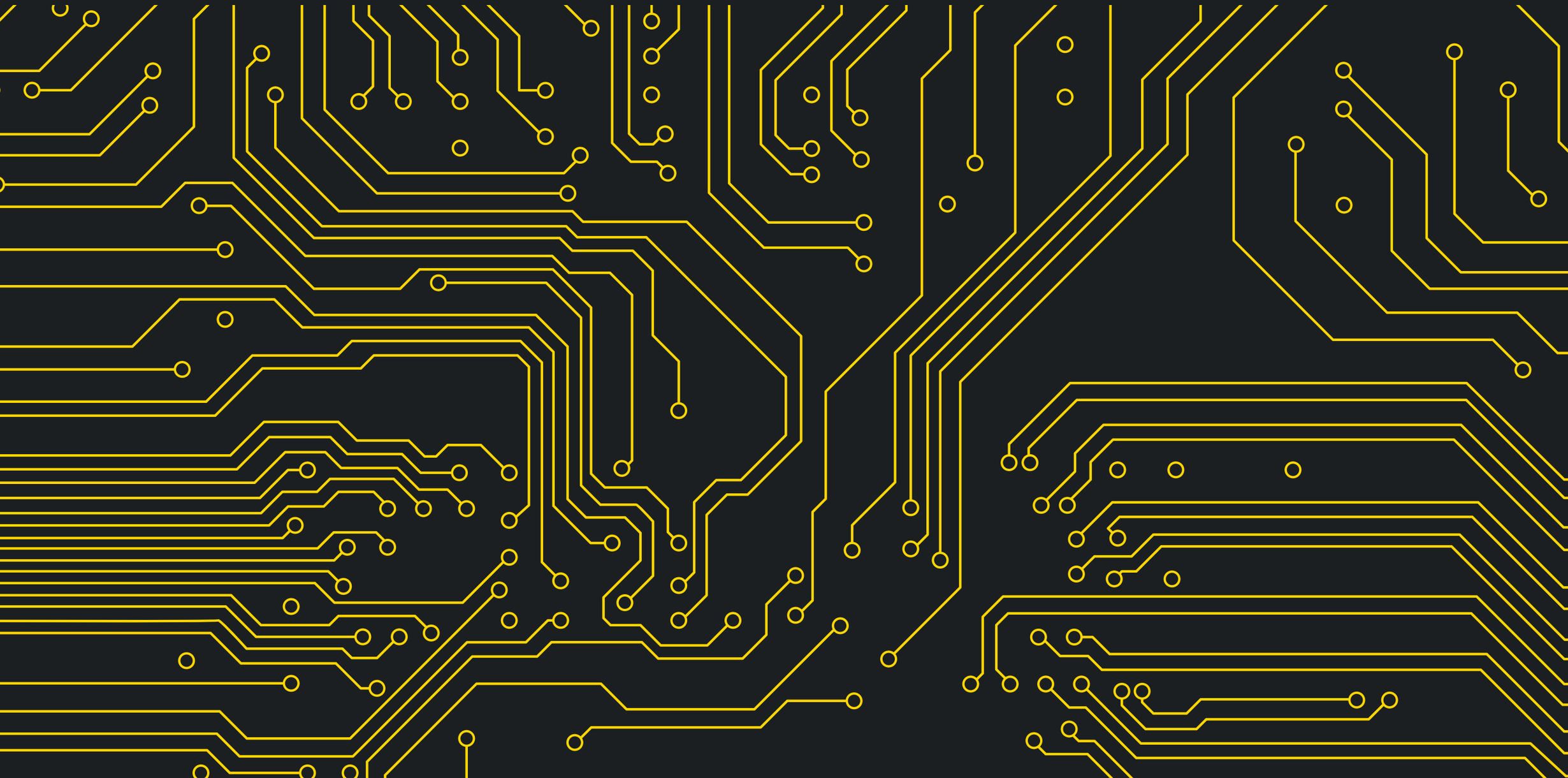
2017 | LAW ENFORCEMENT TECHNOLOGY REPORT



A TECHNOLOGY TURNING POINT

Laying the groundwork

Last year, we set out to compile the latest statistics on law enforcement technology, from cameras to the cloud. What we found was not surprising.

Law enforcement officials said that for too long the technology they used at home was superior to what was at their agency. Cameras and mobile devices were being adopted and used with increasing frequency. Data was being transferred to the cloud.

Looking ahead

This year's report builds off that foundation and looks to the future. We spoke with a range of subject-matter experts to develop this report: lawyers, retired and active law enforcement officials, academics, technology professionals. They shared with us their predictions of what the future will bring.

WHAT WE LEARNED

CAMERAS AND THE CLOUD ARE A GIVEN

There's widespread agreement: An agency without body cameras now will adopt them in the coming years. But agencies aren't just adopting cameras — they're also generating more data and evidence than ever before. As technology becomes increasingly more sophisticated, law enforcement officials will need to turn to the cloud to efficiently handle and intelligently interpret their data.

SECURITY WILL MAKE OR BREAK YOU

More devices mean more opportunities for hackers, who are turning their attention to finding vulnerabilities in the latest smart devices. While technology is changing, the precautions you need to take aren't. Two simple security practices can help protect your agency from hacktivists and data breaches. In this report, we'll cover how how to build strong passwords and detect phishing emails.

A.I. AND MACHINE LEARNING WILL GO BEYOND BUZZWORDS

The future of law enforcement technology looks smarter and more connected, and advancements in artificial intelligence and machine learning will have profound implications for policing. Soon, you'll be able to tell almost immediately if someone has an outstanding warrant against them, thanks to facial recognition technology. And forget about report-writing, since all the information you need to build a report can be extracted from your body camera videos.

TABLE OF CONTENTS

Cameras and the cloud // 5-14

A look at where cameras and the cloud are now, and how they'll transform policing and the justice system in the coming years.

8 // A tool for self-defense: One former sheriff's outlook

9 // Game-changing technology: A former BWC program manager's perspective

12 // Bringing events to life in court: A deputy district attorney's thoughts

Safe and secure // 15-20

Changing technology comes with increased security concerns. We've found that most agencies still need to cover some basic security tips to protect their data.

18 // Tips for any agency: A conversation with TASER's VP of information security

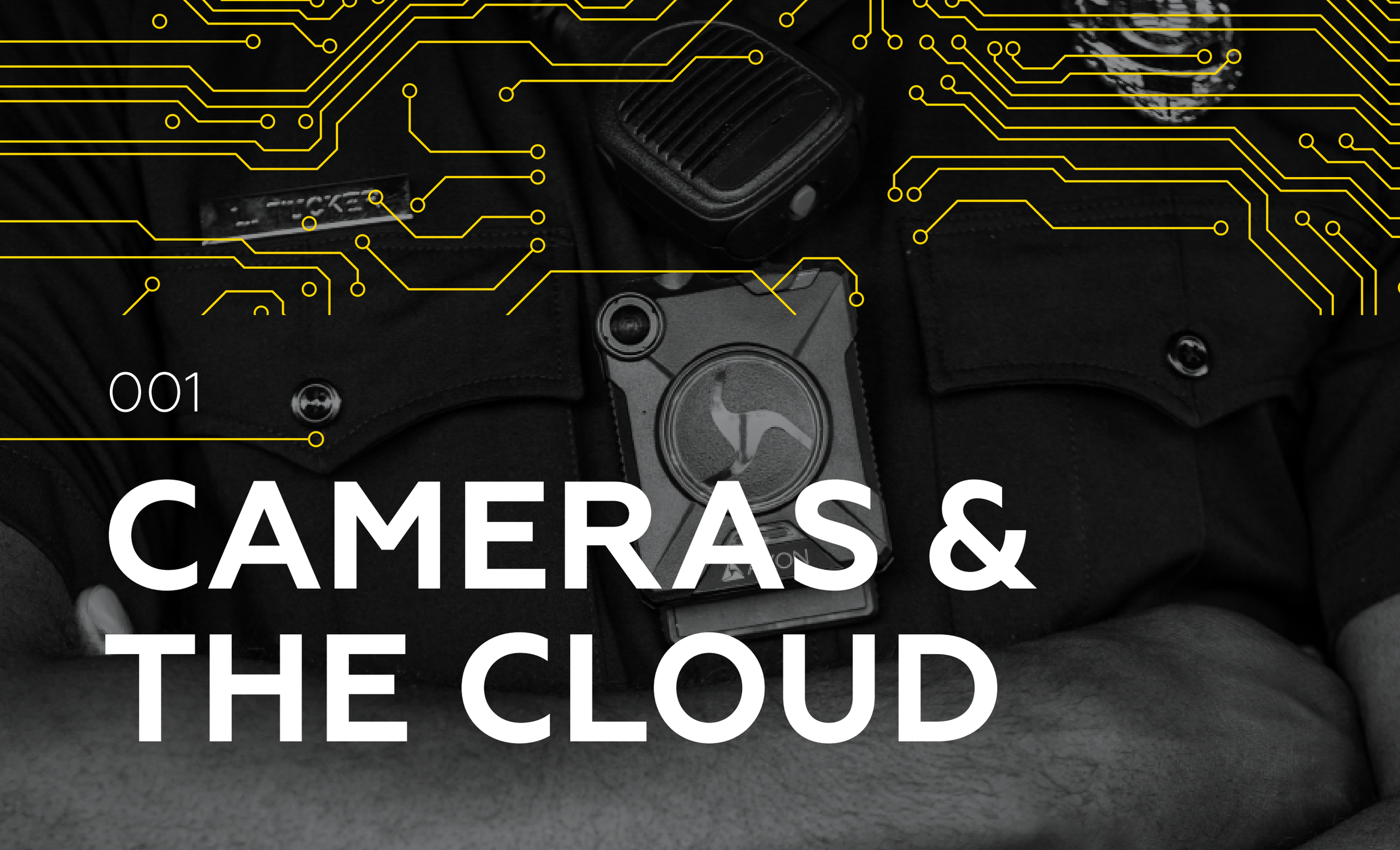
A.I. & machine learning // 21-31

Advancements in artificial intelligence and machine learning will offer agencies the ability to intelligently interpret their data and act almost immediately.

24 // It's all about data: Microsoft's cloud-connected future

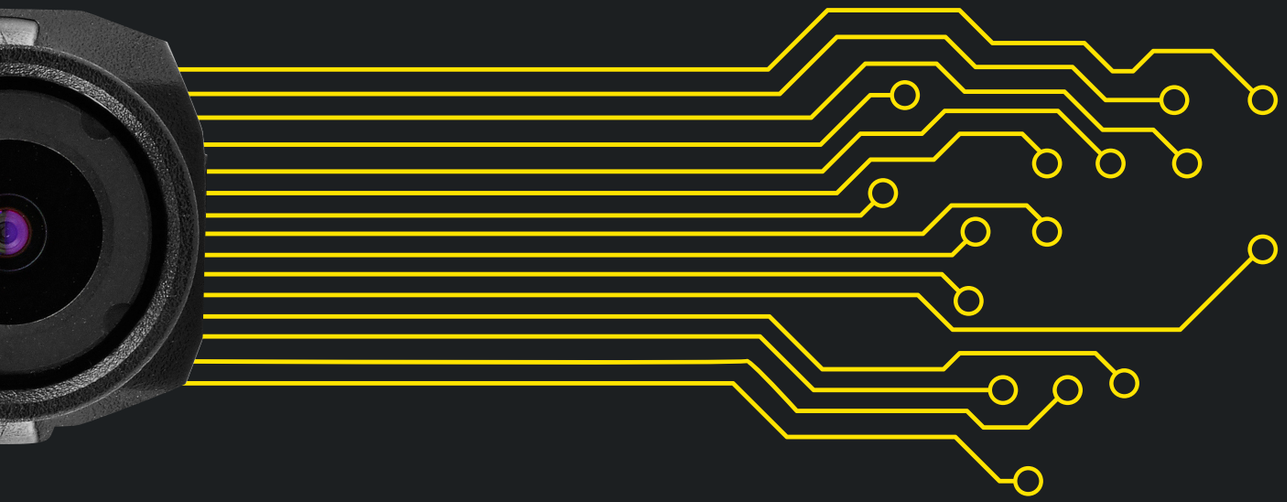
26 // Radical change, fast: One world-renowned researcher's expectations

29 // 'We're not even at 1.0': A discussion with TASER's EVP of Axon Devices



001

CAMERAS & THE CLOUD



Game-changing devices

Body cameras have redefined the justice system. They've been proven to reduce complaints, potentially lower use of force rates, and help bring cases to life in the courtroom.

And that's only the beginning.

In this section, you'll read the thoughts of a former sheriff, a captain and former body camera program manager, and a deputy district attorney. They discuss how cameras have fast become a vital policing tool — and how the cloud has helped unlock their true value, letting agencies manage their evidence more efficiently.

THE TOOL THAT CREATES CONFIDENCE

8,329

Aransas Pass, Texas population

[Source: http://americancityandcounty.com/gov-cloud/why-police-departments-are-moving-cloud]

2-4TB

the amount of data the department generated after deploying cameras (and could handle with the cloud)

1TB equals

85,899,345 pages in a Word doc

310,000 photos

17,000 hours of music

[Source: http://aimblog.uoregon.edu/2014/07/08/a-terabyte-of-storage-space-how-much-is-too-much/#.WHZdtLYrI6g]

97%

Major City Chiefs and Major County Sheriffs who said they expected to proceed with a body camera program

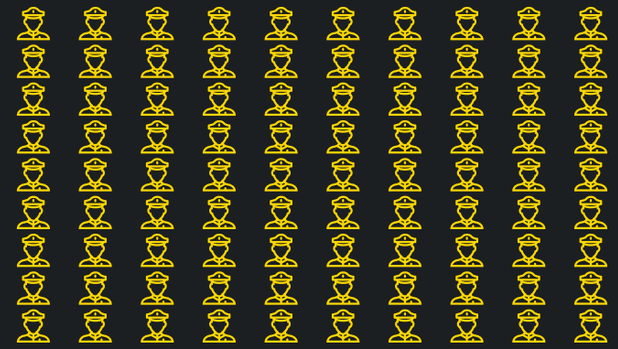
[Source: Survey of Technology Needs – Body Worn Cameras, MCC, MCS, 2016]

18% were fully operational

27% finished pilot and were moving forward

20% were in a pilot

30% intended to implement a program, hadn't begun a pilot



90 officers

in Las Vegas were exonerated after accusations of misconduct led to a review of body camera footage

[Source: 'All Las Vegas police officers will wear body cams in near future, panel says,' The Las Vegas Review-Journal, March 2016]

62%

Drop in likelihood that a complaint will be filed when body cameras are present

[Source: E. C. Hedberg, Charles M. Katz & David E. Choate. 'Body-Worn Cameras and Citizen Interactions with Police Officers: Estimating Plausible Effects Given Varying Compliance Levels,' Justice Quarterly, 2016.]

SELF-DEFENSE: ONE FORMER SHERIFF'S OUTLOOK

The rise of cell phone cameras means law enforcement officials need body cameras more than ever. So says retired Sheriff Jim Pendergraph, who after a 45-year career in law enforcement provided us with a sheriff's view on how body cameras help officers defend themselves.

Just from a sheriff's point-of-view, what have the effects been of adopting body cameras?

Better evidence, and the way I see it, the biggest thing for adopting body cameras is you have a way to prove anything your people do in the line of duty. These days, people want to see DNA, fingerprints, or video. What it's turned into now is that everyone with a cellphone has the capability to [record] anything your people do.

What I hear from most of the sheriffs is that we're doing this for self-defense, because the video off the cell camera from some supposed eyewitness can be manipulated with a cellphone computer program. This is a way to prove the deputy's side. It's unfortunate that it's come to that, but it has. That's just the day and time it is.

How do you ensure that you're never going to miss something that's important for a court case?

Well, you can't prevent that. All you can do is the best you can do.

Most states' and local sheriffs' policies are set by what state law says according to retention of evidence, but most of them are so outdated about the Freedom of Information Act about what you need to keep that most states are scrambling now to change their state law about what's retained.

Do you think that body cameras have reduced officer confidence in their decisions? Do you think officers feel as if their word is no longer trusted and the camera only further impinges on that?

One, I think recruiting has been hurt because of the situation. They don't feel like the community backs their efforts like they used to.

I think the deputies who were opposed, or law enforcement officers who were opposed to body cameras two years ago are all in favor of it now because of some of the things they've seen and heard. They need to protect themselves, and they realize that.

Where do you see technology going in the next five to ten years?

It's hard to determine what's going to happen in the next five years. We would have never dreamed five years ago that this would have turned into such a big thing. It's just the demands of the public and the court system.

I think the body cameras are going to get lighter, smaller, and easier to deploy. The video quality is going to certainly improve. It's good now, but I think it's going to get much better.

FOIA FRUSTRATIONS

100% more

The rate of FOIA requests received by police and sheriffs compared to other state and local agencies in Washington state

[Source: "The Effect of Public Records Requests on State and Local Governments," Washington State Auditor's Office, August 2016.]

GAME-CHANGING TECHNOLOGY: A FORMER BWC PROGRAM MANAGER'S PERSPECTIVE

Captain Daniel Zehnder, former manager of Las Vegas Police Department's body-worn camera program and president of Principis Group Inc., a body-worn camera training and consulting company, calls body cameras one of the three most transformative technology developments in law enforcement history. In our interview, he marveled at how far body cameras have come and argued forcefully for more disclosures.

On body cameras:

I call body cameras one of the top three technologies of major impact in the history of our profession, behind the car and the radio. I don't think we as a profession have come to the realization of how much of a game changer it is yet.

There's a number of hurdles, though. The whole point behind body cameras, from the public's perspective, is this is a transparency and accountability tool. Many agencies, however, either because of state law or local politics, are not sharing the video. That kind of defeats the purpose. Why spend millions of dollars for an accountability and transparency tool, and then nobody can see the video?

My belief is chief executives realize the minute you put a body camera on somebody and send them out to do their job, your organizational culture, your policies, your practices, your officers' adherence to the knowledge of the law, and your training are all being documented. The bigger the agency, the scarier that gets.

There's been a lot of impact, but I suspect there's going to be more to come in the future with this tiny little device. I think we are waiting to see what we can do with the images captured by this camera and the future, from a technology standpoint. I think that's the next big thing for law enforcement – what are we going to do with all this massive [amount] of data?

There is [also] this growing recognition in the profession that body camera recordings have potential to have great impact on the court systems, and that the value of the recordings from an evidentiary standpoint may be just as great, if not greater than the accountability and transparency issue for which the general public sees as a main reason that police agencies should deploy body cameras.

The views expressed in this interview are those of the interviewer and do not necessarily reflect the official position of any agency or organization.

"I could potentially walk down the street with the camera in real time, scanning faces, sending that data back to the cloud. That type of real-time, big data application would be huge."

On the future of body cameras:

What we want to do, what we could do, and what society will accept are a number of different things.

There's going to be a long, hard discussion in legislatures and in the court of public opinion regarding facial recognition technology. We indeed have become a surveillance society. What will be the point where the public will say "Enough is enough"? That perception of the public is going to have a huge impact.

But the fact that I could potentially walk down the street with a camera in real time, scanning faces, doing facial recognition while it's recording, sending that data to the cloud for real-time analysis, have that data come back and somebody tell me, "That guy in the red hat, red shoes you just passed, he's wanted for burglary" That type of real-time, big data analysis application would be huge.

We're not there yet, obviously. But the future and when you crack open those layers of technology, the impact on courts and the justice system, it can go both ways. We don't know what's going to happen. You used to be able to go up and slap a tracker on a car, for a guy who's under surveillance, and then the Supreme Court ruled a couple years ago that's a Fourth Amendment violation. That's an example of technology affecting the legal world, which then turns around and affects police operations.

On public disclosures:

[One] issue that many agencies and local governments are very concerned about is the release of video to the public. This is one of the big discussions in body cameras right now.

As I said earlier, if you're not going to share the video, well, what's the point? Why are we spending the money? There can be measured process to do that which balances public expectation and privacy issues.

Unfortunately, we in law enforcement are being put in squarely in the middle, being the arbiters of what's private and what's evidence.

But we need to be a little more critical of ourselves and how well we're executing that piece of the contract with the citizens we police. Because this idea of "I record an hour of video, but only two minutes is evidentiary. Therefore, you don't get to see any of it" is over-reaching. We need to do better at that as a profession.

I think in some cases we're hiding too much behind that evidence and privacy as a reason not to release video. When the cameras first came out, redaction was the big grind. Now we're kind of past that. And now it becomes, "Yeah, we can redact it, but it's the process to manage all that. That's going to cost resources."

We've got a million reasons why we can't do it, and very few people talking about why we should and how we can.

Some agencies have been very open with releases, and it has paid dividends for them. And you've got other agencies that are constantly in the news because they won't release anything. I believe we can effectively balance privacy, evidence protection and accountability if we put our collective minds to it.

6 states including North Carolina exempt body camera footage.

[Source: http://reason.com/blog/2016/07/14/north-carolina-exempts-police-body-cam-f]

BRINGING EVENTS TO LIFE IN COURT: A DEPUTY DISTRICT ATTORNEY'S THOUGHTS

Few areas have been as affected by body cameras as the courts. San Diego County Deputy District Attorney Damon Mosler expects that soon nearly all of his cases will involve body camera footage. In our wide-ranging conversation, we talked about handling jury expectations of video evidence and the value of having an officer's first contact with a victim or suspect on video.

How has body-worn video affected the court systems? What have been the hurdles, the benefits?

When we are able to introduce video evidence of the initial contact with certain victims, it can be very compelling evidence — much more so than a written report or a person months later testifying and talking about what occurred.

The raw emotional aspect of when they first contact or have contact with the police and describe whatever occurred to them is very powerful. We had one case in particular that was a rape case, and the police report said that the victim was upset. Well, that's correct. But the word upset is only five letters, and didn't convey the impact of her sobbing hysterically when they first responded, telling where the attacker was. The DA who presented that evidence said that the judge almost cried.

That to me is very compelling. I think we will see that more than perhaps necessarily crimes caught on tape, but to see and assess victims and witnesses when they're first contacted by law enforcement I think will show their trustworthiness — more so than I think we're concerned with showing law enforcement's trustworthiness, which is ostensibly what the cameras are for. So I think it will bring the events more to life in court, and I think that can be very powerful, so I am looking forward to seeing that develop.

Challenges will be that we have to provide transcripts of everything we introduce when we introduce video and audio.

It's also just reviewing evidence for discovery — a lot more now that it's videos.

"I think the cameras and using artificial intelligence would be helpful in generating the police report itself."

Where do you personally see the courts headed in the next 5 to 10 years when it comes to technology?

They're going to be the slowest stakeholder partner on the technology side. That's for a multitude of reasons.

One is just the resources. They're the very, very end users. Very little gets there.

What I think we'll see is definitely more video or digital evidence being used in court, in a variety of different presentation modes, whether that's just playing the video or incorporating it into a demonstration of what occurred if we can recreate from the original crime scene when the officer shows up and to backtrack out in terms of showing the crime.

I think the cameras and using artificial intelligence would be helpful in generating the police report itself, In a standardized way that makes it easier for prosecutors to understand what's in the report. Ultimately the witnesses and the officer's observations are the evidence, not a physical report. But we make decisions off physical reports.

"We use so many words recently — transparency, accountability, and privacy. None of those are the same definition that they were 10 years ago."

How do you think courts deal with the change in privacy that comes with all of this video evidence, and will it change as video becomes more widespread and expected?

I think in this day and age we have a much lower true expectation of privacy. I don't think privacy is defined the same way as it once was.

The reality is, when you call an officer and they physically go to your house, you've lost that expectation of privacy anyway. Now we just have a better documentation of it. The biggest issue will be in respect to all of that is the wholesale public release of those types of things.

But increasingly, we have a society that doesn't seem to be bothered by that, with all of the things we see posted almost instantaneously in social media in some fashion. I think people have foregone that, and technology has just made them desensitized to actual and true privacy the way it was understood years ago.

I know that's a concern of many people. We use so many words recently — transparency, accountability, and privacy. None of those are the same definition that they were 10 years ago when body cameras first started or 5 years ago.

There's no transparency unless we release all the videos, but then we're affecting people's privacy. There's a continuum of impact on all of this stuff. I don't know where we are or where society will accept it.

Speaking of shifting definitions, how would you define success when it comes to technology in the courtroom?

In the criminal justice system, I believe we seek justice for the crime victims, and justice is for someone being held accountable. We also seek fair trials. I am not sure that component really can change.

002
SAFE &
SECURE

STAYING ONE STEP AHEAD

If technology is rapidly changing, do agencies' security concerns need to shift as well?

As more devices come to market, agencies need to be vigilant about which technology providers they can trust. And they can't forget about core security principles, like creating strong passwords and not falling for phishing emails.

SAME THREATS, NEW METHODS

Over 80%

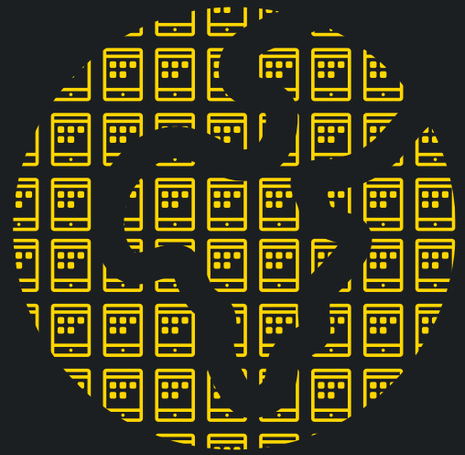
The percentage of data breaches that came from external threats instead of internal agents

[Source: 2016 Verizon Data Breach Investigations Report]

200 billion

The number of smart devices expected to be in use in 2020

[Source: 2016 Verizon Data Breach Investigations Report]



Top Worst Passwords

Rank	Password	Rank	Password
1	123456	14	111111
2	PASSWORD	15	1QAZ2WSX
3	12345678	16	DRAGON
4	QWERTY	17	MASTER
5	12345	18	MONKEY
6	123456789	19	LETMEIN
7	FOOTBALL	20	LOGIN
8	1234	21	PRINCESS
9	1234567	22	QWERTYUIOP
10	BASEBALL	23	SOLO
11	WELCOME	24	PASSWORD
12	1234567890	25	STARWARS
13	ABC123		

[Source: SplashData 2016]

Top 3 reasons for hacking

[Source: Verizon]

1. **Financial gain**
2. **Espionage**
3. **Fun**

5 SECURITY TIPS AND PREDICTIONS

Some companies and organizations don't think about security until they find themselves in the headlines. We sat down with TASER's VP of Information Security Jenner Holden to get his top five tips and predictions on how agencies can protect themselves and where he sees technology heading.

1. Your biggest threat isn't necessarily an insider threat.

What it's traditionally been — there's always been more attacks from the outside, but the insider attacks tended to be the more impactful ones. Less frequent, but more impactful.

Over the last two years or so—and this trend will continue—that's changing, where the external attacks still happen more frequently, but they're becoming more impactful.

For law enforcement, I think it's the same. Their biggest threat are external attackers, hacktivists like Anonymous — not so much an internal rogue IT guy or law enforcement officer who decides they want to hurt their own agency.

****

Passwords Make Perfect

It's easy to predict how most people build passwords. Don't fall for the standard routine of capitalizing the first letter, adding a number after the letters, and ending it all with an exclamation point.

2. Front-line officers need to keep track of passwords and phishing emails.

Don't be the guy that has the really easy-to-guess password.

Being aware of phishing emails is the other [tip]. You could be a target. You need to look carefully at the emails that you get and don't click on them or open the attachment if they don't look quite right or if you're suspicious.

3. Agencies should consider the cloud for increased security.

Is your email going to be more secure running your own exchange server on-premise with your one IT guy trying to take care of it, along with everybody's workstations and everything else, or would your email be more secure running in the cloud with Microsoft's Office 365?

I think we're at the point where finally everyone would agree that it's better in Office 365 in the cloud. And that just needs to be further recognized and further developed. Every system that you do for law enforcement is probably going to be more secure if you do it in the cloud.

Cloud Coverage

Companies with cloud-based web security solutions see...

58% fewer

malware incidents

45% fewer

fewer incidents of data loss or exposure

Greater security levels than what law enforcement agencies could meet by themselves

[Source: http://www.ijis.org/resource/collection/232074EF-6453-4014-BC4E-018BF818D291/Mitigating_Risks_in_the_Application_of_Cloud_Computing_in_Law_Enforcement.pdf]

4. Hackers are targeting smart devices.

The big trends that have already started and will continue is Internet of Things security — right along the lines with our cameras and docking stations, which are Internet-connected devices. In the home, it's your smart devices, your smart locks, your smart lights, your smart outlets, your smart TVs, all those kinds of things.

Each one of those are like little computers. If they're not properly built, supported, patched, and monitored, they're a place to hack into and cause havoc.

The Internet of Things [devices] will be leveraged as launching points for different attacks, which means the providers then, on the counter to that, will be on the hook more. There will be more scrutiny.

Where's my internet?

The October 2016 DNS outage caused by compromised Internet-connected devices slowed or temporarily took down websites like Reddit, Amazon, and Twitter.

[Source: http://www.forbes.com/sites/briansolomon/2016/10/21/hacked-camer-as-cyber-attack-hacking-ddos-dyn-twitter-netflix/#6cf2298f7e6f]

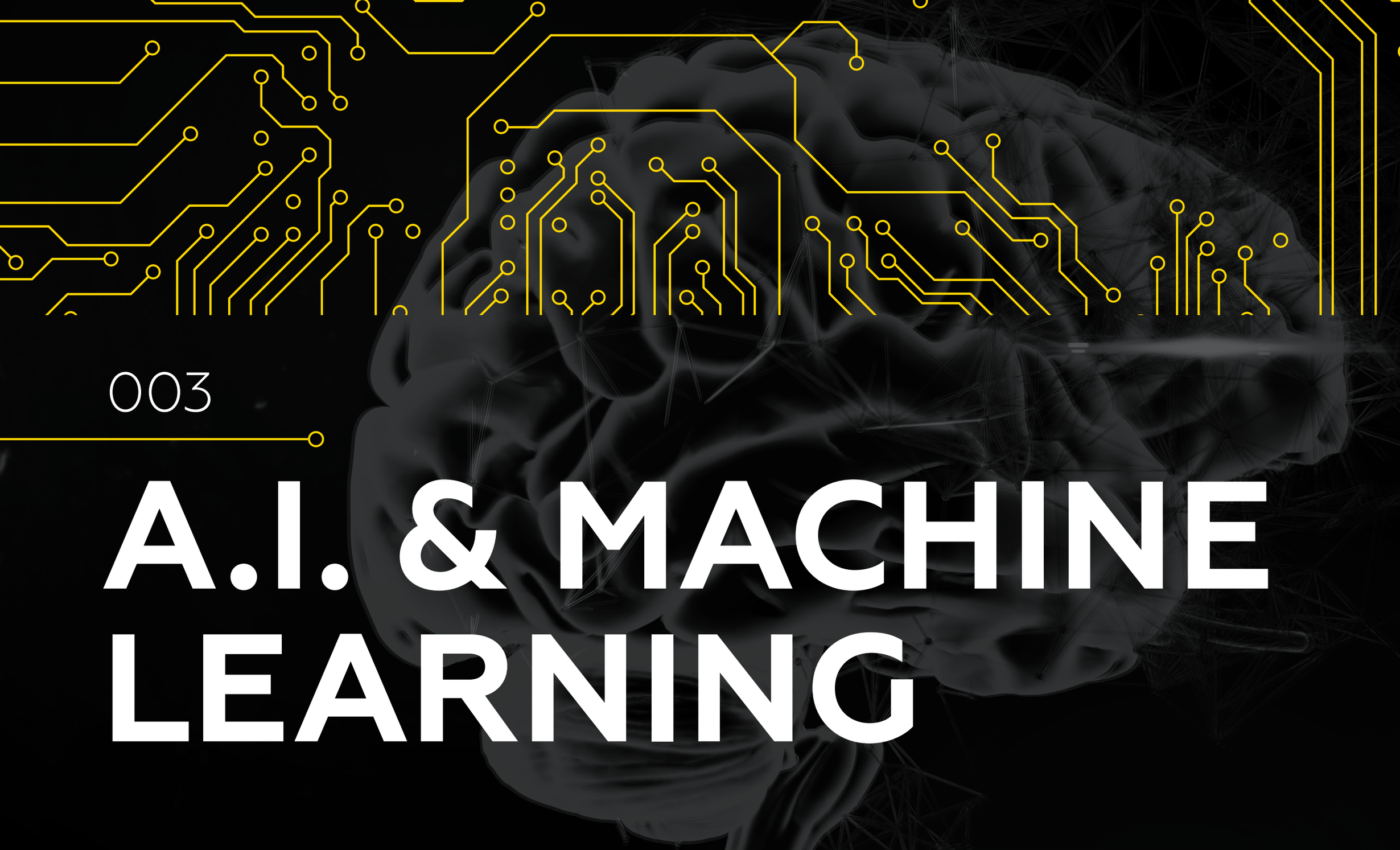
The Internet company Dyn reported they received "tens of millions" of messages during the attack from various smart devices.

[Source: http://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/]

5. The federal government will likely be slow to issue new standards and regulations.

There's already guidance coming from the federal government on how to build Internet of Things devices securely. You can expect regulations coming from the government that say, "Hey, if you're going to build an Internet-connected or smart device for the home or office, it must meet these security standards."

There might even be a body in the next five years that has to certify those, like we do with a lot of other things. Well, the big attacks have already happened. So it's going to be a little bit of a mess for a few years, and these Internet of Things devices hitting the market won't all be very secure, and there will be problems. But that's no different from any set of technologies.



003

A.I. & MACHINE LEARNING

REAL-TIME TECH, REAL-WORLD IMPACT

Body cameras have transformed law enforcement, but now agencies need to make the most of their data.

Major corporations like Walmart have already started to tap into their massive datasets to serve their customers, becoming able to predict exactly what they would like based off of previous purchases.

Soon, law enforcement agencies will be able to leverage those same technology principles to provide their officers with real-time analysis, automate their manual processes, and predict future events.

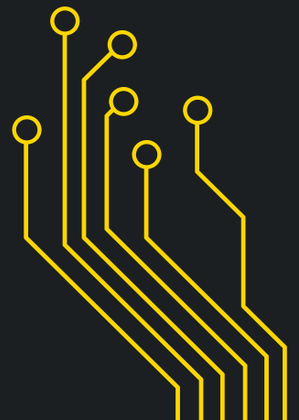
MORE INSTANT

Imagine you can find out if someone has a criminal record instantly — or be notified if someone's demeanor has changed and may now be a threat.

3,500,000,000
Google searches per day

and advancements in machine learnings are helping them tailor the results to each user

[Sources www.internetlivestats.com/google-search-statistics & www.zenithmedia.com/artificial-intelligence-enhances-role-search]



MORE AUTOMATED

What if reports were generated from all the information within body camera footage? The videos could report how far a subject was from the officer and exactly when events occurred and where.

85%

is the percentage of customer interactions that Gartner estimates will occur without human intervention by 2020, cutting wait times and the need for call centers

[Source: www.gartner.com/imagesrv/summits/docs/na/customer-360/C360_2011_brochure_FINAL.pdf]

MORE CONFIDENT

Body cameras could provide officers with more robust training, giving them better situational preparedness. Agencies could also analyze their data to anticipate criminal activity and better allocate their resources.

European banks that swapped their statistical models for machine learning techniques have seen:

10% greater sales of new products

20% greater savings in capital expenditures

20% jump in cash collections

[Source: www.mckinsey.com/industries/high-tech/our-insights/an-executives-guide-to-machine-learning]

IT'S ALL ABOUT DATA: MICROSOFT'S CLOUD-CONNECTED FUTURE

For Jeff King, Senior Solutions Architect at Microsoft, data will drive the future. He shared his thoughts on how agencies can leverage the cloud to make policing smarter and more effective in real-time.

On the top technology trends:

As agencies invest in cloud-based technology solutions, we're beginning to see a high demand for technologies related to the Internet of Things. Much of this is for scale – agencies are investing in sensor-based devices that act as force multipliers. These Internet connected devices (like camera systems and gunshot detectors) allow officers to be in more places at once, capturing and processing data in real-time. First responders are also wearing sensor based equipment: smart weapons and holsters, cameras, and biometric devices, all of which generate, process, and transmit data over the internet. This data can be used by officers both in real-time as well as after the fact. Think of a scenario where an agency could detect when one of their officers has drawn their weapon, and then be able to connect in real-time to their body-worn camera. Dispatchers could relay important information back to other officers responding to the same call, and secondary data could be analyzed after the fact and used for training purposes or crime analysis.

On the greatest challenges agencies face:

As law enforcement agencies begin to embrace new technologies, they are having to manage data in a completely different way. They need to keep it for longer, ensure that it cannot be compromised, is durable (backed-up), and that the data centers storing the data comply with the regulatory compliance guidelines mandated by the FBI like the CJIS Security Policy. They also need to be able to process all this data. Agencies have petabytes of content that they have captured but lack the resources to be able to manually extract important information. Faces, objects, crowd and vehicle movement, can all provide important clues for investigators, as well as real-time information for dispatchers or officers in a real-time-crime-center. Imagine how powerful a camera system could be if it could detect and notify officers in real-time if someone had a weapon at a specific location.

On where technology is headed:

There are clear answers for many of the technology challenges the law enforcement community is facing, and it really all begins with cloud computing. The cloud offers agencies the ability to store and process their data at scale, remain CJIS compliant, take advantage of world-class data protection and security, leverage artificial intelligence capabilities which address citizen privacy concerns, and provide new ways to analyze the data.

A key advantage to cloud is having access to so much data processing power. Using artificial intelligence and hyper-scale compute, agencies can rapidly process digital video, extracting and logging important information automatically. This is an important milestone in the industry – prior to artificial intelligence this analysis would require humans. Now we can ingest data from several thousand cameras pointed at a street corner and automatically detect and flag anomalies as they occur —packages left on corners, a person walking in one direction while the crowd is running in the opposite direction.

Other applications include, automatic redaction (blurring of faces to protect privacy), also once a manual and expensive process, automatic extraction of spoken content, emotion detection, object detection and tagging—the capabilities are endless...

On how Microsoft looks to the future:

We're deepening our investments in cloud computing. We've launched Microsoft Azure for Government, designed specifically for government workloads. We've signed the FBI CJIS security addendum in 26 different states, which is an important and so far incomparable milestone in the industry.

Public safety agencies are undergoing a digital transformation – they require world-class technologies to help them accomplish their mission. We're now looking to other public safety providers to create solutions that are hosted in our cloud, and are growing our portfolio of Azure services everyday. New data centers, artificial intelligence, new data analysis tools, IoT services, and much more.

What we do at Microsoft is all about giving [public safety] a platform so they can leverage all of the different capabilities cloud computing brings our public sector customers. And we do that in a way that keeps communities and officers safer every day.

RADICAL CHANGE, FAST: ONE WORLD-RENOWNED RESEARCHER'S EXPECTATIONS

What if machines are smarter than humans — and what if they can help save officers' lives? We spoke about advancements in artificial intelligence with Dr. George Poste, a renowned researcher, scientist, and scholar, who founded Arizona State University's Biodesign Institute and was a past recipient of R&D Magazine's "Scientist of the Year" award.

On technology enhancing officer judgment:

I'd like to think that ... it would be beneficial. But of course it does require that absolute precision in identification.

So if the camera-video-identification-communication loop is robust, it definitely helps. If an officer is alerted that an individual has a known criminal record, or propensity to violence, even if he has not yet adopted a threatening posture, it heightens the overall threshold of awareness. But if the message comes back that it looks like the person has an impeccable record, no arrest or any other difficulty, then the officer is in a much more relaxed setting immediately.

"Autonomous systems will gain in importance in law enforcement. You're saving police officers' lives by using robots, autonomous vehicles or other systems"

On the evolution of autonomous systems:

A.I. and machine learning is undoubtedly affecting literally every sphere of the human endeavor. We've clearly seen the first wave of automation and decision support systems displacing elements of the workforce. That's clearly going to continue, together with increasingly sophisticated robotics.

What will be the place of autonomous systems in law enforcement? We already have the Dallas police shooting where a robot was used to kill the assailant. If you look at the overall evolution of this type of autonomous system, it may not yet be approaching the fully futuristic dimension of Robocop where you essentially have someone wearing an exoskeleton linked to advanced artificial intelligence capabilities.

But autonomous systems will undoubtedly gain in importance in law enforcement just as they have with the military. You're saving police officers' lives by using robots, autonomous vehicles or other autonomous systems. But then, of course, adoption of lethal autonomous systems raises profound ethical and legal questions for society. For example what is the nature of the software and the pre-set decision threshold at which action to kill is taken and who designs the software and approves the decision criteria?

You've got parallel tracks of technology for law enforcement and technology for the military, plus many of the same technology platforms are associated with advances in other fields, including GIS, medicine, manufacturing, and so forth. In addition, many of these also fall into the so-called "dual use" technology category in which the same information can be used for activities that society deems beneficial and other activities that may be harmful or raise significant societal concerns.

On predictive policing:

Whatever you did for your online Christmas shopping this year, which is the only way I did mine, I'm now bombarded with a whole series of related materials that pertain to my apparent purchasing choices and preferences. You also see this in health care where clearly many elements of decision support software are now eclipsing, in a superior way, the judgment of highly trained professionals, simply because the scale and multidimensionality of the data sets quickly eclipses the cognitive capacity of humans.

We may not be quite at the Tom Cruise 'Minority Report' level of cognitive prediction, but patterns of individual behavior will become increasingly informative in revealing the probability that an individual will act in a particular fashion. And as our data sets become ever bigger, the analytical algorithms will become ever more sophisticated in revealing robust patterns. It is inevitable that predictive policing will expand. I don't view this to be a bad thing and is consistent with TASER's two principles: protect life; protect truth. Any technology platform that can advance these two laudable goals, while protecting the privacy and rights of innocent citizens should, and indeed must, be adopted.

Data-Driven Decisions

2.5 petabytes: The amount of data Walmart analyzes each hour to predict customer needs.

[Source: https://www.dezyre.com/article/how-big-data-analysis-helped-increase-walmarts-sales-turnover/109]

‘WE’RE NOT EVEN AT 1.0’: A DISCUSSION WITH TASER’S EVP OF AXON DEVICES

We sat down with Todd Basche, TASER’s EVP of Axon Devices, to hear where he saw technology headed and why he joined the company in 2016 after an illustrious career that included pitching ideas to Steve Jobs at Apple.

Why did you get involved with TASER?

I love the stat that police officers spend 60% of their time doing mundane paperwork. If we spent 60% of our time that way in product development, we’d still be putting out fax machines. But technology really transforms these spaces, and I think we’re not even at a 1.0 where we are today with Axon and the cameras and the weapons and the cloud-based software.

Officer or Data Entry Clerk?

In surveys we’ve sent to law enforcement officials, we’ve found that respondents report that they can spend as much as two-thirds of their day on paperwork.

How do you think these advancements would affect the day-to-day job of law enforcement officials?

It's so silly that the officer has to write down, "I got out of the car at 6:02, I walked over to the subject, here's what I said to him, here's what he said to me." It's all in the video.

I mean, Google Photos can tell you that your dog is standing in front of the Eiffel Tower. In the not-too-distant future, everything the officer does in the video will be able to be transcribed, like the voice is transcribed.

A Picture Says a Thousand Words

Google Photos analyzes previously published photos to find patterns and determine what is in a photo. The service boasts a captioning accuracy rate of over 93%.

[Source: http://www.forbes.com/sites/paulmonckton/2016/09/29/google-show-and-tell-update/#6ab26ead7eb6]

What privacy concerns arise from all the things we should be able to do in the next 5-10 years?

That's a good question. If I look at the person and can tell that person is a known wanted criminal, did I violate their privacy? I don't know. He or she is still wanted. They're in the database. They committed a crime.

And if they didn't, and you tell them, "Ok, this person isn't a criminal," I don't know. I think privacy is an important concern, but I think if an officer is standing there talking to you, he's going to ask for license and registration and all those kinds of things — is that different from us automatically identifying the guy?

So the nature of privacy transforms as technology changes?

I think so.

When the telephone was invented, people were really upset because they said it's the end of real relationships, that talking to someone on the phone is so disconnected from a face-to-face conversation that it will never catch on in a legitimate use.

Now we have every form of communication you can imagine. We're texting... we take all of those as "I talked to that person." Did you really talk to them? You mean voice to voice? Oh God no. I think the nature of communication changes, and I think the nature of privacy evolves.

But do you ever see technology displacing the actual job of law enforcement?

No.

I think what it does is it lets the officer spend more of their time actually doing [the job of] law enforcement. The other thing is if they start to see the cameras and the recording and the richness of the experience as a teaching tool. Let's say that was institutionalized and they went back at the end of the week and had to spend an hour looking at their highlights, and the software edited it up.

You know how Facebook does their year in review? It could say, "Hey, here's your week — here's the interactions you had, and pick the top ten interactions you had."

You could watch it and say, "Uh, you know what? I should have used more patience there. If I had spent five more minutes with this person, I could have talked them down. I could have deescalated the situation better by watching myself."

It's a feedback tool — not a "big brother is watching" tool.

But these advancements aren't just confined to law enforcement...

I think the rest of public service hasn't thought through how this technology could be helpful to them.

I think real-life training — turning these things into situational training cases that make everybody better at their job very inexpensively. And people getting better at their job saves more lives, both them and other people.

READY FOR THE FUTURE

The future of policing looks smarter and more connected. Advancements in artificial intelligence will help officers act confidently in real time. Agencies will automate manual processes like report-writing and even be able to anticipate future events.

We'll be keeping a close watch as these thoughts and predictions bear out.

FOR MORE ON THE SUBJECTS

Want to learn more about the current state of technology? Here's some additional recommended reading you may find interesting.

BODY CAMERAS: THE LATEST POLICIES AND RESEARCH

State legislatures across the country are debating new legislation related to the use of body cameras. To learn more about the latest policy developments and research, take a look at the National Conference of State Legislature's body camera guide.

[Source: http://www.ncsl.org/research/civil-and-criminal-justice/body-worn-camer-as-interactive-graphic.aspx#/]

SECURITY: VERIZON DATA BREACH REPORT

Want to know where data breaches are occurring, and why? Check out Verizon's annual Data Breach Investigations Report, which tracks the latest security trends.

[Source: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/]

A.I.: HOW GOOGLE IMPROVED GOOGLE TRANSLATE

Still stumped about artificial intelligence? Catch up on how Google dramatically improved Google Translate results by taking advantage of advancements in artificial intelligence technology.

[Source: https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html?_r=0]

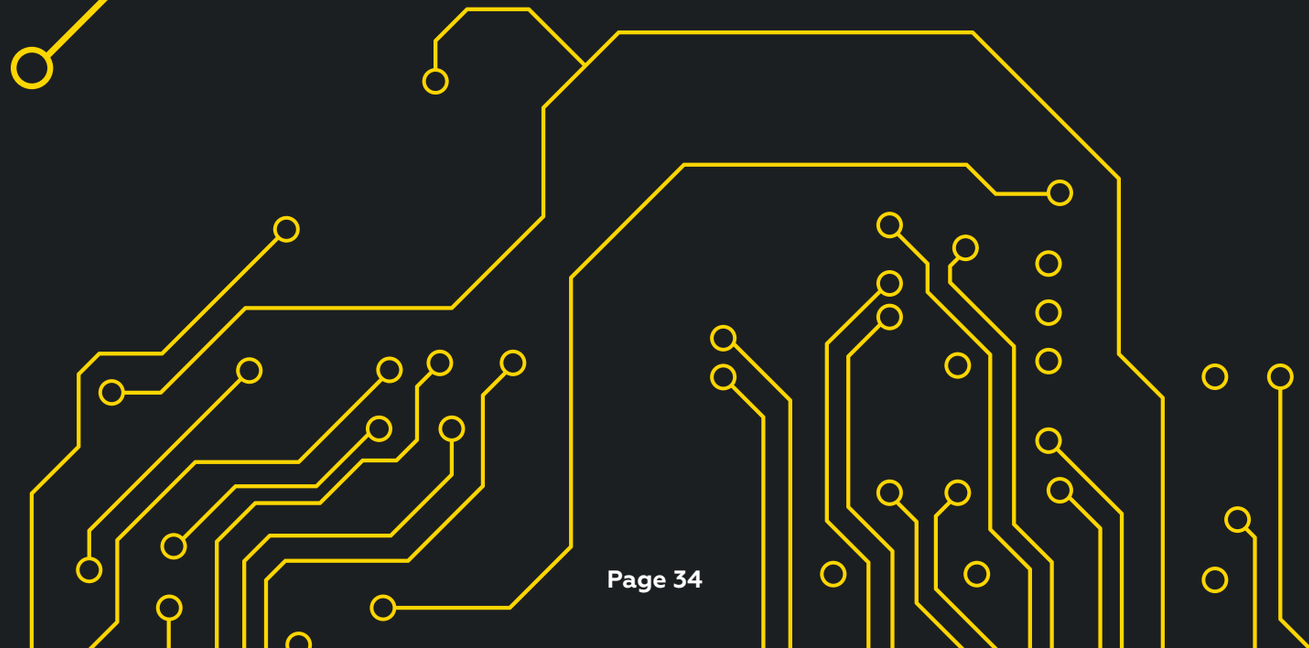
AXON ACCELERATE: BUILD THE FUTURE WITH US

Is your agency ready for all that new technology has to offer?

Join us at the Axon Accelerate conference on June 20-21 to get to the future faster.

At Axon Accelerate, you'll learn how to deploy cutting-edge technologies, network with other law enforcement professionals, and help us build new devices and apps that let you do your job more efficiently than ever before.

axon.io/conference



Amazon is a trademark of Amazon; Facebook is a trademark of Facebook, Inc.; Google, Google Photos, and Google Translate are trademarks of Google Inc.; Twitter is a trademark of Twitter, Inc.; Reddit is a trademark of Reddit, Inc., Verizon Wireless is a trademark of Verizon Trademark Services, LLC; and Walmart is a trademark of Wal-Mart Stores, Inc.

, Axon, TASER, and are trademarks of TASER International, Inc., some of which are registered in the US and other countries. For more information, visit www.taser.com/legal. All rights reserved. © 2017 TASER International, Inc.