NW3C
National White Collar Crime Center

BJA
Bureau of Justice Assistance
U.S. Department of Justice

Global Justice Information Sharing Initiative

Association of State Criminal Investigative Agencies
ASCIA

National Fusion Center Association
NFCA
Helping Protect America

MS-ISAC

Federal Bureau of Investigation
IC3
Internet Crime Complaint Center

Law Enforcement Intelligence Units
LEIU
Founded 1956

IALEIA

Governor's
HOMELAND
SECURITY
Advisory
Council

Understanding Digital Footprints

2016

Steps to Protect Personal Information

A Guide for Law Enforcement

September 2016

Photo Credits: “59902745 copyright sashkin, 2016 used under license from Bigstockphoto.com”, “1830726 copyright PokerMan, 2016 used under license from Bigstockphoto.com”, “95561258 copyright ftotti1988, 2016 used under license from Bigstockphoto.com”

Global Advisory Committee (GAC)

The Global Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment.

The GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global Justice Information Sharing Initiative (Global). BJA engages GAC-member organizations and the constituents they serve through collaborative efforts, such as Global working groups, to help address critical justice information sharing issues for the benefit of practitioners in the field.

Criminal Intelligence Coordinating Council (CICC)

The Criminal Intelligence Coordinating Council supports development and promotion of resources for local, state, and tribal law enforcement and homeland security agencies in their efforts to capture and share criminal intelligence to better serve and protect communities nationwide.

Project Background

Cybercrime is an ever-growing issue for state, local, tribal, and territorial (SLTT) law enforcement. With advancements in technology, coupled with the oversharing of personal information, law enforcement not only needs to ensure the public's safety online but also be cognizant of the digital footprint that people are leaving behind.

This document provides material designed to assist law enforcement personnel in protecting themselves and their families from becoming cyber targets: protecting personal information, cyber dos and don'ts, and links to further cyber training and resources.

Introduction

Internet connectivity has become a large part of nearly everyone's daily routine. Whether through personal or professional use, this technology has been engrained in our society. With this connectivity, the amount of personal information made available to the general public has dramatically increased an individual's digital footprint.[1]

This personal information is enticing to those with malicious intent and can easily be acquired and used to target law enforcement personnel and their families. For example, the 2014 fatal shooting of Michael Brown by a police officer in Ferguson, Missouri,[2] brought widespread media coverage, and the actions surrounding the event led to the compromise of personal information[3] of law enforcement personnel in Ferguson and the surrounding area.

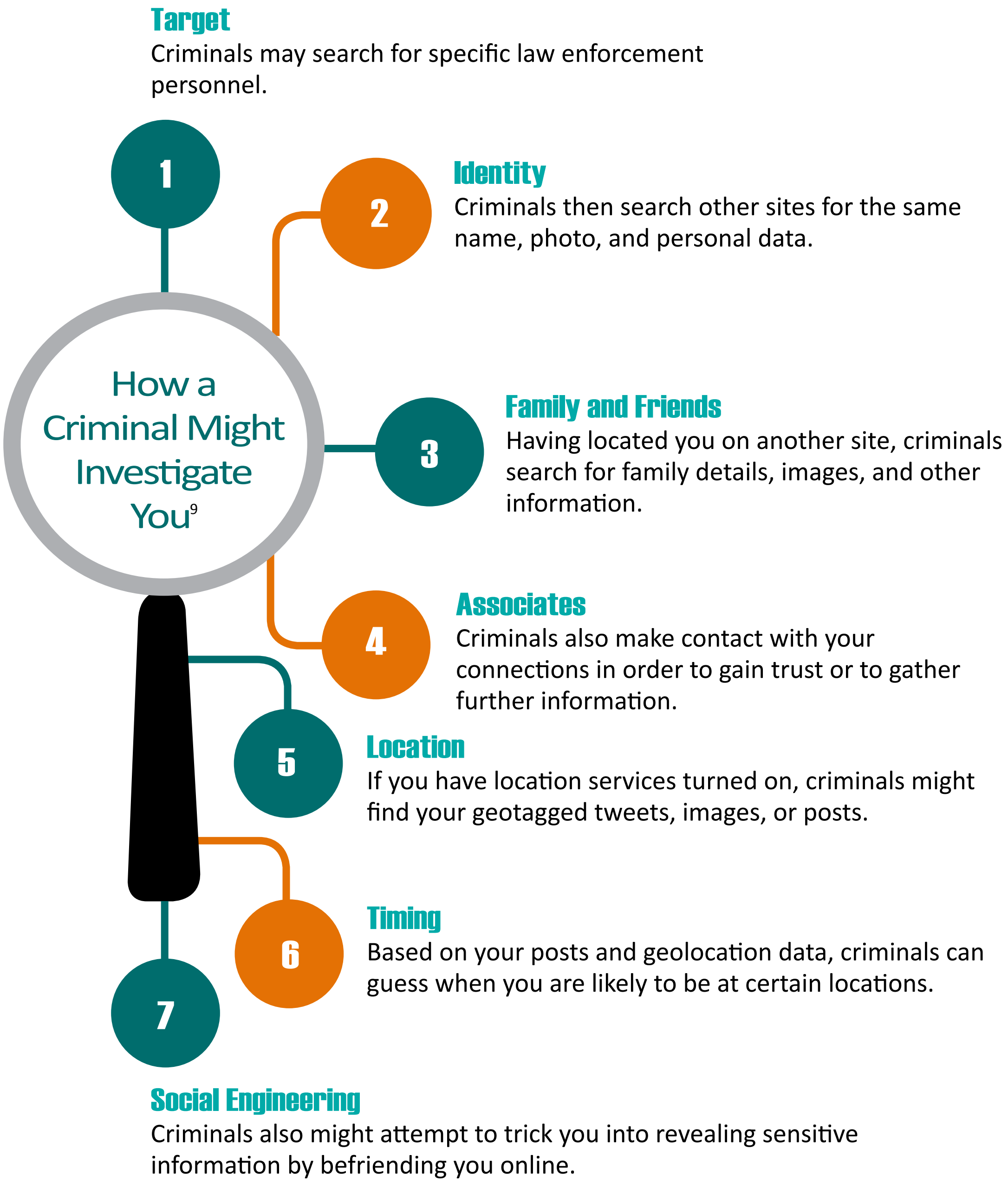
Another recent case example involved more than 30 Minnesota police officers whose personal information was exploited[4] by a hacker group affiliated with ISIS. The information included home and e-mail addresses and personal phone numbers. The names of the officers were posted along with a photo of masked ISIS fighters holding automatic weapons.

Personal information is increasingly distributed online by the media, the public, law enforcement agencies, and even law enforcement personnel themselves. It is imperative that law enforcement personnel understand the importance and consequences of their online activities and be proactive in monitoring and limiting their digital footprint. What may seem like an innocent upload or shared post can have a significant effect not only on law enforcement personnel but on their departments, families, and friends. Law enforcement should take the steps now to protect themselves and their family members before becoming a victim.

Think Before You Click

There are multiple areas in which personal information can be both collected and exposed on the Internet. Data brokers[5] such as PiPl®, Spokeo®, and White Pages® routinely compile comprehensive information from government and public records, such as court filings, real property, telephone directories, recorded liens and mortgages, marriage and death records, retailers, and social media platforms. In many cases, the information collected by these brokers may be out of date or inaccurate, adding additional safety concerns. The information from these brokers is sold or provided for free to anyone with an Internet connection.

Law enforcement personnel can easily make themselves, their families, coworkers, and agencies vulnerable by oversharing their personal information. One area of great concern is social media. With more than 1.6 billion active Facebook® users and more than 7,200 tweets being sent every second,[6] it is critical for law enforcement personnel to understand best practices for keeping their personal information safe and secure.[7] In general, individuals should follow strict privacy settings, maintain strong passwords, and utilize secure networks.



How a Criminal Might Investigate You[9]

1 **Target**
Criminals may search for specific law enforcement personnel.

2 **Identity**
Criminals then search other sites for the same name, photo, and personal data.

3 **Family and Friends**
Having located you on another site, criminals search for family details, images, and other information.

4 **Associates**
Criminals also make contact with your connections in order to gain trust or to gather further information.

5 **Location**
If you have location services turned on, criminals might find your geotagged tweets, images, or posts.

6 **Timing**
Based on your posts and geolocation data, criminals can guess when you are likely to be at certain locations.

7 **Social Engineering**
Criminals also might attempt to trick you into revealing sensitive information by befriending you online.

Doxing

Publicly releasing a person's identifying information, including full name, date of birth, address, phone numbers, and pictures typically retrieved from social networking site profiles.

—Federal Bureau of Investigation (FBI)

Becoming a Target

Individuals can scour the Internet for information such as home addresses, social security numbers, phone numbers, social media accounts, e-mail addresses, and photos.

This information is often easily obtained and posted on hosting sites and further disseminated via social media. This process, also known as **doxing** (also spelled doxxing), has become a popular method for targeting or distracting law enforcement. Doxing is a threat that can manifest itself in many dimensions and can extend the risk beyond the individual involved to include family members and relatives in what are known as blended attacks.[8] The blended-attack strategy often affects law enforcement on a personal level when perpetrators exploit and/or harass family members and friends.

Individuals who target law enforcement personnel or their families online use a variety of searching techniques. A simple search using a search engine such as Google® or Bing® can return numerous results that allow the perpetrator to identify and exploit other pieces of information. Perpetrators are also notorious for using social engineering techniques, befriending or following their targets on social media, which can allow direct access to the information they desire.

Example

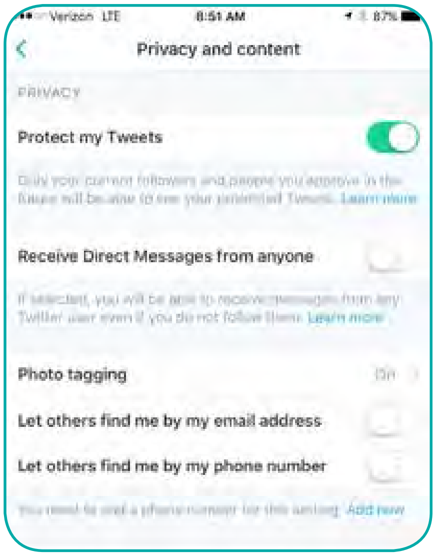
How a law enforcement officer’s information can be used for malicious purposes.

Following a search warrant executed on a suspect’s home, originating from a child exploitation investigation, the suspect began researching the lead investigator of the case online. The suspect set up a fake Gmail account under the guise of the lead investigator and began using the account to send e-mails containing explicit child pornography to recipients that included law enforcement officials and members of the media. The e-mails contained the lead investigator’s cell phone number and government e-mail address, which the perpetrator was able to find online. Upon further investigation handled by the FBI, the perpetrator admitted to sending the e-mails by using a friend’s laptop and free Wi-Fi access points. As a result, the suspect was sentenced to 120 months in prison and 10 years of supervised release for child pornography. In concluding their investigation, the FBI was able to clear the investigating officer of any wrongdoing.

Protecting Personal Information

The amount of personal information available online is astounding, and the process of redacting or removing that information is difficult and time-consuming. While there are resources[10] to help educate and assist law enforcement personnel and their families in accomplishing this task, there is no single solution.

One way to begin removing personal information is to identify and verify the sites where personal data is provided and follow their opt-out[11] procedures. These procedures can vary significantly: some require letters, some require photo identification, and others simply require completing an online form. Once the request to opt out has been identified and completed, individuals should ensure that their information has been removed. This is a continuous process in which individuals should routinely track their digital footprints[12] and review the amount of information available on themselves and their families.


Verizon LTE 8:51 AM 87%

Privacy and content

PRIVACY

Protect my Tweets ●

Only your current followers and people you approve in the future will be able to see your protected Tweets. Learn more

Receive Direct Messages from anyone ○

If selected, you will be able to receive messages from any Twitter user even if you do not follow them. Learn more

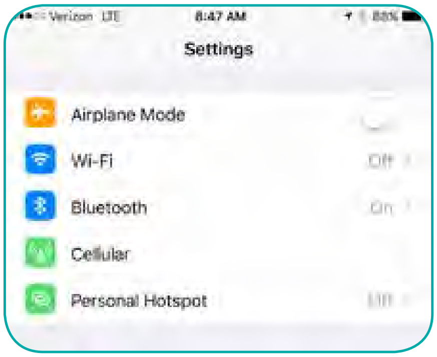
Photo tagging On

Let others find me by my email address ○

Let others find me by my phone number ○

You need to add a phone number for this setting. Add now

Screenshot of Twitter's Privacy Settings


Verizon LTE 8:47 AM 88%

Settings

Airplane Mode ○

Wi-Fi Off

Bluetooth On

Cellular

Personal Hotspot Off

Screenshot of iPhone settings

Many social media platforms have customizable privacy settings. Users should explore these settings and determine best practices for keeping their information secure. For example, Twitter®'s privacy settings allow users to disable location information related to their tweets as well as control who views their tweets. This is just one example of how individuals can keep their information secure.

Privacy settings often change with software and "app" updates, potentially exposing personal information during upgrades or when new features are added. It is imperative to recheck configuration settings after every operating system upgrade and installation to review what personal information (e.g., location and contacts) certain applications have access to when they are installed or upgraded.

Law enforcement personnel should ensure that their mobile devices are secure.[13] If a device has not been made secure, the data on the device could put law enforcement personnel, their families and friends, and their agencies at risk. Contacts, messages, photos, social media feeds, location data, and more can be derived from these devices, with devastating results if they are compromised. Simple solutions such as password protection, two-factor authentication, connecting to secure networks, allowing auto-updates for "apps" and software, and turning off Wi-Fi and Bluetooth when not in use can help prevent personal information from being compromised.

Physical security of mobile devices and personal networks is just as important. Law enforcement personnel and their family members should remain vigilant of those attempting to gain access, take preventive measures such as securing home Wi-Fi, and be conscious of those attempting to "shoulder surf" or use other observation techniques to collect information. Law enforcement personnel should also ensure that devices are protected with biometrics or a password, such as the pattern lock screen on Android devices or Touch ID on iPhones, and enable the lost device or remote tracking/wiping feature(s) and the automatic updates for apps and software on the device.

Law enforcement personnel should also be cognizant in securing internal and external storage devices (hard drives, thumb drives, memory cards, etc.). These devices can be secured either physically or through digital encryption.

In 2015, the International Association of Chiefs of Police (IACP) Computer Crime and Digital Evidence Committee (CCDE)[15] created a resource pertaining to officer safety and mitigating the risks of doxing. This video provides guidance for law enforcement personnel who are attempting to protect their personal information.

Click the image above to launch the IACP CCDE video in browser.[16]

Cyber Tips

The Dos and Don'ts[17]

Dos

- Use social media security settings
- Turn off location services
- Secure online profile data
- Create strong passwords
- Change your password regularly
- Use secure encrypted networks
- Use private browsing
- Use only approved devices and networks
- Enable remote tracking and wiping feature
- Keep systems and programs patched and up to date
- Use multifactor authentication when available for cloud-based and social media services

Don'ts

- Post personal details
- Use easily identifiable photos
- Allow apps to access your contacts or location
- Allow auto "check-in" to social feeds
- Use public WiFi for sensitive tasks
- Save payment information
- Share your passwords
- Leave devices logged on and unattended
- Open unexpected e-mails, links, or attachments
- Use identifiable information within a username or password

What If You Become a Victim?

After taking the necessary proactive steps to secure and limit personal information online, law enforcement personnel and their families still may be at risk of having their personal information compromised. If a compromise does occur, individuals can fall victim to identity theft, financial account takeover, false liens, and even offline harassment. Resources such as Identitytheft.gov[18] and IC3.gov[19] can assist victims in reporting and give guidance on how to mitigate a breach and possibly determine how their information may have been compromised.

Once law enforcement personnel have determined that their personal information has been exploited or has been "doxed," they should report the incident to their department and work closely with the department to mitigate the associated risks.

Report Incident

Report the incident to your agency or another agency capable of investigating cybercrime.

Determine Threat

Determine what information was exploited, the seriousness of the threat, and the point of compromise.

Remove Information

Work with law enforcement to remove the information from the Web site or app.

Monitor Safety

Monitor financial accounts, set up fraud alerts, change log-in and passwords for all online accounts, and stay cognizant of your physical safety.

Training and Resources

Law enforcement personnel must take the necessary proactive steps to manage their digital footprints. Simple steps such as setting up a Google Alert[20] on their names or updating privacy settings on social media accounts can assist in managing their online presence.

Awareness is key to being successful, and resources such as the Law Enforcement Cyber Center (LECC),[21] the International Association of Chiefs of Police Center for Social Media,[22] the Federal Bureau of Investigation (FBI),[23] and the U.S. Department of Homeland Security (DHS),[24] as well as cybercrime training providers such as the National White Collar Crime Center (NW3C),[25] can assist in providing law enforcement personnel with the knowledge and skills required to protect themselves and their families from falling victim to cyber exploitation.

Sources

1 “My Digital Footprint: A Brief Guide.” Crown Copyright, 2015. Web. 1 May 2016. https://www.cpni.gov.uk/Documents/Publications/2015/Digital%20Footprint/09_My%20Digital%20Footprint%20-%20a%20brief%20guide%20FINAL.pdf.

2 “Department of Justice Report Regarding the Criminal Investigation Into the Shooting Death of Michael Brown by Ferguson, Missouri Police Officer Darren Wilson.” U.S. Department of Justice, 4 Mar. 2015. Web. 1 May 2016. https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/doj_report_on_shooting_of_michael_brown_1.pdf.

3 “Anonymous Hackers’ Efforts to Identify Ferguson Police Officer Create Turmoil.” *The New York Times*, 14 Aug. 2014. Web. 3 May 2016. http://www.nytimes.com/2014/08/15/us/ferguson-case-roils-collective-called-anonymous.html.

4 “Kill List” with personal information of 36 Minnesota cops posted by pro-ISIS hackers. *New York Daily News*, 17 March 2016. Web. 7 June 2016. http://www.nydailynews.com/news/national/isis-kill-list-personal-info-36-minn-cops-posted-article-1.2568199.

5 “Data Brokers—A Call for Transparency and Accountability.” Federal Trade Commission, May 2014. Web. Apr. 2016. https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

6 Internet Live Stats. Web. 2 May 2016. http://www.internetlivestats.com.

7 Stay Safe Online. Web. 2 May 2016. https://staysafeonline.org.

8 “Doxxing: The New Threat—Posting the Personal Information of Officers and Their Families.” Virginia Association of Chiefs of Police and Foundation Inc., 22 Mar. 2015. Web. 24 Apr. 2016. http://www.vachiefs.org/index.php/news/item/doxxing_the_new_threat_posting_personal_info_of_officers_and_their_families.

9 Stay Secure Online 2016—A review of the privacy option currently available to users. January 2016. (National Police Chiefs’ Council (NPCC) Data Communications Group, produced in partnership with the Digital Investigation and Intelligence Programme).

10 Privacy for Cops. Web. 5 May 2016. https://www.privacyforcops.org.

11 Just Delete Me. Web. 4 May 2016. http://justdelete.me.

12 “Tracking My Digital Footprint—A Guide to Digital Footprint Discovery and Management.” Crown Copyright 2015. Web. 3 May 2016. https://www.cpni.gov.uk/Documents/Publications/2015/Digital Footprint/10_Tracking my digital footprint_FINAL.pdf.

13 U.S. Department of Homeland Security “Mobile Security Tip Card” Web. 8 June 2016. https://www.dhs.gov/sites/default/files/publications/Mobile%20Security%20Tip%20Card_3.pdf.

14 Federal Communications Commission. “Protecting Your Wireless Network” Web. 8 June 2016. https://www.fcc.gov/consumers/guides/protecting-your-wireless-network.

15 International Association of Chiefs of Police (IACP). Web. 8 June 2016. http://www.iacp.org/Computer-Crime-and-Digital-Evidence.

16 IACP Computer Crime and Digital Evidence Committee Law Enforcement Technology Minute Video—Digital Officer Safety. https://www.youtube.com/watch?v=3sN1dOt7-T4&list=UUQ9UHQ1sRz3ee1pMsEpQ_JQ.

17 Stay Secure Online 2016—A review of the privacy option currently available to users. January 2016. (National Police Chiefs’ Council (NPCC) Data Communications Group, produced in partnership with the Digital Investigation and Intelligence Programme).

18 Federal Trade Commission. Web. 8 June 2016. https://www.identitytheft.gov/.

19 Federal Bureau of Investigation (FBI). Web. 8 June 2016. https://www.fbi.gov/investigate/cyber Internet Crime Complaint Center (IC3). https://www.ic3.gov/default.aspx.

20 Google. Web. 3 May 2016. https://support.google.com/alerts/answer/4815696?hl=en.

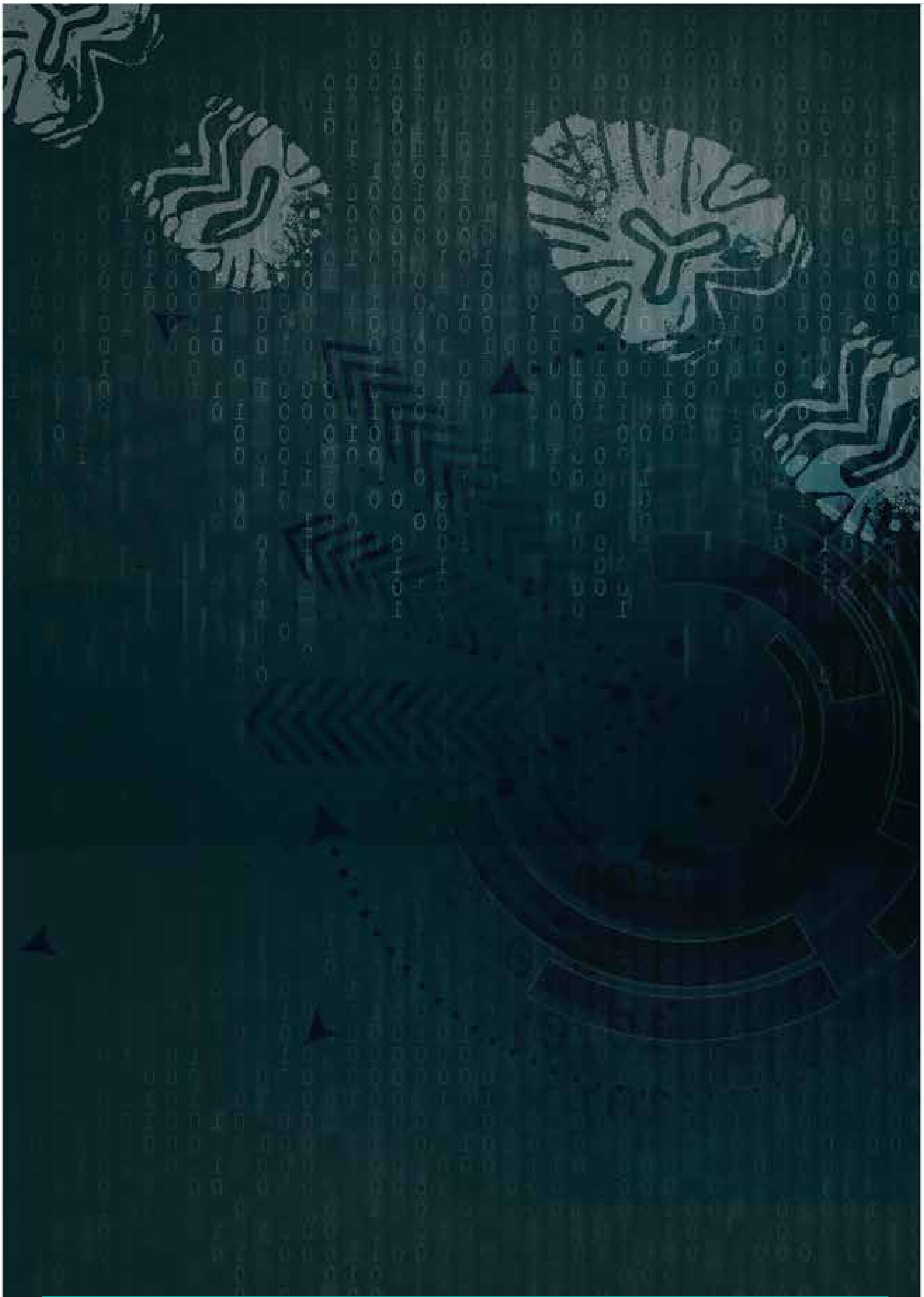
21 Law Enforcement Cyber Center (LECC). International Association of Chiefs of Police. Web. 5 May 2016. http://www.iacpcybercenter.org.

22 IACP Center for Social Media. International Association of Chiefs of Police. Web. 5 May 2016. http://www.iacpsocialmedia.org.

23 Federal Bureau of Investigation (FBI). Web. 7 May 2016. https://www.fbi.gov/investigate/cyber.

24 U.S. Department of Homeland Security (DHS). Web. 7 May 2016. https://www.dhs.gov/stopthinkconnect.

25 National White Collar Crime Center (NW3C). Web. 5 May 2016. https://www.nw3c.org/.



This project was supported by Grant No. 2015-BE-BX-0011 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the U.S. Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Issued 09/2016