Opportunities and Challenges from Artificial Intelligence for Law Enforcement

By Tom Campbell, PhD, Founder & President, FutureGrasp, LLC  •  20 Jul, 2018  •  0 Comments

Law enforcement (LE) has unique challenges—identification of individuals, prediction of criminal actions, tracking of money flows, tagging and defending against fake news, and enhanced communications across agencies, among others—that demand rapid data acquisition and analysis. As artificial intelligence (AI) offers unprecedented capabilities to acquire and analyze big data, it is no surprise that the LE community is interested in applying AI for its purposes. [1] But given LE’s unique requirements on speed, low error rates, and accurate predictions, is AI up to the task yet of helping LE?

We offer here a review of several facets of AI that could benefit or compromise LE. [2] As AI becomes more advanced, the potential for its application by LE experts (and criminals) will only
increase. Let us hope that LE officers in the field and analysts in the office are able to leverage AI to protect people around the world.

DATA, DATA, DATA—THE INTERNET OF THINGS

We are living in a veritable information explosion. Every day we create roughly 2.5 quintillion bytes of new data. [3] The Internet of Things – i.e., the universe of devices connected to the internet – is forecasted to exceed 30 billion devices by 2030. Over a trillion sensors of all forms is projected to be in use by 2020. [4] This digital tsunami tasks our local and federal governments in gathering data, comprehending it, and crafting sound policies. Because of the rapid-response needs of LE, this information must be acquired, curated and analyzed in almost real-time.

AI can assist in managing this surfeit of data. Especially well-positioned here is deep learning (DL), which requires massive datasets in order to yield accurate output. Thus, leveraging DL makes perfect sense for the LE community; each of the technologies described below use some aspect of DL.

FACIAL RECOGNITION (FACE-REC)

There are some people who never forget a face. So-called ‘super-recognizers,’ such individuals can remember people they haven’t seen in decades. For the rest of us, we can use mnemonic tricks to not be embarrassed in conversations. Theoretically, computers should trump everyone on identifying people, as fundamentally face-rec is a challenge of data recall.

In the early days of face-rec competitions with algorithms, we routinely beat our silicon creations… then DL was developed. During an imaging contest using a large database, the Imagenet, one team in 2012 successfully leveraged large computational power with DL to improve face-rec accuracy dramatically. As clarified by MIT Technology Review:

“This was the first time that a deep convolutional neural network had won the competition, and it was a clear victory. In 2010, the winning entry had an error rate of 28.2 percent, in 2011 the error rate had dropped to 25.8 percent. But SuperVision won with an error rate of only 16.4 percent in 2012 (the second best entry had an error rate of 26.2 percent). That clear victory ensured that this approach has been widely copied since then.” [5]

At this writing, the record for face-rec is claimed to be less than one percent error—although exact error values vary as a function of lighting, amount of the face exposed, motion and other factors. Depending on the humans tested, errors by people attempting to recognize others range the gamut from 0% to 50% error. [6]

Recognizing faces is a critical aspect of policing work, yet the techniques for its execution must be trusted. Mug shots and line-ups have been used for decades with human victims attempting to identify criminals. Nevertheless, errors can occur and people can be falsely jailed based upon a mistaken identity. [6] Using algorithms to reduce errors can help, but we must be careful to not be too reliant on them, as even a small error rate can still yield false arrests. [7] Microsoft recently called for the US Government to consider regulating face-rec: “Facial recognition technology raises issues that go to the heart of fundamental human rights protections like privacy and freedom of
expression. These issues heighten responsibility for tech companies that create these products. In our view, they also call for thoughtful government regulation and for the development of norms around acceptable uses. In a democratic republic, there is no substitute for decision making by our elected representatives regarding the issues that require the balancing of public safety with the essence of our democratic freedoms. Facial recognition will require the public and private sectors alike to step up – and to act.” [8]

Law enforcement should proceed with caution on the use of face-rec. At the present stage of its development, algorithmically-generated face-rec should be verified independently by humans to avoid mistaken identities.

CAMERAS

Cameras of all forms (including body cameras-bodycams, CCTV-closed circuit television, and drone cameras) can be a powerful tool for reducing violence both at and from police, as well as identifying criminals. The range of intrusiveness of these systems varies from passive (observation only) to active (seeking matches to faces and other crime scene clues in large databases).

On the passive side, bodycams can be used to protect both the citizen and the police officer, but they have their own limitations. “They record audio and video, often with date and time stamps as well as GPS coordinates. They can also be Bluetooth-enabled and set to stream in real time. Some have to be turned on manually, others can be triggered automatically by, for instance, an officer unholstering his weapon.” [9] Bodycams are controversial, and their effectiveness in reducing violence both at and from police officers has been called into question. A 2017 study, claiming to be the largest on bodycams to date, concluded that these systems offer mixed results. “A new study suggests police body cameras have had no measurable effect in Washington, D.C., when it comes to civilian complaints, use of force incidents, policing activity or judicial outcomes involving the city’s Metropolitan Police Department.” [10] Nevertheless, we should note that these are still early days for video recordings of citizen-police interactions, and that more use and data may offer greater clarity on the effectiveness of this LE tool.

On the active side, machine learning and deep learning can be leveraged to identify a wide range of characteristics of people and objects from cameras. Perhaps the most intrusive application of AI for personal identification via cameras is in China:

“It should give Westerners no comfort that China—a one-party state obsessed with social order—is at the forefront of developing bodycams. One Beijing company says it has invented a shoulder-worn, networked model that can recognize faces. Another Chinese firm has equipped police with facial-recognition cameras embedded in glasses that are meant to let officers know in real time if they are looking at someone on a police blacklist. One estimate values China’s surveillance-tech market in 2018 at $120bn. Human-rights campaigners fear that such technology has already been used to monitor activists, enabling arbitrary detention.” [7]

Although privacy limitations may limit such active scanning and analysis in Western countries, the genie is out of the bottle for many nation states. Cameras with AI built-in for face-rec are now commercially available. [11],[12] It remains to be seen how far LE takes such tools. Applications of cameras have strong implications for other technologies discussed below, however.
UNMANNED AERIAL VEHICLES (UAVs, aka, DRONES)

UAVs have been commercially available for over a decade, but their price-points and capabilities came to levels only just within the past few years so that LE is adopting them. UAVs range in size from an artificial bee [13] to a large aircraft [14]. Their capabilities are just as diverse, with not just cameras, but also weaponization [15], fire-fighting [16], and even tree-planting [17]. Only a lack of imagination limits what one can do with these flying machines.

Privacy advocates have been calling for years to place limitations on drone use. After much debate, the US Federal Aviation Administration (FAA, https://www.faa.gov/) put into laws the conditions under which one must operate to fly a drone of any kind in public. For example, UAVs are not allowed to fly in US national parks without a permit (for concerns of stressing wildlife, endangering people, etc.). [18] [19] All drones within certain size range can be flown legally only with a permit. [20]

LE may have looser restrictions on UAV applications – for example, with a known threat of terrorism or a manhunt underway for a suspected felon. Nevertheless, even LE must comply in the United States with certain limitations to protect the public’s privacy and safety. “Local and state agencies in the US have passed rules imposing strict regulations on how law enforcement and other government agencies can use drones. Indiana law specifies that police departments can use drones for search-and-rescue efforts, to record crash scenes and to help in emergencies, but otherwise a warrant is required to use a drone. That means police probably won’t be able to fly them near large gatherings unless a terrorist attack or crime is under way.” [21]

The implications of UAVs are extensive for LE. The ability to have a birds-eye view practically anywhere (both outdoors and indoors) offers significant upside for LE in tracking, identification and analysis of criminal individuals and actions. Nevertheless, as noted above, UAV use also brings with it great responsibility to ensure safety and privacy of the public. As UAVs advance technologically, LE must continue to engage with local and national governments to ensure these issues are jointly addressed. INTERPOL is taking a lead in assessing drone threats and challenges to LE via its Global Complex for Innovation. [22]

FAKE NEWS

Fake news has a long history. Ever since printed text became widely available, fake news has been used by people to push propaganda and influence one’s enemies. “Fake news took off at the same time that news began to circulate widely, after Johannes Gutenberg invented the printing press in 1439. ‘Real’ news was hard to verify in that era. There were plenty of news sources—from official publications by political and religious authorities, to eyewitness accounts from sailors and merchants—but no concept of journalistic ethics or objectivity. Readers in search of fact had to pay close attention. In the 16th century, those who wanted real news believed that leaked secret government reports were reliable sources, such as Venetian government correspondence, known as relazioni. But it wasn’t long before leaked original documents were soon followed by fake relazioni leaks. By the 17th century, historians began to play a role in verifying the news by publishing their sources as verifiable footnotes. The trial over Galileo’s findings in 1610 also created a desire for scientifically verifiable news and helped create influential scholarly news sources.” [23]
Since those early days, fake news has expanded to include every new recording or communications technology—see image at bottom of text. When photography was first introduced to the public, faking a photograph taken on real film required staging shots or chemical manipulation. Digital photos make it much easier to simply jigger a few pixels and produce any photo one wishes. Now it is a challenge to have a photo be admitted as evidence in a court of law.

As the internet came online in the latter part of the 20th century, fake news really took off. Now with major online platforms such as Facebook and Twitter, as well as the 24/7 news cycle, we struggle to identify what is real or not while living in our chosen filter bubbles. Nation states such as Russia and China have embraced social media as a means for pushing their own messages or propaganda.

We are now progressing into even more sophisticated fake news. Audio and video can be manipulated at will. One research group claims that all they need is 3.7 seconds of a human’s voice soundwaves to mimic them with an algorithm. [24] Another research group takes such work to another level by superimposing a researcher’s face onto that of another individual, and consequently enabling the researcher to make the victim say anything with any expression the researcher desires. [25]

Further into the realm of difficulty and complexity, augmented and virtual realities (AR and VR) will become the next-gen platforms for fake news. As AR and VR are used more by companies and governments, we may fully expect them to be target platforms for fake news. Essentially, any mode of communications is now fair game for fake news generation.

Law enforcement has an important role to play in fake news, albeit one that appears to be still gelling in terms of its scope. Police officers and nation states must both identify and defend against fake news. During the recent Mexico elections (July 2018), an effort was made to identify fake news in text, audio and video by AI. Human curators then reviewed the tagged media and decided if it was truly false and what to do with it if so. [26] At this writing, it is unclear how effective this work was.

As we expand how we exchange news, nefarious individuals will continue to manipulate our communications and distribute their own narratives or influence efforts. It is upon the shoulders of LE and nation states to ensure that fake news is identified and does not result in skewed elections or criminal actions. Sadly, the veracity of news is a competition between criminals and LE with no foreseeable end.

PREDICTIVE POLICING

In the 2002 movie Minority Report, the character played by Tom Cruise uses a bio-based computing system to predict crimes before they happen and thus arrest perpetrators before they commit their nefarious deeds. We are a ways away from being able to make such fully accurate predictions—and accurate they must be; imagine being falsely accused for murder because of algorithmic error or bias?—but we may still consider that the summation of the technologies described above and others are leading us down this path. Whether and how quickly predictive policing moves out of fiction into every police station remains to be seen. Nevertheless, significant efforts and research dollars are being expended to make predictive policing become the norm in identifying crime locations and
individuals in advance. We list below just a few examples of the research now underway, and already deployed tools, to enable future Tom Cruises to wield their predictive hands against crime.

In the United States, the company Palantir has been testing predictive policing in large cities for several years. Unbeknownst to several city council members, Palantir algorithms were used in New Orleans for over six years; the Palantir contract has since been cancelled. [27] The Los Angeles Police Department (LAPD) still uses Palantir’s models, but there are claims that the results have inherent racial bias. [28] Because of concerns of opaqueness (lack of disclosure of the databases) and bias, there are now major lawsuits pending against Palantir in Chicago, Los Angeles, New Orleans and New York City. [29]

Japan recently announced a major effort to enable predictive policing. “The AI-based system would employ a ‘deep learning’ algorithm that allows the computer to teach itself by analyzing big data. It would encompass the fields of criminology, mathematics and statistics while gathering data on times, places, weather and geographical conditions as well as other aspects of crimes and accidents.” [30] The Japanese government hopes to prove the system in at least one prefecture first, and then deploy it further at the 2020 Tokyo Olympics. [31]

Perhaps China has taken the level of predictive policing to its most intrusive level, violating international human rights norms in the process. In the prefecture of Xinjiang, local authorities and police use big data analytics to monitor a wide variety of personally identifiable information (PII) on minority citizens, often without their knowledge. Individuals can then be arrested and imprisoned without trial. [32] Chinese citizens, although said by Chinese officials to be trusting of the technology wielded by their local law enforcement, are known to cover their faces when cameras are pointed at them. [33]

Thus, other than a few nation states such as China, widespread use of predictive policing is not yet the norm. An informal survey made during the recent INTERPOL—UNICRI meeting in Singapore on AI, robotics and law enforcement showed that none of the 20 attending countries had significant predictive policing programs planned or in place at this writing (China was not present at the meeting). [1] This lack of broad application may change, though, as algorithm, data and computational capabilities increase. Ultimately, caution should be exercised by all parties in deployment of predictive policing to ensure that it does not compromise the privacy of innocent civilians and/or result in ill will and lawsuits against LE that may take the technology too far.

**CONCLUSIONS & IMPLICATIONS**

One can argue that AI is certainly capable of helping to address some of the data acquisition and analysis needs in LE, but with the caveat that its use must be monitored and proofed before arrests or litigation decisions are made. Technologies such as face-rec with algorithm-enabled digital cameras, as well as nascent experiments in predictive policing, offer LE officers new tools by which to perform their tasks. The challenges of fake news are increasing in complexity and may require AI to assist LE in its identification and digital removal. Nevertheless, inherent limitations of AI such as inherent bias, opaque algorithms, and lack of complete datasets should give us pause before unchecked deployment of AI in LE. In the United States and elsewhere there are major lawsuits pending against LE agencies that may have deployed AI algorithms too soon without rigorous verification and validation (V&V) mechanisms in place. Other nations such as China have gone all-
in on AI-enabled LE capabilities, but at the cost of human rights for its citizens who in minor cases lose privacy and in worst cases get falsely arrested and jailed without warrants.

Despite technical and ethical challenges, the use of AI by LE is entering an inexorable state. In many criminal cases, there is simply too much data for the traditional officer or detective alone to capture and assess all relevant evidence. Whether and how individual police departments, small towns, cities and nation states apply the powers of AI algorithms remains to be seen. Moreover, its adoption will most probably be driven by culture and nation state interests. Let us hope that the applications of AI in LE are made after careful consideration of both the benefits to LE agencies and the citizens they are charged to protect.

NOTES (all websites accessed July 2018)


[2] Note this review is not meant to be comprehensive, but merely an introduction to the field. Substantial literature has been written about each of the overview sections here.


[8] “Facial recognition technology: The need for public regulation and corporate responsibility,” Microsoft Blogs, June 13, 2018, https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/?ranMID=24542&ranEID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-kig_5rwdCle73fiVClXDjg&epi=je6NUbpObpQ-kig_5rwdCle73fiVClXDjg&irgwc=1&OCID=AID681541 Aff_7593_1243925&tduid=(ir_W8kVW1XE3ns3NhV1m05%3ATJDUkjVTBXmPxzmUg0)(7593)(1243925)(je6NUbpObpQ-


[18] Years ago, I was in Yosemite National Park and saw a small UAV being used to film a valley, despite a large crowd present in the same area. I asked the operator if he had a permit—the individual feigned surprise, then immediately landed the drone, grabbed it, and took-off in his pickup truck.


FutureGrasp, LLC--News Media, Nested in Order of Increasing Complexity, that are Vulnerable to Fake News