License Plate Readers Exposed! How Public Safety Agencies Responded to Major Vulnerabilities in Vehicle Surveillance Tech

Cooper Quintin and Dave Maass ⋮ 17-22 minutes ⋮ 10/28/2015

Law enforcement agencies around the country have been all too eager to adopt mass surveillance technologies, but sometimes they have put little effort into ensuring the systems are secure and the sensitive data they collect on everyday people is protected.

Case in point: automated license plate recognition (ALPR) systems.

Earlier this year, EFF learned that more than a hundred ALPR cameras were exposed online, often with totally open Web pages accessible by anyone with a browser. In five cases, we were able to track the cameras to their sources: St. Tammany Parish Sheriff's Office, Jefferson Parish Sheriff's Office, and the Kenner Police in Louisiana; Hialeah Police Department in Florida; and the University of Southern California's public safety department. These cases are very similar, but unrelated to, major vulnerabilities in Boston's ALPR network uncovered in September by DigBoston and the Boston Institute for Nonprofit Journalism.

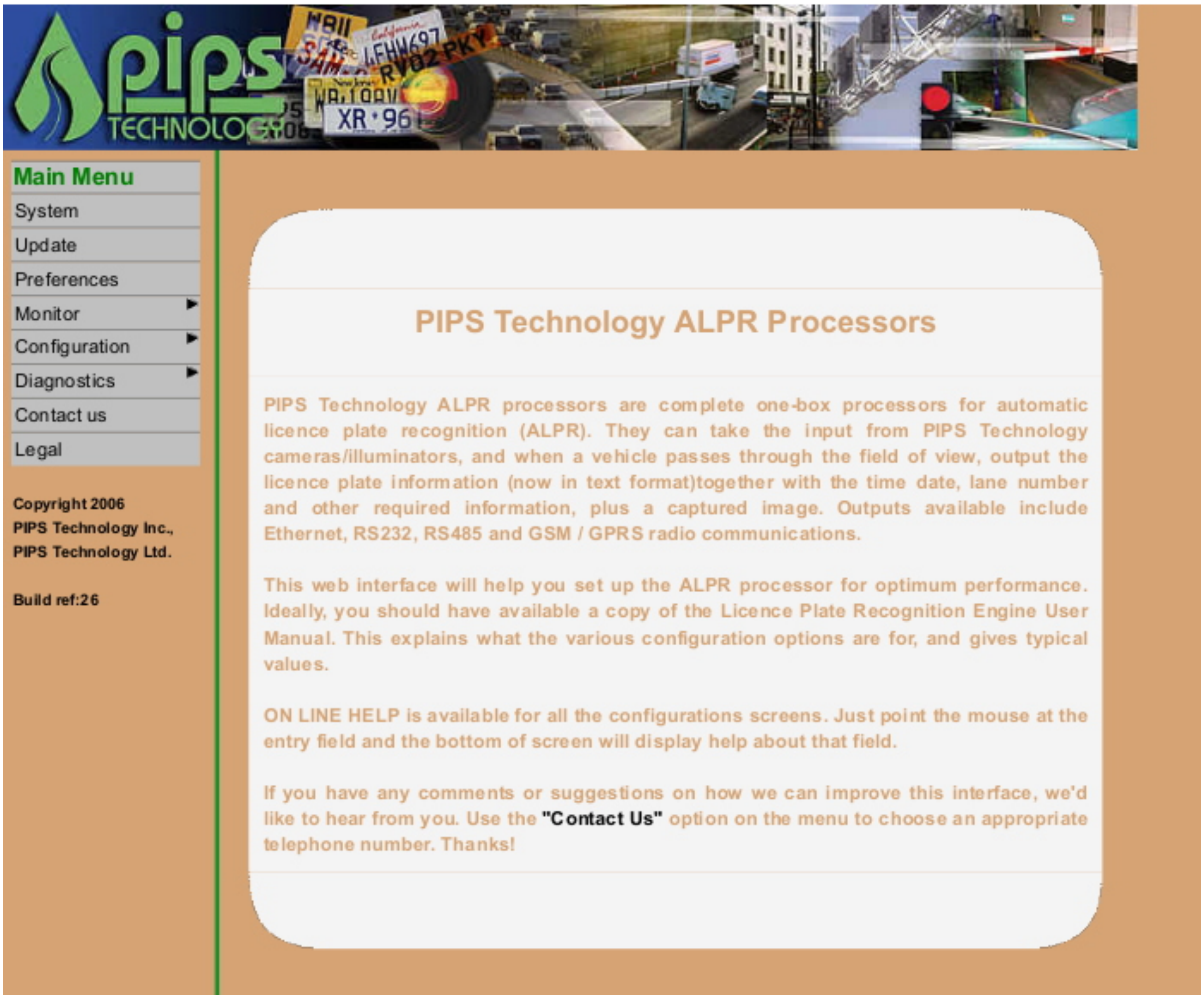
After five months of engagement with these entities, we are releasing the results of our research and the actions these offices undertook in response to our warnings.

What is ALPR?

ALPRs are networks of cameras that take pictures of every passing car and capture data on each car's license plate number, including the time, date, and location where the vehicle was photographed. ALPR cameras are often mounted on patrol cars or affixed to stationary roadside structures, such as light poles and traffic signals.

The systems will alert police when a camera recognizes a car on a "hot list," an index of cars that are stolen or believed to be tied to criminal activities. However, most ALPR systems collect and store data on *every* car (i.e. they don't distinguish between suspects and innocent civilians). Even if a vehicle isn't involved in a crime, data on where it was and when may be stored for many years, just in case the vehicle later comes under suspicion. Consequently, a breach of an ALPR system is a breach of potentially every driver's travel history. Depending on how much data has been collected, this information in aggregate can reveal all sorts of personal information, including what doctors you visit, what protests you attend, and where you work, shop, worship, and sleep at night.

The ALPR systems at the center of our investigation were sold by a company called PIPS Technology, which has since been bought by 3M. In 2011, prior to the acquisition, the company bragged of installing more than 20,000 cameras around the globe. After independent security researchers alerted us to the vulnerabilities, we discovered that many stationary ALPR cameras from PIPS were individually connected to the Internet and freely accessible online to anyone who knew where to look.



Copyright 2006
PIPS Technology Inc.,
PIPS Technology Ltd.

Build ref:26

PIPS Technology ALPR Processors

PIPS Technology ALPR processors are complete one-box processors for automatic licence plate recognition (ALPR). They can take the input from PIPS Technology cameras/illuminators, and when a vehicle passes through the field of view, output the licence plate information (now in text format)together with the time date, lane number and other required information, plus a captured image. Outputs available include Ethernet, RS232, RS485 and GSM / GPRS radio communications.

This web interface will help you set up the ALPR processor for optimum performance. Ideally, you should have available a copy of the Licence Plate Recognition Engine User Manual. This explains what the various configuration options are for, and gives typical values.

ON LINE HELP is available for all the configurations screens. Just point the mouse at the entry field and the bottom of screen will display help about that field.

If you have any comments or suggestions on how we can improve this interface, we'd like to hear from you. Use the **"Contact Us"** option on the menu to choose an appropriate telephone number. Thanks!

In some cases, anyone could open a window and view a camera's live video stream and witness the plate captures in real time. There was essentially nothing to stop someone from siphoning off the stream of ALPR data in transmission or potentially controlling the cameras. The agencies that ostensibly controlled the ALPR systems hadn't even put in place warning language about unauthorized access to the systems.

When asked about the vulnerabilities, 3M provided EFF with this written statement:

> We cannot comment on issues PIPS may have had prior to the acquisition, but I can tell you any issues with our products are taken very seriously and directly addressed with the customer.
>
> We stand behind the security features of our cameras. 3M's ALPR cameras have inherent security measures, which must be enabled, such as password protection for the serial, Telnet and web interfaces. These security features are clearly explained in our packaging.

To the agencies' credit, all the Louisiana agencies and the University of Southern California (USC) have now taken action to secure the systems.

A Brief History of ALPR Vulnerability Research

A few years ago, security researchers began to ring the alarm over what they originally misidentified as hundreds of red-light cameras that were connected to the Internet without any security measures in place. The cameras were spread throughout the country, with two distinct clusters in California and Louisiana.

Earlier this year, EFF began drilling down on the data and confirmed that these were not traffic cameras at all, but stationary ALPR systems—networks of cameras mounted on street poles to capture the plates of passing cars as part of ongoing law enforcement dragnet surveillance programs.

The first big tip we received came from John Matherly, the security specialist behind Shodan, a search engine that scans and catalogs connected devices and hardware, i.e. the Internet of Things. If you plugged certain keywords into Shodan, the site retrieved hundreds of PIPS camera systems connected to the Internet, often with control panels open and completely accessible through a Web browser. At the time, Matherly and his colleague Dan Tentler highlighted these vulnerabilities at security conferences. CNN even talked about these cameras while featuring Tentler's work.

When CNN contacted 3M in 2013, the company disclaimed responsibility:

> 3M spokeswoman Jacqueline Berry noted that Autoplate's systems feature robust security protocols, including password protection and encryption. They just have to be used.
>
> "We're very confident in the security of our systems," she said.

Independently, a researcher named Darius Freamon found that you could access the control panels via Telnet and generate statistics about plate captures. Building off Freamon's work, a team of computer scientists at the University of Arizona dug further into the data and found vulnerable cameras in Washington, California, Texas, Oklahoma, Louisiana, Mississippi, Alabama, Florida, Virginia, Ohio, and Pennsylvania. The largest cluster was in southeastern Louisiana.

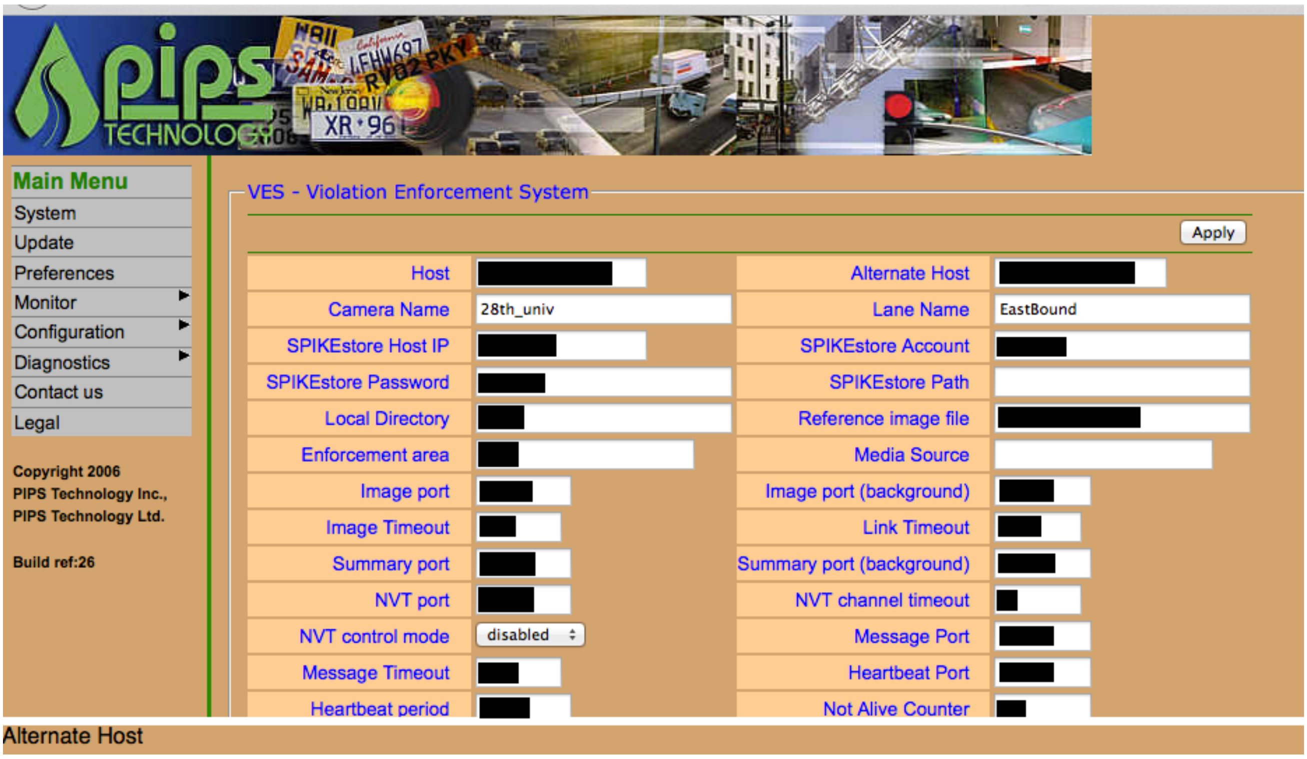
Alarmingly, these researchers reported:

> We were able to observe the number plate information and live images. We were also able to modify the configuration settings.

Matherly revisited the issue this year, presenting at the Hack in the Box conference on how he easily siphoned 64,000 plate images and corresponding locational data points from these cameras over a one-week period.

EFF began confirming this research in spring 2015. We tested more than 100 cameras, documenting when they had publicly viewable configuration Web pages, Telnet access, and especially when a visitor was able to view live feeds and capture data. The testing process involved confirming that a camera was online and responding to requests by connecting to it with a Web browser or by connecting to it over Telnet. If the camera had a password on both the Web and Telnet interface we left it alone, but if the camera was not protected with a password we were able to recover configuration information. However, when the Web was locked down, but Telnet was not, we were sometimes able to view password information in the Telnet configuration. Often these passwords were set to the default or were otherwise not sophisticated enough to be secure.

We also began to use information embedded in these pages to map out the specific location of these cameras, which we then linked to news articles and public records showing which agencies were likely responsible for the cameras (the USC cameras were obvious, because they had giveaway URLs, such as "Pipscam7.usc.edu"). Using information contained within the configuration and Google Streetview, we were able pinpoint the location of these cameras.



VES - Violation Enforcement System

Host	[redacted]	Alternate Host	[redacted]
Camera Name	28th_univ	Lane Name	EastBound
SPIKEstore Host IP	[redacted]	SPIKEstore Account	[redacted]
SPIKEstore Password	[redacted]	SPIKEstore Path	
Local Directory	[redacted]	Reference image file	[redacted]
Enforcement area	[redacted]	Media Source	
Image port	[redacted]	Image port (background)	[redacted]
Image Timeout	[redacted]	Link Timeout	[redacted]
Summary port	[redacted]	Summary port (background)	[redacted]
NVT port	[redacted]	NVT channel timeout	[redacted]
NVT control mode	disabled	Message Port	[redacted]
Message Timeout	[redacted]	Heartbeat Port	[redacted]
Heartbeat period	[redacted]	Not Alive Counter	[redacted]

Vulnerability Disclosures

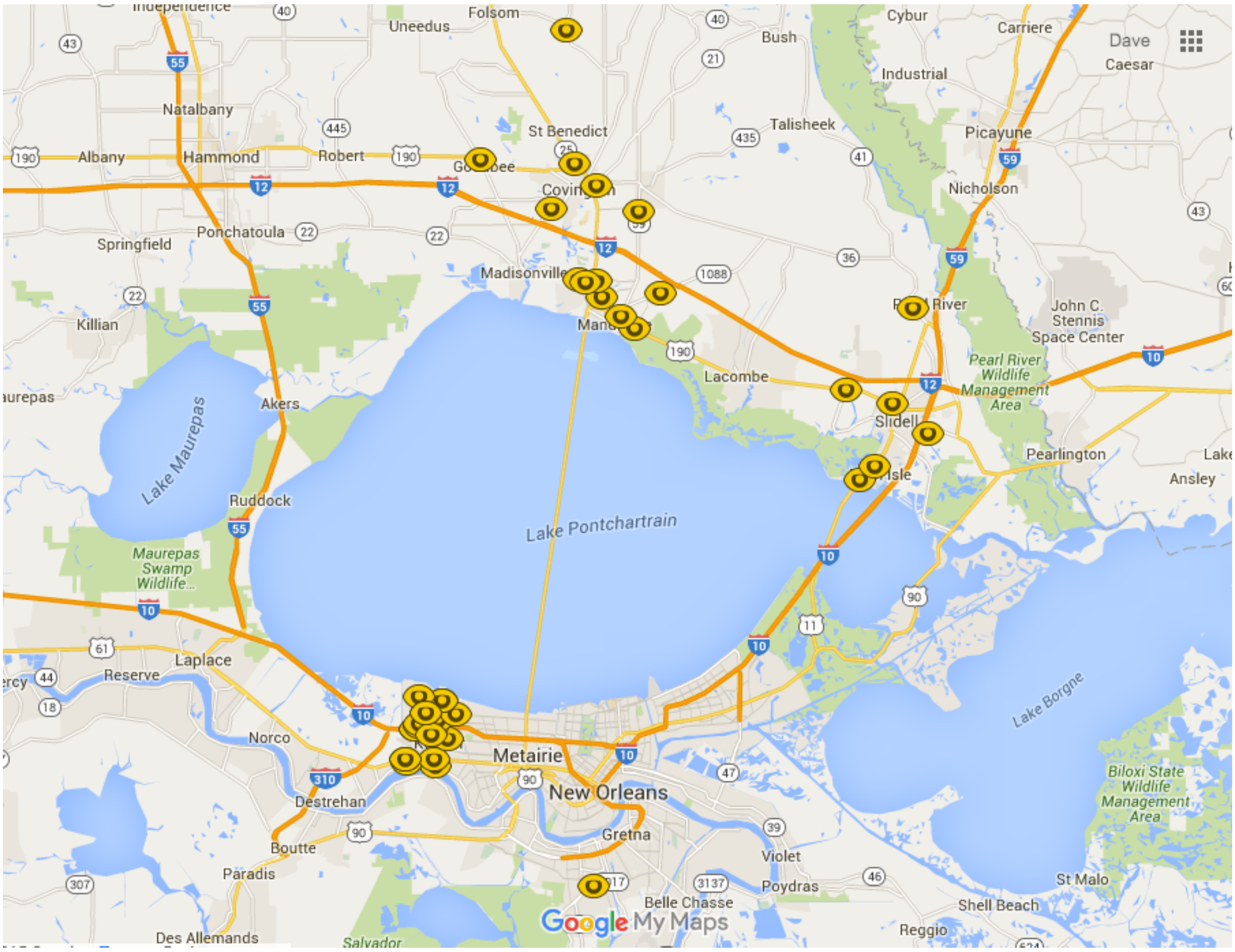
As longtime critics of mass surveillance systems, EFF would like nothing more than to see a law enforcement agency take its ALPR networks offline. In fact, in letters and emails we sent to the agencies, we advised that a shut down would be the most effective measure. But that’s a decision for the agencies to make, not computer researchers. Our greatest concern was ensuring that, if they were going to continue to use these systems, they not put the public’s privacy at risk of a data breach.

When probing the ALPR systems, EFF was careful to observe and document our findings. We did not change any configurations or otherwise tamper with the systems. Instead, we connected to the systems via Web browsers and public Telnet interfaces. We took notes and screen captures, and used that data to compose our letters to the agencies. At that time, we told the agencies that we would not release our data until they had enough time to fix the gaping holes in their security.

EFF is not publishing the letters we sent or the communications we received in response. However, we encourage reporters to pose questions and file public records requests. The agencies themselves are best suited to know what information can and cannot be released.

We are, however, comfortable sharing images and general descriptions of what we found—including the location of the cameras, most of which are otherwise visible on the street.

Southeastern Louisiana



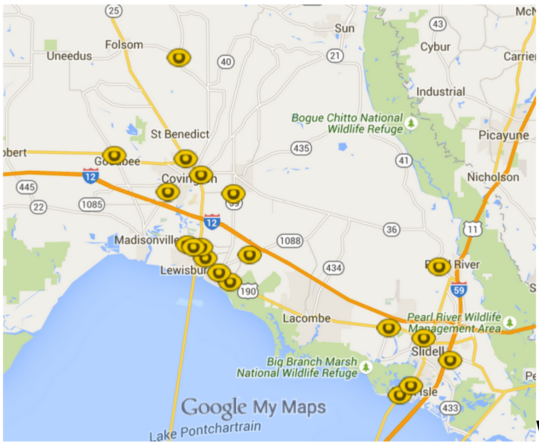
We have created this interactive map showing the location of approximately 40 ALPR cameras based on information contained in each camera's configuration.

Launch map of suspected ALPR cameras in southeastern Louisiana (Note, this map is hosted by Google. If you click this link, your visit to Google Maps will be governed by Google's privacy policy.)

These geolocation points may not be 100% accurate, since the location descriptions of some cameras were often vague or misspelled. Whenever possible, we confirmed the existence of each cameras using Google Streetview. In those cases, follow the links to see the camera's exact location.

The Louisiana cameras were generally clustered on the north and south banks of Lake Pontchartrain. News articles indicated that agencies in the region began installing the PIPS cameras as early as 2008. At first we could not definitively determine which cameras belonged to which agency, so we sent letters and emails to five separate agencies. It turned out approximately half the cameras belonged to the St. Tammany Parish Sheriffs Office, half belonged to the Kenner Police Department, and at least one camera belonged to the Jefferson Parish Sheriff's Office.

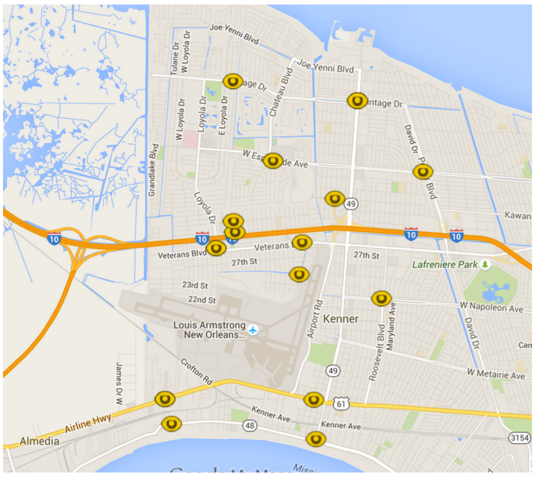
St. Tammany Parish Sheriff's Office



When contacted by EFF, the St. Tammany Parish Sheriff's Office immediately began reevaluating their systems and investigating both short-term and longer-term fixes to ensure the systems were not publicly accessible. The agency engaged in daily conversations with contractors and site visits to each camera. EFF also honored the office's request to rescan the devices once the new security measures were put in place.

As of publication, we believe the St. Tammany system has been secured.

Kenner Police Department



Early on, we believed these cameras could have belonged to the Jefferson Parish Sheriff's Office, based on news articles about the agency's long-running ALPR system.

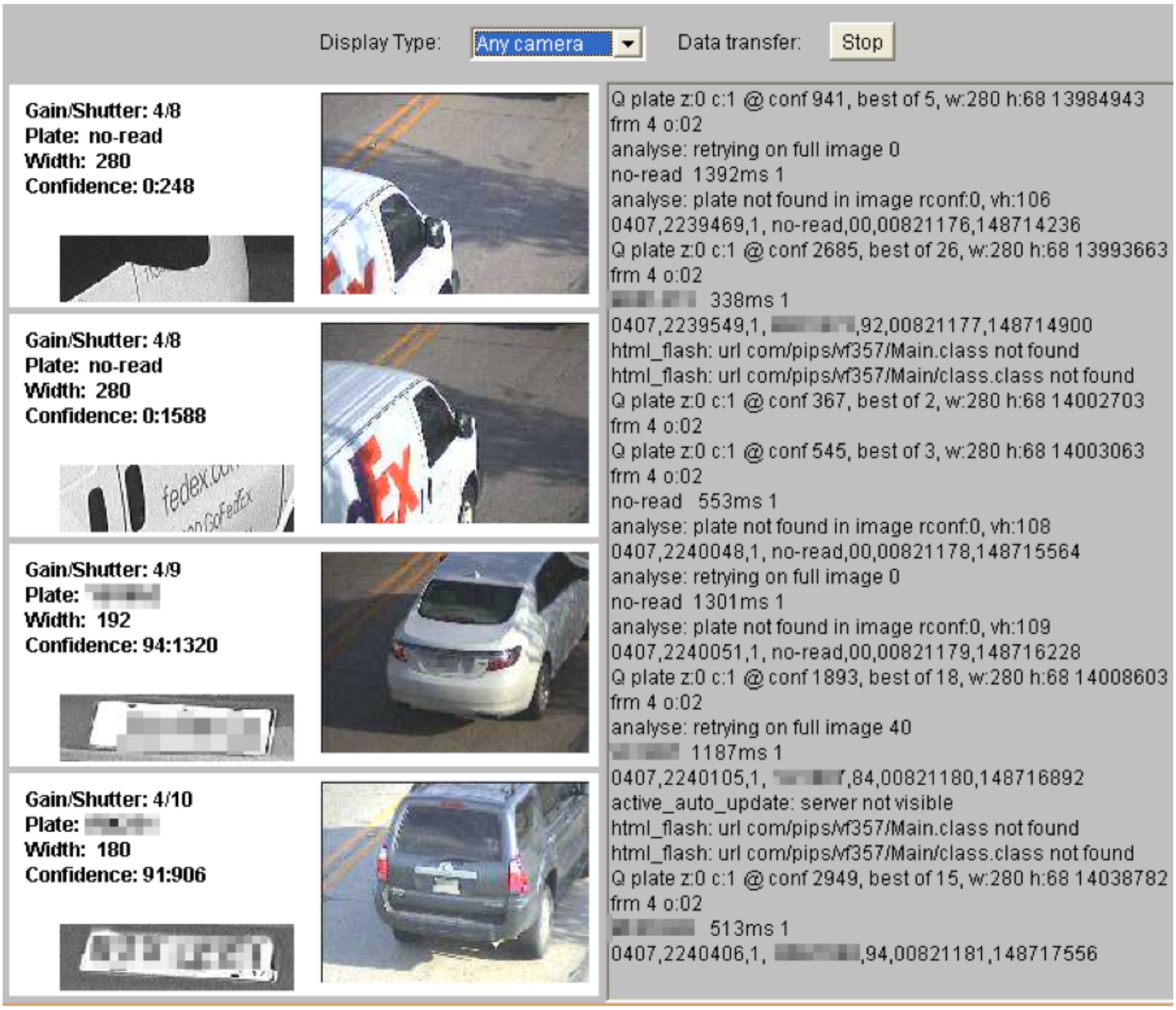
However, thanks to the cooperation of the St. Tammany Parish Sheriff's Office—which communicated with several other agencies—we were able to determine that the other batch of cameras belonged to the Kenner Police Department (KPD).

KPD secured the cameras within a matter of weeks.

Jefferson Parish Sheriff's Office

Once we had eliminated the Kenner and St. Tammany Parish cameras from our list of vulnerable ALPR cameras, one single camera remained. This one, positioned near a church in the Woodmere area, was especially vulnerable.

An example of what we able to view (plates have been redacted to protect the privacy of the drivers):



Display Type: Any camera ▾ Data transfer: Stop

Gain/Shutter: 4/8
Plate: no-read
Width: 280
Confidence: 0:248

Gain/Shutter: 4/8
Plate: no-read
Width: 280
Confidence: 0:1588

Gain/Shutter: 4/9
Plate: [redacted]
Width: 192
Confidence: 94:1320

Gain/Shutter: 4/10
Plate: [redacted]
Width: 180
Confidence: 91:906

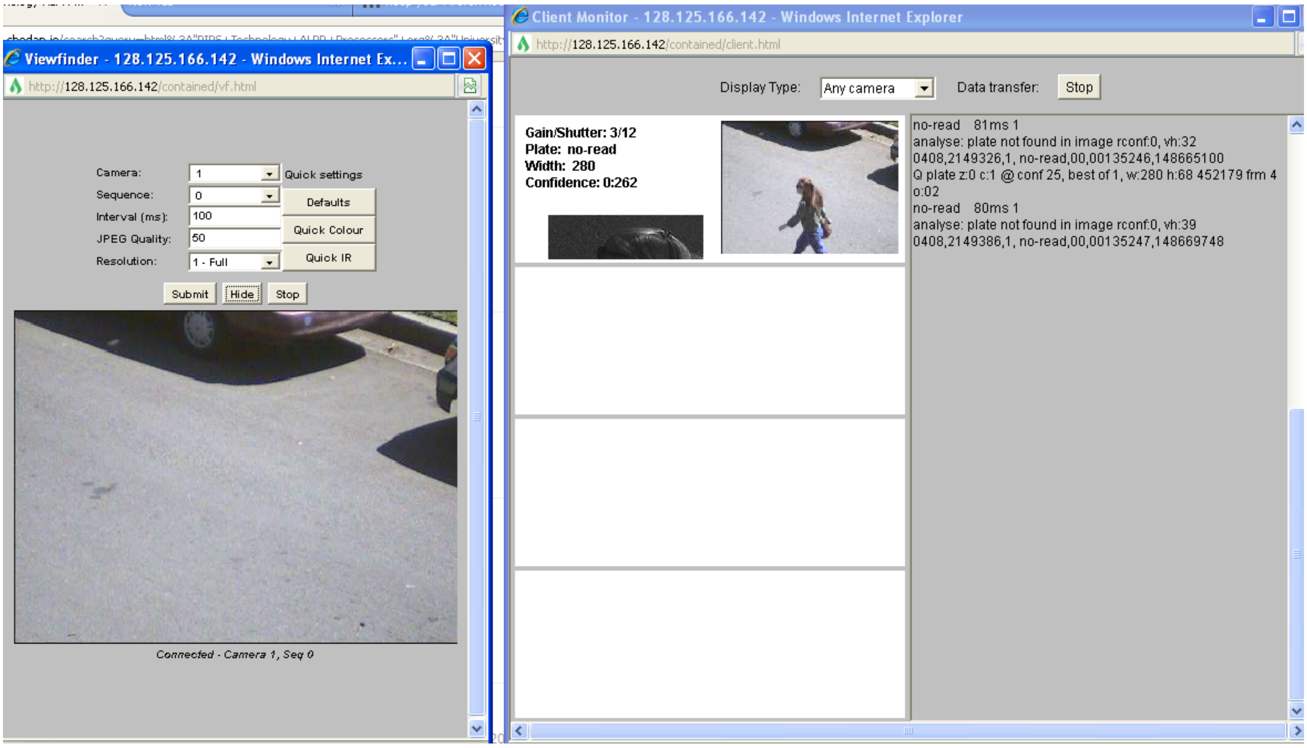
```
Q plate z:0 c:1 @ conf 941, best of 5, w:280 h:68 13984943
frm 4 o:02
analyse: retrying on full image 0
no-read  1392ms 1
analyse: plate not found in image rconf:0, vh:106
0407,2239469,1, no-read,00,00821176,148714236
Q plate z:0 c:1 @ conf 2685, best of 26, w:280 h:68 13993663
frm 4 o:02
[redacted]  338ms 1
0407,2239549,1, [redacted],92,00821177,148714900
html_flash: url com/pips/vf357/Main.class not found
html_flash: url com/pips/vf357/Main/class.class not found
Q plate z:0 c:1 @ conf 367, best of 2, w:280 h:68 14002703
frm 4 o:02
Q plate z:0 c:1 @ conf 545, best of 3, w:280 h:68 14003063
frm 4 o:02
no-read   553ms 1
analyse: plate not found in image rconf:0, vh:108
0407,2240048,1, no-read,00,00821178,148715564
analyse: retrying on full image 0
no-read  1301ms 1
analyse: plate not found in image rconf:0, vh:109
0407,2240051,1, no-read,00,00821179,148716228
Q plate z:0 c:1 @ conf 1893, best of 18, w:280 h:68 14008603
frm 4 o:02
analyse: retrying on full image 40
[redacted]  1187ms 1
0407,2240105,1, [redacted],84,00821180,148716892
active_auto_update: server not visible
html_flash: url com/pips/vf357/Main.class not found
html_flash: url com/pips/vf357/Main/class.class not found
Q plate z:0 c:1 @ conf 2949, best of 15, w:280 h:68 14038782
frm 4 o:02
[redacted]  513ms 1
0407,2240406,1, [redacted],94,00821181,148717556
```

The Jefferson Parish Sheriff's Office initially did not respond to our communications; however, it seems that after communicating with counterparts in St. Tammany Parish, it was able to secure this camera. Eventually, the Jefferson Parish Sheriff did respond: a representative confirmed the camera was now secure, but to double check, they planned to remove the camera for a technical inspection.

University of Southern California

USC had far fewer ALPR cameras exposed than those in Louisiana—only four of what is likely a 60-plus camera network. However, these four cameras were even more vulnerable than the Louisiana cameras, since their controls were hosted on public university pages, with obvious URLs such as pipscam9.usc.edu.

Pipscam9 was particularly problematic. Located on "Fraternity Row" (see it here) and directly across from the Pi Kappa Phi house, the ALPR camera was completely unprotected. One could not only see the license plates passing down the street, but also watch a live video feed (below) of people crossing the street.



Viewfinder - 128.125.166.142 - Windows Internet Ex...

http://128.125.166.142/contained/vf.html

Camera: 1

Sequence: 0

Interval (ms): 100

JPEG Quality: 50

Resolution: 1 - Full

Connected - Camera 1, Seq 0

Client Monitor - 128.125.166.142 - Windows Internet Explorer

http://128.125.166.142/contained/client.html

Display Type: Any camera

Data transfer: Stop

Gain/Shutter: 3/12
Plate: no-read
Width: 280
Confidence: 0:262

```
no-read   81ms 1
analyse: plate not found in image rconf:0, vh:32
0408,2149326,1, no-read,00,00135246,148665100
Q plate z:0 c:1 @ conf 25, best of 1, w:280 h:68 452179 frm 4
o:02
no-read   80ms 1
analyse: plate not found in image rconf:0, vh:39
0408,2149386,1, no-read,00,00135247,148669748
```

Another set of cameras was similarly viewable in a residential neighborhood at 29th St. and Hoover.

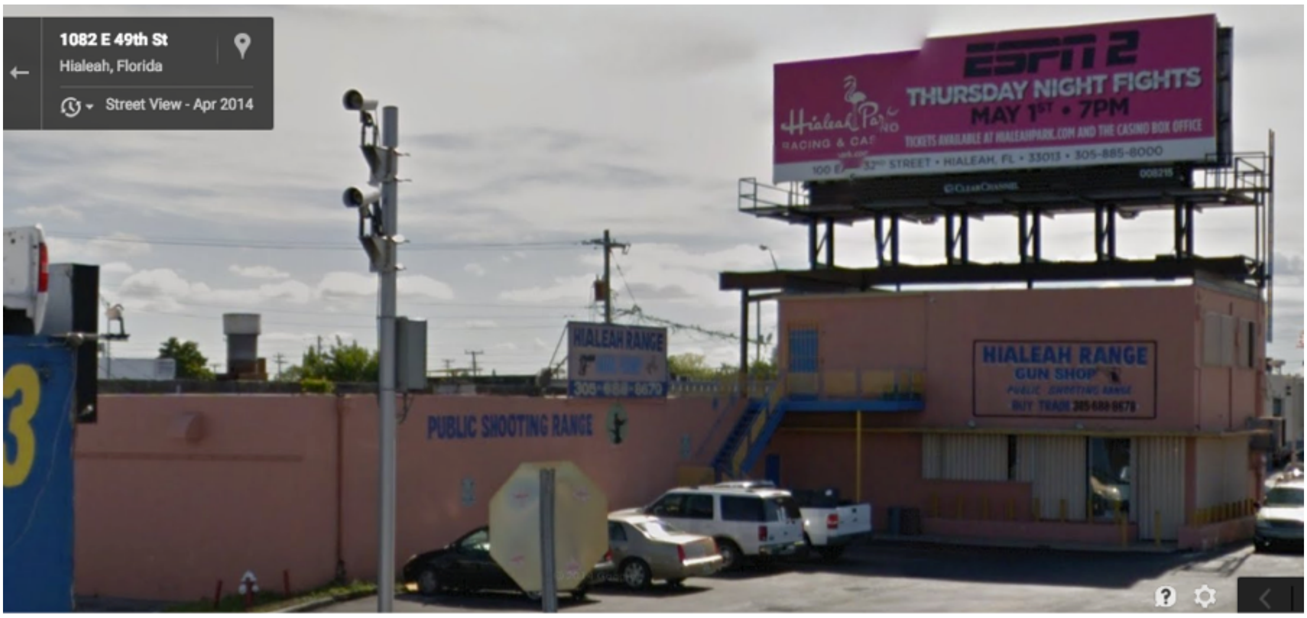
In correspondence with EFF, USC Department of Public Safety Chief John Thomas confirmed our findings after beginning a system-wide audit. Vulnerable cameras were taken offline. USC also improved the complexity of the ALPR administrative passwords.

Thomas wrote:

> As a result of your email I believe we have a more secure ALPR environment and are focused on preventing this from happening again in the future. I am encouraged by the possibility of the Department of Public Safety and EFF having open dialogue regarding information security and will continue working toward a secure crime suppression technology environment.

We subsequently asked USC for its ALPR data retention policies, but Thomas did not respond to the request. Under a new law, USC will need to disclose that information starting in 2016 (see S.B. 34 below).

Hialeah, Florida



Our research turned up at least two cameras in Hialeah, a city in Miami-Dade County, Florida. One of these cameras was near a public firing range and gun shop, positioned in such a way as to capture licenses plates that turned right out of the parking lot.

We initiated discussion with Hialeah's staff, who assured us they would take care of the systems. However, they have since stopped responding to our calls.

Legislation

While we agreed not to talk publicly about these systems when the security issue had yet to be addressed, we felt it was important to use this research to inform decisions over major ALPR-related legislation in California and Louisiana.

Louisiana Senate Bill 250

EFF contacted Louisiana Governor Bobby Jindal's legislative staff, who were weighing whether the governor would sign or veto a bill that would have created a massive statewide ALPR network statewide used to identify uninsured motorists. We expressed our opposition to the legislation, explaining that the government should not expand ALPR surveillance when it has not proven it can safely manage the system currently in place. Subsequently, the governor vetoed the bill, writing:

> Senate Bill No. 250 would authorize the use of automatic license plate reader camera surveillance programs in various parishes throughout the state. The personal information captured by these cameras, which includes a person's vehicle location, would be retained in a central database and accessible to not only participating law enforcement agencies but other specified private entities for a period of time regardless of whether or not the system detects that person is in violation of vehicle insurance requirements. Camera programs such as these make private information readily available beyond the scope of lawn enforcement, pose a fundamental risk to personal privacy and create large pools of information belonging to law abiding citizens that can be extremely vulnerable to theft of misuse.

California Senate Bill 34

The California legislature passed a bill that classified ALPR data as "personal information" under the state's data breach notification laws.The bill required any ALPR operator, including private institutions such as USC, to "maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure." In addition, ALPR system operators are required to publicly post detailed usage and privacy policies.

EFF wrote a letter in support of the measure and described the situation with USC to the governor's office to emphasize that the problems with ALPR were not hypothetical. On October 6, Gov.Jerry Brown signed the bill into law.

Conclusion

While EFF was able to affect ALPR system security in these jurisdictions, dozens of cameras may still be vulnerable in some form. However, in many cases, tracking these devices to their sources has been impossible. It is our hope that with publication of this report, all agencies responsible for PIPS cameras, wherever they are in the country, initiate comprehensive security audits of their devices. ALPR systems are a form of mass surveillance, plain and simple. This technology captures information on every driver, regardless of whether they are under suspicion. In fact, when EFF and the ACLU sent a public records request for ALPR data to the Los Angeles Police Department and Los Angeles County Sheriff's Office, the agencies refused to hand over the data, citing a provision in California law that allows them to withhold investigative records. Who are they investigating? The answer: all cars in California.

If law enforcement agencies are going to pursue this technology, then they should limit storage of this data to as short a time period as possible—days, not years or indefinitely, as is the current practice of many agencies. The safest policy would be to not store data unrelated to crimes at all, but only capture data on hot-listed vehicles suspected of involvement in crimes.

As these cases illustrate, when law enforcement agencies use surveillance systems, they need to be far more vigilant in ensuring that the technology is secure before they deploy it. They must also continue to modernize systems to protect against emerging threats and vulnerabilities. What was cutting edge in 2008 is unlikely to withstand the sophisticated threats of 2015.

Law enforcement should not collect information they can’t protect. Surveillance technology without adequate security measures puts everyone’s safety at risk.

Join EFF Lists