OHLEG

Ohio Law Enforcement Gateway

Ohio Law Enforcement Gateway Advisory Group

Report of Recommendations from the OHLEG Advisory Group

Yvette McGee Brown, Jones Day
Evelyn Lundberg Stratton, Vorys, Sater, Seymour, and Pease LLP
Co-Chairs, former Ohio Supreme Court Justices

October 25, 2013

OHLEG Advisory Group Recommendations

OHLEG Advisory Group Members

Evelyn Lundberg Stratton, Vorys, Sater, Seymour, and Pease LLP, former Ohio Supreme Court Justice
Yvette McGee Brown, Jones Day, former Ohio Supreme Court Justice
Shelby County Common Pleas Court Judge James Stevenson
Pickaway County Juvenile Court Judge Jan Long
Union County Prosecutor David Phillips
Lorain County Sheriff Phil Stammitti
Administrative Counsel to the Ohio Public Defender Dan Jones
Grove City Chief of Police Steve Robinette
Montgomery County Coroner Dr. Kent Harshbarger

The OHLEG Advisory Group is grateful to the following invited guests who appeared before it:

Deputy Tim Winebrenner, Madison County Sheriff's Office
Detective Erik Gilleland, Dublin Police Department
Probation Officer Kimberly Chandler, Franklin County
Detective Brian Lowe, Lancaster Police Department
Professor Dennis Hirsch, Capital University Law School
OHLEG Training Coordinator Terry Staderman
OHLEG Training Coordinator Jill Small
Chief Operating Officer Kimberly Murnieks, Ohio Attorney General's Office

Introduction

Technology plays an integral part in our daily lives, including work done every day by law enforcement to keep our citizens safe. When Ohio law enforcement personnel take advantage of the efficiencies and speed that technology offers, the data needed to help solve crimes can be searched and sorted quickly.

For the past ten years, Ohio has operated the Ohio Law Enforcement Gateway, or OHLEG, a unique platform allowing law enforcement to access and search databases. No databases are created through OHLEG. Rather, OHLEG provides access to existing databases. No other state or the federal government has a system quite like it.

A new addition to OHLEG is facial recognition technology. It is a biometric technology that measures points on a person's face that are unique — much like individual fingerprints are unique. Like technologies that rely on DNA or fingerprints, facial recognition technology is a tool that helps law enforcement identify people. As we move forward with adding new technology such as facial recognition, it is important to examine the security and technology behind OHLEG to ensure the system is serving as a tool for criminal justice practitioners and not being used improperly.

Attorney General Mike DeWine created the OHLEG Advisory Group to examine not only facial recognition, but the entire OHLEG system.

It was our pleasure to serve as co-chairs of this advisory group, and we believe that the recommendations contained in this report will be helpful to the future operation of OHLEG and the citizens of Ohio.

Sincerely,

Yvette McGee Brown

Evelyn Lundberg Stratton

General

The OHLEG Advisory Group reviewed OHLEG policies and procedures with a critical eye. The group's purpose was to offer recommendations that would protect the integrity of OHLEG and provide confidence to the public that safe guards are in place to protect the data that is accessible by criminal justice personnel. To that end, it is important that there be in place a body, or bodies, whose function it will be to continually review OHLEG policies and procedures as the system evolves. To ensure that OHLEG continues to operate in a publicly accountable manner, the following recommendations are made.

Recommendations

(1) OHLEG Steering Committee: The authority provided under Ohio Revised Code Section 109.57(C)(4) should be exercised and an OHLEG steering committee should be established. Pursuant to that section, the committee should be comprised of "criminal justice agencies ... that use [OHLEG]." The committee should be tasked with the review, monitoring, training, and updating of the OHLEG and facial recognition policies, to include ongoing review of the implementation of these recommendations. In addition, the committee should review risk assessments to the system and continue to develop new anti-hacking and security policies as new threats become known.

(2) Advisory Group to the OHLEG Steering Committee: An advisory group consisting of professionals from a broad range of agencies with an interest in OHLEG activities should be established. The advisory group should serve as a sounding board for the OHLEG Steering Committee and the Attorney General as new policies are developed. The advisory group should meet at least twice a year or as needed (see comment 1 on page 9 of this report for an additional remark regarding this recommendation).

(3) OHLEG Records Retention: The length of time OHLEG search information needs to be retained should be assessed and a records retention policy for such records should be established.

Access

Testimony from invited guests made clear that not all criminal justice professionals require the same access to the various applications offered through OHLEG. However, individual job responsibilities vary widely from county to county, even when job titles are identical. Limiting OHLEG access to only those applications necessary to perform one's job duties will mitigate the risk of OHLEG misuse.

Of particular importance is the distinction between law enforcement and non-law enforcement agencies. Criminal justice professionals who work in a law enforcement agency (i.e., police officers and sheriff's deputies) require a greater degree of OHLEG access than those who work for non-law enforcement agencies (i.e., court employees). For purposes of these recommendations, "law enforcement agency" means a police department, the office of a sheriff, the state highway patrol, a county prosecuting attorney, or a federal, state, or local governmental body that enforces criminal laws and has employees who have a statutory power of arrest. See Ohio Rev. Code § 109.573(A)(8).

Recommendations

(1) General OHLEG Access: The current project to tailor OHLEG access as determined by the chief executive officer of an organization should continue. OHLEG users should only access the information they need for their job responsibilities. This includes access to information gained through facial recognition searches. Guidelines and procedures for immediately removing access and for reporting to OHLEG when an individual user is terminated, retires, or otherwise becomes ineligible to access OHLEG have been developed and should be implemented as soon as possible.

(2) Facial Recognition: Although the general OHLEG access recommendation above is sufficient for law enforcement agencies, non-law enforcement agencies require stricter access to this technology. Non-law enforcement agencies should not have access to OHLEG facial recognition technology without the express written permission of the Superintendent of the Bureau of Criminal Investigation (BCI).

(3) Juvenile Records: Access to juvenile records should be referred to the OHLEG steering committee, which should proceed in consultation with the Ohio Association of Juvenile Court Judges and the Ohio Attorney General's Task Force on Criminal Justice and Mental Illness.

(4) Out-of-State Access: A written policy governing access by out-of-state agencies should be developed. Such a policy should require out-of-state OHLEG applicants to expressly consent to personal jurisdiction in Madison County, Ohio. When possible, reciprocal access to the other jurisdiction's database should be requested.

No direct access to OHLEG should be granted to out-of-state, non-law enforcement agencies, without the express, written authorization of the Superintendent of BCI. (It should be noted that OHLEG access has not been provided to any out-of-state, non-law enforcement agencies to date.)

(5) Research Access: A written policy for entities wishing to conduct research involving OHLEG should be established. All applicants seeking access to records for research purposes should be subject to the same training and misuse warnings as other OHLEG users.

Training

Training is an essential tool to ensure that users of OHLEG gain an appreciation for OHLEG's value and understand the responsibility associated with its use as well as the consequences for its misuse. The development of a standardized training program is paramount to OHLEG reaching its full potential in a publicly acceptable manner.

Recommendations

(1) Mandatory Training: A mandatory, standardized training program that is also geared to the audience should provide training and protocols. Such training could be offered online provided that completion can be verified. Training should include: (1) penalties for misuse with real life examples of prosecutions to stress

the seriousness of the consequences; and (2) guidelines for reporting and prosecuting infractions. Necessary steps to take after discovering misuse should be provided.

(2) Ongoing User Training: Periodic training modules that would require OHLEG users to acknowledge receipt of training updates should be implemented. These training modules, discussed by BCI, seek to ensure compliance with and remind users of the regulations for the use of OHLEG. Where appropriate, training should be conducted through eOPOTA.

(3) Simulated Training Platform: A training platform should be established to permit users to practice searches without accessing official records.

Monitoring OHLEG Use

Proactive monitoring of OHLEG use is perhaps the most effective measure of whether the system is being properly implemented for its intended criminal justice purpose. While it is understood that chief executive officers may not engage in daily hands-on OHLEG activity, they are the party responsible for ensuring that their agency meets the criminal justice requirements set forth by the Attorney General's Office. Delegation of authority in order to implement OHLEG policies on a local level will not absolve CEOs of this responsibility.

Recommendations

(1) General OHLEG Audits: Dedicated OHLEG staff should perform random audits on a regular basis to be sure there is compliance with both Ohio law and OHLEG policies. The current project to easily generate a comprehensive list of all users that identifies each user by name and agency should continue.

(2) Local Monitoring: One person should be in charge of and responsible for monitoring an agency's usage. The current plan to provide a clear policy regarding duties of agency chief executive officers should continue. Agency CEOs

should be charged with monitoring who has access, levels of access, who has completed training, and account termination.

(3) Model OHLEG Policy: A model OHLEG use policy for local agencies should be developed and made available to all OHLEG user agencies. Guidelines for reporting and prosecuting infractions should be developed. Necessary steps to take after discovering misuse should be provided.

Public Education

Public education about information found in OHLEG can increase the accuracy of those records while improving public perception of the system. For instance, oftentimes the most efficient manner in which to review criminal records for accuracy is to permit the subject of those records access. In order to effectuate this solution, the public must be made aware of the procedure through which individual criminal histories can be obtained. If, after obtaining a copy of his or her criminal history, an individual discovers his or her identity was used in an unauthorized manner, direction as to how to correct resulting errors in that criminal history is necessary.

Recommendations

(1) Mental Health Records Education: Law enforcement should be apprised of the availability of mental health information under the Suzanne Hopper Act.

(2) Facial Recognition: The public should be informed as to how facial recognition searches can benefit them. Facial recognition searches mitigate the ability of others to steal their identity by immediately matching a face with data. It can clear an innocent person when someone else has their stolen driver's license or other identification.

(3) Computerized Criminal Histories: The fact that anyone can access his or her own criminal history pursuant to Ohio Administrative Code 109:5-1-01, should be publicized on the Ohio Attorney General's website. The Ohio Attorney General should work with the Ohio Public Defender and others who represent the indigent to ensure they are aware they can access their clients' criminal histories (see comment 2 on page 9 of this report for an additional remark regarding this recommendation).

(4) Correction of Errors: The public should be informed of how to correct errors found in records such as criminal histories and driver's license information. Although records obtained through OHLEG must be corrected by the source of those records, this information should be relayed to the public.

Comments from Individual OHLEG Advisory Group Members

1. Chief Robinette would remove this recommendation and broaden the description of the OHLEG Steering Committee. A more efficient approach would be to expressly authorize the OHLEG Steering Committee to, from time to time, take testimony from interested parties on OHLEG practices and use.

2. The Ohio Public Defender's Office would augment this recommendation to add that any Ohio citizen should be able to access and review his or her own criminal history record through a secure internet portal using his or her social security number, in a manner similar to obtaining a consumer credit history check under federal consumer protection laws, via the website www.AnnualCreditReport.com. And as with the credit report model, once annually any Ohio citizen should be allowed to access his or her own criminal history record at no cost. This process would allow Ohio citizens to report any errors or identity theft concerns to BCI and/or the court system, and thus would contribute to the validity of the database, as contemplated by recommendation (4), above.