stationary for demand letters. Such demand letters are deceptive because they imply that the lawyer is involved in the debt collection. By allowing a client to use the lawyer's letterhead, the lawyer is a party to the deception. (ABA Comm. on Prof'l Ethics & Grievances, Formal Op. 253 (1943); N.J. Comm. on the Unauthorized Practice of Law & Advisory Comm. on Prof'l Ethics, Joint Ops. 48 & 725 (2012).)

Opinion 469 states that demand letters written on a prosecutor's letterhead "are even more deceptive . . . because they misuse the criminal justice system by deploying the apparent authority of a prosecutor to intimidate an individual." The demand letters imply that the prosecutor's office is involved in the debt collection and that criminal prosecution will follow if the alleged debtor does not make restitution and pay any additional fees tacked on by the debt collection agency, including the cost of participating in a class on financial responsibility. In some instances, the fees tacked on may be twice the amount of restitution required. In addition to being deceptive, the committee explains in a footnote that the prosecutor could also be participating in extortion if the threat to file a criminal action meets the jurisdiction's elements of extortion. (See, e.g., *State ex rel. Neb. State Bar Ass'n v. Gobel*, 271 N.W.2d 41 (Neb. 1978) (suspending county attorney for three months for threatening debtor of private client with criminal charges if debtor did not satisfy debt).)

Although it focused on prosecutor offices selling their letterhead, Opinion 469 is equally applicable

to state attorney general offices doing the same or permitting lawyers, like the private lawyers the Ohio attorney general contracted with to serve as special counsel, to use official letterhead to collect debts owed to the state. Such letters misrepresent the authority of the sender and are misleading. In analyzing why such a practice is false, deceptive, and misleading, the Sixth Circuit stated: “Intimidation is at the heart of this case. There is no compelling reason for special counsel to use the OAG [Ohio Attorney General] letterhead, other than to misrepresent their authority and place pressure on those individuals receiving the letters.” (*Gillie*, 785 F.3d at 1105.)

Assisting in unauthorized practice of law. An additional ethics violation, assisting in the unauthorized practice of law, arises if a prosecutor or attorney general permits a debt collector who is not a lawyer to send out demand letters on the prosecutor’s or attorney general’s stationery. Model Rule 5.5 prohibits a lawyer from assisting another to practice law in violation of a jurisdiction’s regulations on the practice of law. The ABA has long held that a lawyer providing a client with the lawyer’s signed letterhead to send demand letters to debtors is assisting in the unauthorized practice of law. (ABA Comm. on Prof’l Ethics & Grievances, Formal Op. 68 (1932).)

In Opinion 469, the ABA ethics committee reasoned that prosecutors permitting debt collectors to use their letterhead are similarly assisting another in the unauthorized practice of law in violation of Model Rule 5.5. The committee found the practice of prosecutors letting debt collectors use their letterhead “even more abusive . . . because it gives the impression that the machinery of the criminal justice system has been mobilized against the debtor, and that unless the debtor pays the debt, the debtor faces criminal prosecution and possible incarceration.”

ABA Opinion 469’s holding concerning the unauthorized practice of law parallels ABA Opinion 68 and state court decisions and state bar ethics opinions in California, Georgia, Illinois, Indiana, Kentucky, Minnesota, New York, and Washington, disapproving the use of lawyer letterhead by clients, and Opinion 469 cites these cases and ethics opinions. To date, however, it does not appear that state bar disciplinary authorities have addressed the practice of prosecutors selling letterhead to debt collectors.

A perverse incentive. Ethics rules reflect a serious concern about lawyers engaging in practices that generate perverse incentives—incentives that threaten to undermine fulfillment of a lawyer’s obligation to a client. This concern is typically expressed in conflict-of-interest rules. The debt collection arrangements discussed above that generate funds for a prosecutor’s office do not fall easily under the

Model Rules’ definition of a conflict of interest, because the threat to the prosecutor’s fulfillment of duties to the client does not arise from the prosecutor’s personal interests or the interests of another client or third party. But the money coming in from these arrangements with debt collectors nonetheless can create a substantial risk of distorting the prosecutor’s professional judgment.

To understand this risk, it is useful to look at other examples of potential sources of income to a prosecutor’s office that have recently given rise to concern. For example, overdependence on the use of traffic fines to fill public coffers can distort the judgment of prosecutors and police when it comes to monitoring the validity of traffic violations. To curb this, the recent Ferguson report recommended limits on the amount of money local governments can make from traffic fines. The same type of conflict can arise from a prosecutor’s overdependence on asset forfeiture to fund his or her office. There have in recent years been several exposés in the news about some police departments across the country adopting highly questionable asset forfeiture practices because those departments have come to depend on asset forfeiture as a source of revenue. The same sort of perverse incentive can arise for a prosecutor obtaining funding from debt collection agencies.

Whether or not we label this a “conflict of interest” under the Model Rules, the problem of a substantial threat to professional judgment arising from reliance on money from debt collectors raises a serious objection to the practice. The nature of the financial arrangement between the prosecutor’s office and the debt collector is one in which there are perverse incentives to not monitor the debt collectors and to forgo prosecution in some cases that might well merit prosecution in order to keep money flowing to the debt collectors and to the prosecutor’s coffers.

Competence. Prosecutors’ completely turning over the handling of debt collection cases to private debt collection agencies raises significant competence issues. Model Rule 1.1 requires a lawyer to provide competent representation, which “requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” To understand the competence issues raised by the sale of letterhead to debt collectors, it is helpful to examine two different facets of prosecutorial decision making at the outset of a case: the powers to (1) threaten legal action and (2) decline prosecution. In regard to the first power, the lawyers in the prosecutor’s office should be deciding and screening which debtors should and should not be threatened with criminal legal action. Prosecutors who sell their letterhead to debt collectors violate the duty

of competence by abdicating their responsibility to do this and letting the debt collectors decide who should be threatened. In regard to the second power, the lawyers in the prosecutor's office should be deciding which cases involving conduct such as bad check writing prosecution should be declined. Again by turning over such decisions to the debt collectors, they fail to competently exercise an important power of their office.

Competent exercise of the power to threaten criminal prosecution and the power to decline prosecution requires diligent screening by the prosecutor's office of those debtors who are suitable for referral to debt collection rather than prosecution, and monitoring of the debt collector's practices, including the content of the demand letters and other steps taken to collect the debts. Anything short of this indicates a lack of thoroughness necessary for the representation of the government and the government's interests in the fair enforcement of the law.

Campaign Contributors Drafting Letters

Assisting in unauthorized practice of law. Unlike the use of official letterhead by debt collectors, attorneys general use of letters or other work produced by campaign contributors does not raise the unauthorized practice of law issue. Here, the attorney general is reviewing the work produced and adopting it. Even if the letter or other work is drafted by a nonlawyer, the attorney general is not assisting a nonlawyer in the practice of law because it is the attorney general, a lawyer, who is using the material. This is similar to a lawyer using work produced by a paralegal or law clerk.

Conflict of interest. Model Rule 1.7(a)(2) states that a conflict of interest exists when "there is a *significant risk* that the representation of one or more clients will be materially limited . . . by a *personal interest of the lawyer*" (emphasis added). Similarly, the Restatement (Third) of the Law Governing Lawyers section 121 defines a conflict of interest as occurring whenever there is a "*substantial risk*" that the lawyer's representation of a client will be "materially and adversely affected by the lawyer's own interests" (emphasis added). The Restatement explains that there must be a "significant and plausible" risk of adverse effect on the representation of the client. (*Id.*) In sum, both the Model Rules and the Restatement focus on the risk that various incentives may adversely affect a lawyer's representation of his or her client.

Attorneys general who garner campaign contributions by using work produced by lobbyists and campaign contributors run afoul of these conflict-of-interest rules. The conflict between the lawyer's

personal interest in raising money for his or her campaign and the obligations to his or her client, the state, in the fair enforcement of the law is obvious.

While it is accepted that persons running for attorney general often adopt various positions in order to generate both financial and electoral support for their campaigns, once in office as an attorney general the lawyer's obligation is to advance the interests of the state and not those of campaign contributors. The secretive nature of attorneys general using letters or other work produced by lobbyists and campaign contributors suggests that the attorneys general realize the risk of subordinating the interests of the state to those of their campaign contributors. That secrecy also increases the risk, because it makes monitoring the impact of campaign contributions on the attorney general's judgment more difficult.

Competence. Using letters and other work produced by lobbyists and campaign contributors also raises competence issues. When an attorney general uses drafts prepared by private parties and not lawyers in his or her office, it raises serious concern that the attorney general has failed to investigate and research the factual and legal merits of the position the attorney general is advancing as required by Model Rule 1.1.

Using the work of others outside of the attorney general's office also raises issues of diligence, as required by Model Rule 1.3. Diligence speaks to performing work for which an attorney is hired. In the case of using letters or other work supplied by persons outside of the attorney general's office, the duty of diligence would be violated if the attorney general did not ensure that the work adopted was accurate, relevant, and had a sound basis in law.

Conclusion

Prosecutors and attorneys general misuse of letterhead raises a number of ethical issues. The ABA Standing Committee's Opinion 469 should be a wake-up call for prosecutors who have entered, or who are considering entering, into agreements to sell their letterhead to debt collection agencies. The ethics opinion should also have the intended effect of curbing such agreements.

As this column outlines, attorneys general who misuse their letterhead by sending letters and other work product drafted by lobbyists and campaign contributors also engage in a practice that raises ethical concerns. Although there are no ethics opinions providing guidance, we believe that attorneys general should stop such practices before they proliferate and distort the normal operations of their offices. ■

Protecting Confidentiality of a Criminal Defendant's Litigation File

BY J. VINCENT APRILE II

When an appointed criminal defense attorney withdraws or is relieved as assigned counsel, should the assigning court be permitted to require the former attorney of record to transfer the client's litigation file to either the court clerk or the judge's chambers for safekeeping pending the appointment of replacement counsel? What are the responsibilities of the former defense attorney who has the client's litigation files in his or her possession when directed to turn over the client's files to a court clerk or a member of the judge's staff?

Although the court may be responsible for assigning defense counsel to represent the indigent accused, the court does not control the defense litigation file assembled on behalf of the client by appointed counsel. The custodian of the client's litigation file, even after counsel has withdrawn or been relieved, is the former attorney until a substitute or replacement counsel is assigned. In this regard, an indigent defendant's file should be treated the same way as the file of a defendant who has the wherewithal to retain a defense attorney. No court would, absent a request from the defendant, ordered a retained attorney who has ceased to represent the client to turn over the defense file to a third party until a new defense counsel entered an appearance in the case. Neither the court nor the clerk's office is a proper custodian of a defendant's litigation file.

Even though a retained defense attorney is discharged or withdraws from a case, that attorney remains the custodian of the client's litigation file until either the former client or successor counsel, with the consent of the client, requests the file. Ethics opinions from a number of jurisdictions emphasize the duty of the former attorney to maintain the litigation file as well as former counsel's obligation to provide the file upon request to either the

former client or successor counsel, with the client's consent. Even "[w]hen successor counsel enters a representation, prior counsel should still act to protect the client's privileges, confidences and secrets, and obtain consent (express or implied) from the client before providing such information to the new counsel." (STANDARDS FOR CRIMINAL JUSTICE: DEF. FUNCTION Standard 4-3.10(c) (4th ed. 2015).)

Does the transfer of the client's litigation file to either the court clerk's office or to the judge's office constitute a "disclosure" of or "unauthorized access" to confidential information? "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." (MODEL RULES OF PROF'L CONDUCT R. 1.6(c).) This provision "requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties." (MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 18.) The ethical obligation imposed is prophylactic in nature, requiring even appointed counsel to anticipate and take measures to prevent inadvertent or unauthorized disclosures of and access to confidential information, including the litigation file.

This ethical precept applies equally to former counsel, particularly one who has the client's litigation file in his or her possession. "The duty of confidentiality continues after the client-lawyer relationship has terminated." (MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 20.) As the guardian/custodian of a former client's file, counsel must assess the risks of, at the least, inadvertent/unauthorized disclosure of and/or unauthorized access to confidential information contained in the client's litigation file should that file be transferred to either the office of the clerk of the court or the court's chambers. Virtually all of the litigation file will be confidential. "The confidentiality rule . . . applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source." (MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 3.) This includes matters covered by the attorney-client privilege, the work product doctrine, and the ethical rule of confidentiality. Equally important, the prohibition against the disclosure of confidential information "also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person." (MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 4.) In this regard, "disclosure" and "access" should be read to include transfers of confidential files to third parties, despite a claim that the confidentiality of the file will be respected and protected by those third parties. The judge's staff and the clerk's staff are, for all practical purposes, third persons with regard to



J. VINCENT APRILE II retired after 30 years as a public defender with the Kentucky Department of Public Advocacy and joined Lynch, Cox, Gilman & Goodman, P.S.C., in Louisville, Kentucky, where he specializes in criminal law, both trial and appeal, employment law, and litigation. He is past-chair and current member of the editorial board of Criminal Justice magazine and a regular columnist. He is the recipient of the 2012 Louisville Bar Association's Distinguished Service Award.

the indigent defendant's litigation file. Under these circumstances, the risk of inadvertent/unauthorized disclosure or unauthorized access is appreciably increased for no legitimate reason.


When a client's litigation file is stored, even temporarily, in either the clerk's office or the judge's office, that file no longer has a custodian who is ethically required to protect the confidentiality of the file against even inadvertent disclosure or unauthorized access. Many types of materials are routinely stored in either the clerk's office or the judge's chambers that are not confidential in nature and do not require protection against unintentional disclosure or unauthorized access. This factor alone increases the possibility of inadvertent/unauthorized disclosure or unauthorized access when a litigation file is stored in either of those places.

Contrast that situation with the former appointed counsel retaining the client's file in his or her office until successor counsel or the client requests it. The risk of inadvertent disclosure or unauthorized access remains negligible in this scenario. An attorney appointed to represent an indigent defendant has an additional ethical duty in this situation. "A lawyer shall not accept compensation for representing a client from one other than the client unless . . . information relating to representation of a client is protected as required by Rule 1.6." (MODEL RULES OF PROF'L CONDUCT R. 1.8(f).) As a result, an attorney accepting an appointment as assigned counsel must be guaranteed that the administration of the public defender program, even when performed by a judge, will not undermine counsel's ethical obligation to protect the confidentiality of the indigent client's litigation file.

"A lawyer may be ordered to reveal information relating to the representation of a client by a court or by another tribunal . . . claiming authority pursuant to other law to compel the disclosure." (MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 15.) This would appear to fit the situation created by a trial judge ordering a former assigned counsel to turn over the client's litigation file to the court clerk or a member of the court's staff, even though the judge is not specifically ordering confidential information to be disclosed or accessed. "Absent informed consent of the client to do otherwise, the lawyer should assert on behalf of the client all nonfrivolous claims that the order is not authorized by other law or that the information sought is protected against disclosure by the attorney-client privilege or other applicable law." (*Id.*) The former assigned counsel would be ethically compelled in this instance to raise all colorable claims against the transfer, absent informed consent from the former client to do otherwise. "The provisions of this [confidentiality] Rule are for the protection of former clients and can be

waived if the client gives informed consent" (MODEL RULES OF PROF'L CONDUCT R. 1.9 cmt. 9.)

When a former assigned attorney still has possession of the client's file, that attorney has standing on behalf of his or her former client to challenge the order requiring counsel to turn over the file to a third party, even though counsel no longer represents the defendant in the case. In that situation, counsel should determine whether the former client objects to this transfer after being fully advised of the potential risks of acquiescing to the transfer order. "A fundamental principle in the client-lawyer relationship is that, *in the absence of the client's informed consent*, the lawyer must not reveal information



CELEBRATING
30Years

**30th Annual National Institute
on White Collar Crime**

March 2-4, 2016

Marriott Marquis
San Diego Marina
San Diego, CA

**General & Ethics/Professional
CLE available**

<http://tinyurl.com/oox6row>

relating to the representation.” (MODEL RULES OF PROF’L CONDUCT R. 1.6 cmt. 2 (emphasis added).) This applies equally to former counsel.

The indigent defendant’s former attorney lacks the authority to allow a third party access to a former client’s confidential information *without the client’s informed consent*. “‘Informed consent’ denotes the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct.” (MODEL RULES OF PROF’L CONDUCT R. 1.0(e).)

The attorney-client privilege belongs to the client, not the attorney. (*Hunt v. Blackburn*, 128 U.S. 464, 470 (1888).) The attorney cannot waive the attorney-client privilege except with the consent of the client. Similarly, counsel cannot waive the work product privilege without the client’s consent.

Former counsel may wish to provide the court ordering the transfer of the files with a signed and dated written statement by the client that, after being advised by former counsel, the accused does not consent to the transfer of the litigation files as ordered by the court.

Even assuming the former assigned counsel has been discharged by the court for unethical or otherwise improper conduct in the case, is it appropriate for the judge to order the former attorney to turn over the client’s litigation files to either the clerk’s office or the judge’s staff? Here again the answer should be no. Instead, the judge should immediately appoint, albeit only temporarily, an attorney to receive the litigation file and to safeguard its confidentiality until appointment of permanent replacement counsel, who can then request the file from the lawyer “safekeeping” the file. Laments that temporarily assigning an attorney to perform this function will be an unnecessary expense should be readily discounted. An indigent defendant should have continuous representation once assigned counsel has been initially provided—even if that interim counsel will have little to do pending the appointment of substitute counsel—not only to assume possession of the litigation file, but also to be available to the defendant should an emergency arise.

What is the impact on an indigent defendant when informed by court order that his or her former defense attorney must transfer the client’s litigation file to the court clerk or the judge’s office until a replacement counsel is assigned? The indigent defendant will undoubtedly be concerned that any information in that file, whether adverse or beneficial to the defense, will be available to someone other than a defense attorney representing the client’s best interests. The impression generated by this approach is one that is incompatible with the

integrity of the judicial process. The temporary possession of the defense litigation file by a third party, even though ordered by the court, will always raise questions as to whether the confidentiality of that file was breached, either inadvertently or without proper authorization, during the period the file was not in the hands of the defendant’s counsel, whether present or former counsel.

A counsel who is no longer representing an indigent defendant and who is in possession of that client’s litigation file has an ethical obligation to resist a court order directing counsel to transfer that file to a third party, such as the court clerk or the judge’s office, for safekeeping, pending the appointment of a new attorney to represent the defendant. A criminal defense attorney, not a third party, should be the custodian of the defense litigation file at all times because of the attorney’s continuing ethical obligations to safeguard the confidentiality and integrity of that file. That remains true even when the defendant is an indigent represented by appointed counsel. ■

ANTS

(continued from page 29)

are frustrated that their orders have failed. Most important, people who were counting on the fresh start promised by the expungement procedure are frustrated, and may have experienced a major life setback as a result. But eliminating a criminal case is the best remedy for people who have paid their debts to society and no longer present heightened risk of criminal behavior. If the case is not known, then employers, landlords, and others need not be relied upon to apply the law properly or use sound discretion when evaluating that case. We can, and should, be prepared to deal with the background screeners who must be brought into line to avoid undermining the efficacy of this crucial remedy for people who are trying to put their lives back on track. ■

Eighth Annual Fall Institute and CJS Fall Meetings

BY RABIAH BURKS AND KYO SUH

The ABA Criminal Justice Section's 8th Annual Fall Institute was held on October 23, 2015, at Loews Madison Hotel in Washington, D.C. This year's institute was titled "Criminal Justice in the 21st Century: Calibrating the Scales of Justice" and explored a range of topics including surveillance technology and the law, wrongful convictions, the role of judges in criminal justice, and the media's role in criminal justice policy.

US Rep. Steve Cohen (D-TN) provided opening remarks, and ABA President Paulette Brown spoke during the Inaugural Criminal Justice Section Awards Luncheon. CJS Fall Meetings, held at the hotel and the ABA's D.C. offices, included Council and various committee meetings.

The Inaugural CJS Awards Luncheon

The Inaugural Criminal Justice Section Awards Luncheon was held during the 8th Annual Fall Institute on October 23, 2015, in Washington, D.C. The five Criminal Justice Section awards were presented to the following recipients:

Charles R. English Award: Ronald Goldstock, Commissioner, Waterfront Commission of New York Harbor, Larchmont, NY;

Frank Carrington Crime Victim Attorney Award: Lenore Anderson, Executive Director, Californians for Safety and Justice, Oakland, CA;

Livingston Hall Juvenile Justice Award: Mark Friedenthal, Assistant Public Defender, Office of the Public Defender, Baltimore, MD;

Raeder-Taslitz Award: Professor James Coleman, Duke University School of Law, Durham, NC; and

Norm Maleng Minister of Justice Award: Pearl Kim, Assistant District Attorney, Office of the District Attorney, Delaware County, Media, PA.

RABIAH BURKS is the senior public relations specialist for the Criminal Justice Section and editor of the Leadership Connection; contact her at rabiah.burks@americanbar.org.

KYO SUH is the technology and publications manager for the Criminal Justice Section; contact him at kyo.suh@americanbar.org. Both are regular columnists for Criminal Justice magazine.

Fourth International White Collar Crime Institute

The ABA Criminal Justice Section's Fourth International White Collar Crime Institute was held October 12–13, 2015, at the Law Offices of Berwin Leighton Paisner (Adelaide House) in London, UK.

The conference featured topflight legal practitioners from around the globe tackling such topics as corporate espionage and cybercrimes, tax prosecution and money laundering, extradition, and public corruption and FCPA issues.

Lord Alex Carlile CBE QC, a member of the House of Lords, spoke as the luncheon keynote speaker. Lord Carlile served as a Liberal Democrat member of Parliament from 1983 to 1997. He was the independent reviewer of terrorism legislation between 2001 and 2011 and has a strong interest in cyber-related issues, especially regarding national security.

The opening session featured a discussion on "Monitors: Ensuring Compliance When You Need It Most!" with former US Deputy Attorney General James M. Cole and independent compliance monitor Michael Cherkasky. The session was moderated by Judge Bernice B. Donald, ABA Criminal Justice Section chair.



A panel from the Fourth International White Collar Crime Institute in London, Oct. 12–13, 2015.

Visit the ABA
Criminal Justice Section website

www.americanbar.org/crimjust

for the latest Section news and
updates, upcoming events, new
resources, and project information.

Southeastern White Collar Crime Institute

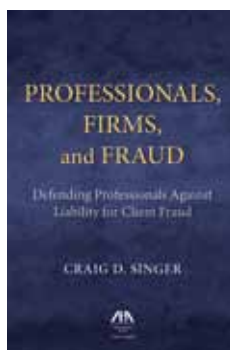
The ABA Criminal Justice Section hosted the Southeastern White Collar Crime Institute on September 10–11, 2015, in Braselton, Georgia, near Atlanta. The conference featured expert panelists and speakers who delved into topics such as the effective use of criminal discovery, litigating prosecutorial conduct, Supreme Court updates and other developments in criminal law, law enforcement initiatives, sentencing issues in economic crimes, and white collar criminal enforcement. James Cole, former US deputy attorney general, discussed his experiences with the Department of Justice in the area of white collar crime.

NEW BOOKS

Professionals, Firms, and Fraud: Defending Professionals against Liability for Client Fraud

By Craig D. Singer

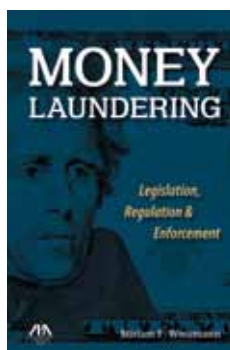
This book surveys the law regarding claims and defenses that commonly arise in a client fraud scenario. It focuses on identifying some of the most promising defenses and other strategies to help professional firms minimize the fallout from such events. Each of the chapters is devoted to claims against professionals of a discrete type or from a distinct source.



Money Laundering: Legislation, Regulation, and Enforcement

By Miriam F. Weismann

This book provides an updated and comprehensive review of the subject of anti-money laundering activity. The text is designed to organize and simplify (to the extent possible) the explanation of the laws, regulations, and salient cases. The book also examines the role of the regulatory agencies, US Department of Justice prosecution policies, most common methods of money laundering, and how legitimate financial institutions, in concert with other professionals, facilitate the practically open and notorious operation of money laundering activities. ■



From left: Chair-Elect Matt Redle, Chair Judge Bernice Donald, Keynote Speaker US Rep. Steve Cohen, First Vice Chair Sandy Weinberg at the 8th CJS Fall Institute, Oct. 23, 2015, in Washington, D.C.

UPCOMING EVENTS

National Institute on White Collar Crime

March 2–4, 2016

San Diego, CA

CJS Spring Meeting

April 28–May 1, 2016

Albuquerque, NM

CJS Programs & ABA Annual Meeting

August 5–7, 2016

San Francisco, CA

7th Annual Prescriptions for Criminal

Justice Forensics

June 3, 2016

New York, NY

Southeastern White Collar Crime Institute

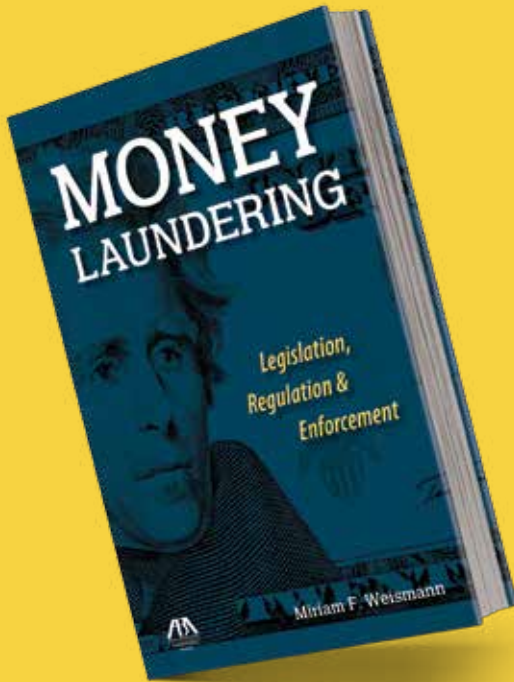
Sept. 8–9, 2016

Braselton, GA (near Atlanta)

5th International White Collar Crime Institute

Oct. 10–11, 2016

London, UK



MONEY LAUNDERING

Legislation, Regulation, and Enforcement

By Miriam F. Weismann

Given the complexity of domestic and global money laundering schemes and networks and the laws designed to prevent and detect it, it's more difficult than ever for practitioners, courts, and scholars to manage the scope of the available information.

Money Laundering is designed to organize and simplify the explanation of the laws, regulations, and salient cases surround this ever-expanding criminal area of activity. The book also examines the role of the regulatory agencies, U.S. Department of Justice prosecution policies, most common methods of money laundering and how legitimate financial institutions, in concert with other professionals, may facilitate such activities.

2014 • 6 x 9 • 293 PAGES
PRODUCT CODE: 5090152
\$74.95 REGULAR
\$69.95 ABA MEMBER
\$59.95 CJ SECTION MEMBER

Topics covered in depth:

- \$ Bank Secrecy Act
- \$ The USA Patriot Act
- \$ Money Laundering Crimes and Criminal Penalties
- \$ Role of Government Agencies and Advisory Organizations
- \$ Information Sharing Among Financial Institutions and Law Enforcement
- \$ Global Enforcement Cooperation Measures

**To order, call the
ABA Service Center
at (800) 285-2221 or
visit our website at
www.ShopABA.org.**

A must-have for federal and state prosecutors looking to build a criminal case, whistleblowers and their attorneys, and criminal defense attorneys, this book is an excellent resource for those involved in cases raising issues regarding the transfer of funds and compliance efforts to meet the growing demands to adhere strictly to the law.

AMERICAN BAR ASSOCIATION

www.ShopABA.org
Phone: 1-800-285-2221
Fax: 1-312-988-5568

Publication Orders
P.O. Box 10892
Chicago, IL 60610





INTERNATIONAL SOCIETY FOR THE REFORM OF CRIMINAL LAW

PROTECTING PRIVACY - DOMESTIC AND INTERNATIONAL CRIMINAL JUSTICE RESPONSES TO CRIMES AGAINST PERSONAL PRIVACY AND THE BALANCE BETWEEN INDIVIDUAL PRIVACY AND COLLECTIVE SECURITY

**July 24 – 28th, 2016
Halifax Convention Centre
Halifax, NS, Canada**

Conference Chairs

Hon. Justice Thomas Cromwell
Supreme Court of Canada
Ottawa, ON, Canada

Hon. Chief Justice Michael MacDonald
Nova Scotia Court of Appeal
Halifax, NS, Canada

Conference Theme

This conference will examine and promote discussion and debate of the challenges that privacy concerns and technological change pose to international and national criminal justice systems. The key question is how the criminal justice system can properly respond to the competing demands of privacy, law enforcement effectiveness and national security. Topics to be addressed include: international cooperation in the fight against cybercrime; the human rights implications of sharing personal information and other intelligence across national borders; the boundaries of surveillance, search and seizure; the scope and place of privacy as a human right and as a limit on state investigative and intelligence activities; the collection, use and potential abuse of personal data; and the implications of intrusions into privacy for the exercise of democratic rights.

International Society for the Reform of Criminal Law
#1000 – 840 Howe St
Vancouver, BC, Canada
V6Z 2M1
secretariat@isrcl.com

For more information please visit www.isrcl.com or email north@allard.ubc.ca

AGREEMENT CONCERNING BULK DISTRIBUTION OF ELECTRONIC CASE
RECORD INFORMATION ON RECURRING BASIS

This AGREEMENT made this _____ day of _____, 20__ is entered into by the Administrative Office of Pennsylvania Courts (“AOPC”) of the Unified Judicial System (UJS) of the Commonwealth of Pennsylvania, with offices at 5035 Ritter Rd, Suite 700 Mechanicsburg, Pennsylvania, 17055, hereinafter called the “COMMONWEALTH” and _____ (“SUBSCRIBER”).

The purpose of this AGREEMENT is to establish the terms and conditions under which the COMMONWEALTH agrees to provide the SUBSCRIBER with a recurring bulk distribution of electronic case record information.

Terms and Conditions of AGREEMENT

1. DEFINITIONS.

- A. “CPCMS” means the Common Pleas Criminal Court Case Management System.
- B. “Electronic Case Record” means information or data created, collected, received, produced or maintained by a court or office in connection with a particular case that exists in the PACMS, CPCMS, or MDJS and is provided in response to bulk distribution requests, regardless of format.
- C. “MDJS” means the Magisterial District Judge Automated System.
- D. “PACMS” means the Pennsylvania Appellate Courts Case Management System.
- E. “Request for Bulk Distribution of Electronic Case Records” means any request regardless of the format the information is requested to be received in, for all or a subset of electronic case records that is releasable to the public pursuant to the provisions of the *Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania*.

2. SERVICES.

- A. The COMMONWEALTH will provide SUBSCRIBER with electronic case record information from the PACMS, CPCMS and/or MDJS consistent with the provisions of the *Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania*.
- B. For those SUBSCRIBERS receiving electronic case record information from the CPCMS and/or MDJS, the COMMONWEALTH will provide a LifeCycle file on a weekly basis which SUBSCRIBER shall use as described in Section 3(b) and (c).

- C. When the electronic case record information is requested in electronic media, the COMMONWEALTH shall, in its sole discretion, determine the appropriate format.
- D. The COMMONWEALTH specifically reserves the right, in its sole discretion and at any time without prior notice, to make any changes it deems appropriate relating to the information and data provided under this AGREEMENT. Such changes include, but are not limited to altering the format of the information, file structures, display changes, operating hours, computer programs and network services.
- E. Recent entries made in the court filing offices may not be immediately reflected in the electronic case record information provided. Neither the courts of the COMMONWEALTH nor the COMMONWEALTH assumes any liability for inaccurate or delayed data, errors or omissions. Electronic case record information should not be used in place of a criminal history background check, which can only be provided by the Pennsylvania State Police. Employers who do not comply with the provisions of the Criminal History Record Information Act (18 Pa.C.S. § 9101 et seq.) may be subject to civil liability in 18 Pa.C.S. § 9183.

3. OBLIGATIONS OF SUBSCRIBER.

- A. SUBSCRIBER shall notify its users, customers, clients or other third party recipients that the electronic case record information received from the COMMONWEALTH is not an official case record; official case records are maintained by the court in which the record was filed.
- B. SUBSCRIBER shall retrieve and access the appropriate LifeCycle file(s) created by AOPC on a weekly basis and update their data accordingly. Each file will contain a list of CPCMS or MDJS cases that must be removed from subscriber data in order for the same to remain current and up to date. Therefore, subscribers of only CPCMS information will need to retrieve and access the CPCMS LifeCycle file. However, subscribers of CPCMS and MDJS information will need to retrieve and access two LifeCycle files, one for each system: CPCMS and MDJS. The MDJS LifeCycle files will be located at: <ftp://common.pacourts.us> (Directory: SEMIPRIVATE/ACTIONS/LIFECYCLE/MDJS/WEEKLY/PUBLISH). The CPCMS LifeCycle files will be located at: <ftp://common.pacourts.us> (Directory: SEMIPRIVATE/ACTIONS/LIFECYCLE/CPCMS/WEEKLY/PUBLISH).
- C. SUBSCRIBER agrees to promptly comply with all COMMONWEALTH instructions and directions concerning the electronic case record information provided, including the LifeCycle files. Failure to comply may result in immediate termination of this AGREEMENT.

- D. SUBSCRIBER shall timely make all payments due to the COMMONWEALTH in accordance with Section 5.
- E. In the event of termination of this AGREEMENT, SUBSCRIBER agrees to immediately stop all use of the electronic case record information that has been provided by the COMMONWEALTH, including LifeCycle files, remove all such data from its databases, notify its users, customers, clients or other third party recipients to stop using the data, and ensure that users, customers, clients or other third party recipients remove the data from their databases.
- F. The SUBSCRIBER agrees to provide the following disclosure statement to each user, customer, client or other third party recipient at the time any electronic case information is provided. The SUBSCRIBER shall ensure that the following statement is displayed or provided every time electronic case information is provided:

"The data or information provided is based upon information received by the Administrative Office of Pennsylvania Courts ("AOPC"). AOPC makes no representation as to the accuracy, completeness or utility, for any general or specific purpose, of the information provided and as such, assumes no liability for inaccurate or delayed data, errors or omissions. Use of this information is at your own risk. AOPC makes no representations regarding the identity of any persons whose names appear in the records. User should verify that the information is accurate and current by personally consulting the official record reposing in the court wherein the record is maintained."

- G. The SUBSCRIBER agrees to provide the COMMONWEALTH with a list of all the SUBSCRIBER'S websites, subsidiaries, affiliates, customers, clients and other third party recipients that use or distribute information obtained from the COMMONWEALTH, and all other names which the SUBSCRIBER uses in the course of doing business. The SUBSCRIBER agrees to update this list and send it to the COMMONWEALTH within thirty (30) days of any change.
- H. The SUBSCRIBER shall delete any electronic case record information that is inadvertently included in the data or information provided by the COMMONWEALTH and is excluded from public access under Section 3.00 of the *Electronic Case Record Public Access Policy of the Unified Judicial System of Pennsylvania*. A copy of this policy is attached. The SUBSCRIBER shall take other appropriate action to ensure that such electronic case record information is not disclosed to others.
- I. The SUBSCRIBER shall designate a Contract Administrator who shall be the sole point-of-contact with regard to all contractual matters.

4. AUDITS

- A. The COMMONWEALTH may, at its discretion, perform audits of the SUBSCRIBER to verify compliance with the terms and conditions of this AGREEMENT and the appropriate use of the information and data provided by the COMMONWEALTH. The SUBSCRIBER agrees to cooperate with the COMMONWEALTH in the event of such an audit.
- B. SUBSCRIBER agrees to provide the COMMONWEALTH with access at no charge to any database created using the data or information from the electronic case record information as well as an online account for the SUBSCRIBER'S service with valid user logon identifiers and passwords for the purposes of monitoring and auditing contract compliance. SUBSCRIBER shall also provide to the COMMONWEALTH copies of materials and information that SUBSCRIBER provides its subscribers, customers, clients or other third parties.

5. FEES

- A. SUBSCRIBER agrees to pay all amounts due under this AGREEMENT, as described in "Attachment A – Fees", as appended to this AGREEMENT. The schedule of fees in Attachment A is subject to change. SUBSCRIBER will be provided at least thirty (30) days' notice before the effective date of any change in fees.
- B. The COMMONWEALTH may terminate service, without notice, to SUBSCRIBER if SUBSCRIBER'S account is overdue.

6. LIMITATION OF LIABILITY

- A. SUBSCRIBER acknowledges and accepts that all information and data provided under this AGREEMENT may be subject to error or omission and correspondingly agrees that the COMMONWEALTH and the courts of the Unified Judicial System of the Commonwealth of Pennsylvania shall not be responsible or liable in any way whatsoever for the accuracy and completeness of any data provided or for the use of the information or data provided. Specifically:
 - i. The COMMONWEALTH and the courts of the Unified Judicial System of the Commonwealth of Pennsylvania shall not be liable for any demand or claim, regardless of form of action or venue thereof, for any damages resulting from the use of any information, data or other materials provided under this AGREEMENT.

- ii. THE COMMONWEALTH and the courts of the Unified Judicial System of the Commonwealth of Pennsylvania shall not be liable for any demand or claim, regardless of form of action or venue thereof, for any damages arising from incorrect or incomplete information or data provided under this AGREEMENT.
- iii. THE COMMONWEALTH and the courts of the Unified Judicial System of the Commonwealth of Pennsylvania shall not be liable to SUBSCRIBER or any other party for any loss, including revenue, profits, time, goodwill, computer time, destruction, damage or loss of data, or any other indirect, special, or consequential damage which may arise from the use, operation, or modification of data provided under this AGREEMENT.

- B. THE COMMONWEALTH provides no warranties, express or implied, including the implied warranty of fitness for a particular purpose, that the information or data provided under this AGREEMENT is accurate, reliable, timely or complete. It is expressly understood by the parties that it is SUBSCRIBER'S responsibility to verify information or data obtained through this AGREEMENT with official court information reposing at the court where the official case records resides.
- C. Personal liability. No official, director, officer, agent or employee of the COMMONWEALTH or the courts of the Unified Judicial System of the Commonwealth of Pennsylvania shall be charged personally or held personally liable to SUBSCRIBER under any term or provision of this contract because of any breach hereof or because of its execution, approval or attempted execution.

7. WARRANTIES.

- A. THE COMMONWEALTH provides the electronic case record information as is.
- B. Use of this information is at the risk of the requestor.
- C. The COMMONWEALTH makes no representation as to the accuracy, completeness or utility, for any general or specific purpose, of the information provided and as such, assumes no liability for inaccurate or delayed data, errors or omissions.
- D. The electronic case record information contained in the PACMS, CPCMS and MDJS is not supported by fingerprints. Therefore, it should not be used for the purpose of linking cases to specific individuals.

- E. THE COMMONWEALTH provides no warranties of any kind or nature, express or implied, in connection with the services the COMMONWEALTH provides pursuant to this AGREEMENT including that the service will be uninterrupted.

8. TERMINATION

- A. Either party by written notice may immediately terminate this AGREEMENT, PROVIDED that if the SUBSCRIBER'S account is overdue, the COMMONWEALTH may terminate the SUBSCRIBER'S service without notice.
- B. COMMONWEALTH may terminate this AGREEMENT at any time without notice and penalty, if the COMMONWEALTH determines that such termination is in the COMMONWEALTH'S best interest.
- C. In the event that the COMMONWEALTH terminates this AGREEMENT, the COMMONWEALTH will have any remedy available to it under law or equity.
- D. In the event of termination of this AGREEMENT and should subscriber wish to re-subscribe, SUBSCRIBER will be required to sign the then-current version of the Agreement Concerning Bulk Distribution of Electronic Case Record Information on Recurring Basis and pay any outstanding balance in order to resume service.

- 9. ASSIGNMENT. SUBSCRIBER shall not assign or transfer any interest in this AGREEMENT without prior written approval of the COMMONWEALTH. The COMMONWEALTH reserves the right to assign or transfer the AGREEMENT to any person, office or entity under the control of the COMMONWEALTH, as it deems appropriate or as ordered by the Commonwealth of Pennsylvania.

- 10. SURVIVAL. The provisions of Paragraphs 3, 4(a), 5, 6, and 7 of this AGREEMENT shall survive the termination of this AGREEMENT.

- 11. SEVERABILITY. If any provision of this AGREEMENT, or application thereof to any person or circumstance, is held to be invalid, such invalidity shall not affect other provisions or applications of this AGREEMENT which can be given effect without the invalid provision or application, and to this end the provisions of this contract are severable.

- 12. WAIVER. No term or provision hereof shall be deemed waived and no breach or default excused by the COMMONWEALTH unless such waiver or consent shall be in writing. Any consent by the COMMONWEALTH to, or waiver of breach or default by the SUBSCRIBER, whether express or implied shall not

constitute consent to, waiver of, or excuse for any different or subsequent breach or default.

13. **GOVERNING LAW.** This AGREEMENT shall be interpreted, construed, and enforced in accordance with the laws of the Commonwealth of Pennsylvania. In the event of any conflict between the laws of the Commonwealth of Pennsylvania and any provision of this AGREEMENT, the laws of the Commonwealth shall automatically preempt such provisions in this contract and become a part of this AGREEMENT, fully binding on the parties hereto. Venue and jurisdiction for any disputes arising under this Agreement shall lie in Pennsylvania.
14. **INDEMNIFICATION.** SUBSCRIBER agrees to indemnify, defend and hold harmless the COMMONWEALTH its agents, officers and employees; and the Unified Judicial System of Pennsylvania, its agents, officers and employees from all claims, suits, or actions of whatever nature resulting from or arising out of the activities of the SUBSCRIBER or its officers, employees, subcontractors, agents, clients or customers under this AGREEMENT.
15. **SUBSCRIBER INFORMATION**

Subscriber's Name: _____
Business Name: _____
Contract Administrator: _____
Technical Contact: _____
Address: _____
City, State, ZIP: _____
Phone Number: _____
Fax Number: _____
Email Address: _____
16. **ENTIRE AGREEMENT.** This AGREEMENT contains the entire AGREEMENT between the parties. No amendment or modification changing its scope or terms has any force or effect unless it is in writing and signed by all parties to the AGREEMENT with the exception of periodic fee changes set forth in Attachment A.
17. **RETURN OF CONTRACT.** Failure to sign and return this contract within fifteen (15) days of receipt will result in withdrawal of approval and denial of this request.
18. **AVAILABILITY OF STATE FUNDS.** The performance of COMMONWEALTH'S duties under this AGREEMENT is subject to the availability of State Funds to enable it to perform those duties.
19. The COMMONWEALTH shall designate a Contract Administrator, who shall be the single authority to act for the COMMONWEALTH under this contract.

Whenever the COMMONWEALTH is required by terms of the contract to provide written notice to the SUBSCRIBER, such notice must be signed by the Contract Administrator, or in that individual's absence, or inability to act, such notice shall be signed by the Contract Administrator's designee.

IN WITNESS WHEREOF, this AGREEMENT has been executed by and on behalf of the parties hereto, the date and year first written above.

Accepted by:

ADMINISTRATIVE OFFICE OF PA COURTS
(COMMONWEALTH)

SUBSCRIBER

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

Summary of Application of Fair Credit Reporting Act (“FCRA”) to Criminal Background Checks

**By: Sharon M. Dietrich
Community Legal Services, Inc., Philadelphia, PA**

Where a criminal record report is provided to an employer by a credit reporting agency (“CRA”), the Fair Credit Reporting Act (“FCRA”), 15 U.S.C. § 1681 *et seq.*, is applicable. See Beaudette, FTC Informal Staff Opinion Letter, June 9, 1998 (attached and available at <http://www.ftc.gov/os/statutes/fcra/beaudett.htm>). FCRA creates obligations both on CRAs preparing criminal background reports and on employers using them.

Among the duties on CRAs compiling criminal background reports for employers are the following.

- CRAs may not report arrests or other adverse information (other than convictions of crimes) which are more than seven years old, provided that the report does not concern employment of an individual who has an annual salary that is \$75,000 or more.¹ 15 U.S.C. §§ 1681c(a)(5), 1681c(b)(3).
- CRAs must use “reasonable procedures” to insure “maximum possible accuracy” of the information in the report. 15 U.S.C. §1681e(b).

Elements of cause of action: (1) Inaccurate information in report; (2) inaccuracy due to CRA’s failure to follow reasonable procedures to assure maximum possible accuracy; (3) consumer suffered injury (can include emotional injury); and (4) injury was caused by inaccurate entry. Crane v. Trans Union, 282 F.Supp.2d 311 (E.D. Pa. 2003)(Dalzell) (citing Philin v. Trans Union Corp., 101 F.3d 957, 963 (3d Cir. 1996)).

- A CRA reporting public record information for employment purposes which “is likely to have an adverse effect on the consumer’s ability to obtain employment” must either notify the person that the public record information is being reported and provide the name and address of the person who is requesting the information at the time that the information is provider to the user or the CRA must maintain strict procedures to insure that the information it reports is complete and up to date. 15 U.S.C. §1681k.

¹ For many years, the seven year limit also applied to reporting of convictions. However, this seven year limit was eliminated by Congress in the Consumer Reporting Employment Clarification Act of 1998, P.L. 105-347, Sect. 5. Note that several states have credit reporting laws that retain limitations on the length of time during which convictions can be considered (most notably, New York and Massachusetts).

- If the completeness or accuracy of the information is disputed, the CRA must conduct a reasonable reinvestigation of the information within 30 days of receiving notice of the dispute and delete or modify the information if it is found to be inaccurate or incomplete or cannot be verified. 15 U.S.C. §1681i.

Among the duties that FCRA imposes when an employer uses a consumer report of a criminal record provided by a CRA for purposes of a hiring decision are the following.

- The employer must provide a clear written notice in a stand-alone document to the job applicant that it may obtain a consumer report. 15 U.S.C. § 1681b(b)(2). It also must obtain written authorization from the job applicant to get the report. 15 U.S.C. § 1681b(b)(2). Therefore, in situations where a CRA is involved, ex-offenders ought to be made aware that their criminal record will be scrutinized, which often is not the case when criminal records are obtained directly by the employer from public sources.
- If the employer intends to take adverse action based on the consumer report, a copy of the report and a Federal Trade Commission (“FTC”) Summary of Rights must be provided to the job applicant before the action is taken. 15 U.S.C. § 1681b(b)(3). The obvious reason for this requirement is to permit a job applicant to address the report before an employment decision is made. If this requirement were satisfied, ex-offenders would have a rare chance to check whether their criminal record were correctly reported and to address whether they would be suitable employees for the particular job notwithstanding their records.
- Afterwards, the employer, as a user of a consumer report, must notify the job applicant that an adverse decision was made as a result of the report and must provide, among other things, the name, address and telephone number of the CRA and the right to dispute the accuracy or completeness of the report. 15 U.S.C. § 1681m(a).

Updated, 8/16/2017