



Outlook

---

**Reminder: Tips and Trends**

---

**From** ICJE, Inc. <jimrechel@icje.ccsend.com>

**Date** Wed 9/9/2026 6:30 PM

**To** pcalvert@alacop.us <pcalvert@alacop.us>



AUGUST 2026

## **When Trust Is Lost**

The corrosive impact of discovering that the people we trusted may not have been who we thought they were.

Several years ago I wrote an ICJE article about a training I conducted for employees of financial institutions in the Shelbyville, Kentucky area. During the presentation I discussed the case of a bank robber named Mike Kirk.

Kirk was from the Shelbyville, Kentucky area. He was not someone who fit the image most people would have of a bank robber. He was a husband, a longtime employee, a member of the community, and an avid hot-air-balloon pilot. Yet he eventually robbed a bank in Paris, Kentucky.

What followed was far more than a bank robbery. His escape became an extended confrontation with law enforcement that included stolen vehicles, gunfire, and an extensive manhunt. Kirk ultimately took his own life when he was surrounded by police.

There was another unusual aspect to the case. Kirk had traveled to Albuquerque, NM for the annual hot-air-balloon festival and stole 78 license plates from vehicles during the trip. Those details, along with the robbery and pursuit, painted a picture of a man whose behavior was radically different from the person many people in his community believed they knew.

I had finished the presentation when a woman approached me. She waited until most of the other attendees had left. She told me that she knew Mike Kirk—not casually. She and her husband had been friends with Kirk and his wife. They attended church together, went out to dinner together, and participated in community activities together. She believed she knew him.

And now she had just heard, in his own voice, what he had done. She stayed and talked with me for quite some time. What she said has stayed with me ever since.

She wasn't simply angry at Mike Kirk. She wasn't simply shocked that he had committed a crime. She had lost something much more fundamental.

She had lost confidence in her own ability to judge people.

If she could know someone for years, socialize with him, attend church with him, and consider him a friend, and still be so completely wrong about who he was, then who else might she be wrong about? Her problem was no longer just Mike Kirk. It was trust itself.

I have thought about that conversation many times since.

## **Trust Is the Invisible Infrastructure of Society**

We tend to think of trust as something personal. I trust my wife. I trust my children. I trust my friends. I trust my doctor. I trust the person handling my money.

But trust operates on a much larger scale. We trust banks to safeguard our money. We trust scientists to report what they believe the evidence demonstrates. We trust physicians to give us their best medical judgment. We trust law enforcement officers to tell us what they know. We trust courts to apply the law fairly. We trust journalists to distinguish fact from opinion. We trust government officials to tell us the truth, even when the truth may be inconvenient.

Most of the time, we don't consciously think about any of this. We don't have the time or ability to independently verify everything. Trust is the invisible infrastructure that allows society to function. It is the lubricant that keeps the machinery of community running. And like other infrastructure, we tend not to notice it until it begins to fail.

## The Problem With Broken Trust

When trust is broken, the damage doesn't necessarily stop with the person or institution that broke it. That is what I saw in Shelbyville. The woman didn't simply conclude, "I can't trust Mike Kirk." Her conclusion was much broader: "If I was wrong about him, who else might I be wrong about?"

That is the corrosive part of lost trust. The circle of suspicion expands. One person becomes several. Several become an organization. An organization becomes an institution. And eventually, people can begin to question the very systems upon which they depend. That is where a personal problem becomes a societal problem.

## We Have Been Watching This Happen

Over the past several years, Americans have been confronted with a steady stream of revelations, conflicting statements, revised explanations, private communications, and newly released documents involving institutions and people we once assumed were trustworthy.

The COVID-19 pandemic provides one of the clearest examples. I am not reopening the debates over specific COVID policies or figures. Those debates have become intensely political, and that is not the point I want to make.

***The larger issue is what happens when people discover information that appears inconsistent with what they were previously told. When a person who was presented as a trusted authority appears to have said something privately that differs from what the public understood him or her to believe, something happens that goes beyond the specific issue being debated.***

People begin asking: "What else don't I know?" And then: "Who else isn't telling me the whole story?" That is the same question I heard from the woman in my training class. The scale is simply different.

## From Personal Distrust to Collective Distrust

One person losing trust in another is unfortunate. Millions of people losing trust in institutions is something else entirely. A person who no

longer trusts one bank can move his money to another. A person who no longer trusts one physician can find another.

But what happens when people begin believing that all banks, all doctors, all scientists, all journalists, all government agencies, or all institutions are potentially untrustworthy?

There is no easy replacement. And that creates a vacuum. Into that vacuum rushes social media, partisan commentary, conspiracy theories, anonymous sources, influencers, and people who claim to possess the “real truth.”

Some of those sources may be correct. Some may be completely wrong.

The problem is that once trust has been sufficiently damaged, people can lose the ability to distinguish between the two. They don't necessarily evaluate information based upon its credibility. They evaluate it based upon whether they trust the person delivering it. We stop asking “Is this true?” and begin asking “Do I trust the person telling me this?” That is a dangerous transition.

## **Trust Does Not Require Perfection**

There is another important point. Trust does not mean believing that someone will always be right. Scientists will be wrong. Doctors will be wrong. Police officers will be wrong. Bankers will be wrong. Government officials will be wrong. All of us will be wrong.

The critical distinction is whether someone is honest about being wrong. There is an enormous difference between “We believed this was true based upon what we knew at the time, but we were wrong” and “We never said that.”

The first can actually strengthen trust. The second can destroy it. People can forgive mistakes. They have a much harder time forgiving deception.

## **The Cost of Distrust**

The consequences extend far beyond hurt feelings. When trust declines, cooperation becomes more difficult. People become more suspicious. Employees question management. Customers question businesses. Citizens question government. Patients question doctors. People question scientific research. Communities become more divided. And every new piece of information is viewed through the lens of suspicion.

That creates a vicious cycle. Less trust produces more suspicion. More suspicion produces less cooperation. Less cooperation produces more division. And more division produces even less trust.

Eventually, society begins operating on the assumption that everyone has an agenda. That is a very difficult environment in which to solve problems.

## **The Fraud Connection**

For those of us involved in financial crime and fraud prevention, this is not an abstract concept, it is the daily terrain we operate in. Trust is at the center of what we do. Every fraud involves the manipulation of trust. The fraudster wants the victim to believe something that isn't true.

The email looks legitimate. The caller sounds legitimate. The website looks legitimate. The employee appears legitimate. The transaction appears legitimate. The fraud succeeds when the victim's normal willingness to trust is exploited.

But there is a paradox. We spend enormous amounts of time teaching people to recognize fraud, yet we cannot build a society in which nobody trusts anyone. That would be impossible. We need trust. We simply need *informed trust*.

We need to understand that trust is earned, maintained, and reinforced by consistent behavior. And when mistakes occur, trust is often preserved by transparency rather than concealment.

## **What I Remember**

I don't remember every detail of the training session that day. I don't remember every slide I presented. I don't remember every question I was asked. But I remember that woman. Because she taught me something about trust that no textbook could have taught me.

The most painful part of discovering that someone has deceived you may not be what they did. It may be realizing that you believed them. And when that happens, the question becomes much larger than the person who deceived you. It becomes: "How do I know whom I can trust?"

That is the question I believe we are increasingly asking as a society. And that should concern all of us.

Because a society can survive disagreement. It can survive political differences. It can survive mistakes. It can even survive bad decisions. What is much harder to survive is a widespread belief that truth itself can no longer be trusted.

## **Rebuilding Trust**

Trust, once lost, is difficult to rebuild. It cannot be restored with a press release. It cannot be restored by telling people that they should

trust again. And it certainly cannot be restored by attacking people who have legitimate questions.

Trust is rebuilt the same way it was originally earned: through consistent behavior. Tell people what you know. Tell them what you don't know.

Admit mistakes. Correct the record.

Explain why decisions changed. Don't pretend yesterday's position never existed.

And most importantly, understand that people have long memories when their trust has been violated.

The woman in Shelbyville, KY taught me that.

Mike Kirk didn't just rob a bank. In the mind of one woman who thought she knew him, he robbed her of something much more difficult to replace: certainty. She could no longer be certain that the people she thought she knew were actually the people she believed them to be.

That is the real danger of shattered trust. And perhaps the question we should all be asking is not simply "Who can I trust?" It is: "What are we doing, as individuals, as institutions, and as a society, to make ourselves worthy of being trusted?"

Because once trust is lost, rebuilding it is not somebody else's responsibility. Trust is rebuilt one decision, one promise, and one interaction at a time. It begins with each of us, in our work, our homes, and every encounter where someone places confidence in us.

May God bless you each and every day as we strive to live according to His will.

Thanks,

Jim Rechel  
ICJE Newsletter Editor

[jimrechel@icje.org](mailto:jimrechel@icje.org)

Mike Kirk - In the Bank



## Training Desk: Educational Opportunities

The ICJE training list has been updated, and we are working on new programs and initiatives, so visit the ICJE website for more 2026 program details.

[Visit our Website](#)

## Open-Source Intelligence (OSINT) for Law Enforcement- Prattville, Alabama

Dates: September 24, 2026

Meets: Th from 9:00 AM to 4:00 PM

Location: Prattville Public Safety Training Center

290 Echlin Blvd

Prattville, AL 36067

APOST Hours: 6.00

Cost: \$0.00

Sorry, this course is full, but you can add your name to the waiting list below.

**NOTE: Students are required to bring a laptop computer capable of accessing the internet. A mobile hotspot is recommended to ensure reliable internet connectivity during practical exercises.**

This course combines classroom instruction with hands-on practical exercises in Open-Source Intelligence (OSINT) gathering and analysis. OSINT is the process of collecting, evaluating, and utilizing information that is legally and publicly available to develop actionable intelligence for investigations, threat assessments, and informed decision-making.

Participants will learn how to identify, collect, verify, and analyze information from a variety of publicly accessible sources, including public records, websites, social media platforms, news reports, online forums, and other open-source resources.

The course emphasizes lawful and ethical methods of information gathering while demonstrating how open-source data can support criminal investigations, intelligence operations, and public safety missions without reliance on classified or restricted information.

Through guided exercises and real-world scenarios, students will develop practical skills in conducting online investigations, validating information,

documenting findings, and transforming publicly available information into usable intelligence products.

Add Your Name to Waiting List

# Intelligence Briefings

Fraud • Physical Security • Investigations • Leadership

## "Flock" for Thought

### **Beyond “Nothing to Hide”: Why Flock and Mass Vehicle Surveillance May Demand Closer Scrutiny**

Republican lieutenant gubernatorial nominee John Wahl recently spoke out against Flock Safety cameras during an episode of Mobile radio's "Jeff Poor Show."

According to Wahl, the automated license plate readers violate the U.S. Constitution, specifically its Fourth Amendment. So I thought it might be something that needs more analysis.

In city council meetings and online debates, two phrases surface again and again whenever automated license plate readers (ALPRs) like those from Flock Safety come up: “If you’re not doing anything wrong, you have nothing to worry about,” and “There’s no expectation of privacy on public roads.”

A closely related view is equally common: giving up some privacy of travel is a small price to pay if it helps catch criminals.

These responses feel intuitive. License plates are required to be displayed. Cars travel in public. Crime is real. Why should anyone object to technology that records what is already visible and aids investigations?

The deeper issues are more consequential than those dismissals allow. The scale, persistence, analytical power, and infrastructure of modern ALPR networks, especially systems that create searchable “vehicle fingerprints”, raise questions about the kind of society we are building and the constitutional and practical limits we are willing to accept. Treating continuous, population-wide monitoring as an acceptable trade-off deserves careful examination rather than reflexive acceptance.

## **License Plates Were Never Designed for This**

Laws requiring vehicles to display identifying markers originated in the early 1900s. New York’s 1901 statute and Massachusetts’ 1903 state-issued plates were responses to reckless “scorchers,” accidents involving horses and pedestrians, and the need to hold specific drivers accountable after specific incidents. The purpose was human-scale identification so that a witness or officer could report a number and authorities could locate the owner.

What exists today is different in kind. Dense networks of cameras automatically capture not only plates but also make, model, color, body type, dents, damage, bumper stickers, roof racks, trailers, and other visible features. These attributes form a “Vehicle Fingerprint” that can be searched even when a plate is missing, partial, or unreadable. Data are retained for days or weeks (historically often 30 days, with newer recommendations around 7 days plus evidence preservation), time-stamped, location-stamped, and queryable across jurisdictions by authorized users.

**The result is a retrospective, searchable log of the movements of the driving population, not a tool for identifying a particular vehicle after a particular event.**

That transformation matters. Aggregation turns discrete public observations into a detailed historical record capable of revealing routines, associations, and the “privacies of life.”

## **The Constitutional Stakes Are Real**

Under the framework established in *Katz v. United States* (1967) and elaborated in cases such as *United States v. Jones* (2012) and *Carpenter v. United States* (2018), the Fourth Amendment protects reasonable expectations of privacy even in public spaces when surveillance becomes comprehensive, effortless, and retrospective.

Prolonged tracking that creates an intimate window into a person's movements can constitute a search requiring a warrant.

Challenges to Flock and similar systems argue precisely this. Vehicle fingerprinting strengthens the claim: each capture becomes more unique and linkable, enabling route reconstruction, convoy analysis, and searches based on visual descriptions rather than plates alone. Stickers can reveal political or religious associations.

Dense networks make it difficult to drive any meaningful distance without generating records. Warrantless querying of the resulting database, critics contend, exceeds the limited identification function that justified plate-display laws in the first place.

Courts have so far often distinguished current deployments from the continuous, person-linked data in *Carpenter*, citing camera density and retention periods. Litigation continues, including appeals and denser-network cases, and state constitutions or specific privacy statutes sometimes provide additional avenues. The legal outcome remains unsettled, but the underlying tension is clear: technology has outpaced the original regulatory bargain.

## **What the Systems Actually Collect and Enable**

Flock states that its ALPR cameras focus on vehicles rather than people, do not use facial recognition, and do not collect biometric or personal identifying information linked to individuals inside the system. Those claims are accurate as far as the product's designed search functions go. Yet the images retained are of the vehicle's rear and can, under favorable lighting, angle, and window conditions, include visible occupants. Law enforcement users who receive those images can examine them visually or apply external tools.

More significantly, the marketed capability to search by dents, stickers, racks, and similar features expands utility far beyond basic plate reading. When privacy concerns are raised, emphasis often shifts to "vehicles, not people" and the public nature of plates. When demonstrating value to agencies, the power of the full fingerprint is highlighted. Both descriptions can be true; the selective emphasis shapes public understanding.

Access is controlled by customers, primarily law enforcement agencies and some private entities, who own their data and decide sharing arrangements. Private customers generally cannot access government data, and sharing is often configurable. Still, once collected and retained, the data exist in a system designed for investigative querying, with audit logs but without a warrant requirement for most searches.

## Why “A Small Price to Catch Criminals” Undersells the Trade-Off

The argument that privacy of travel is a minor cost for greater public safety rests on several assumptions that deserve scrutiny.

First, these systems do not primarily collect data on criminals. They indiscriminately log the movements of the vast majority of drivers who are not suspected of any crime. The database is populated by ordinary travel; investigative use is a secondary filter applied later. The “price” is therefore paid continuously by the general public, not only by those who ultimately become subjects of investigation.

Second, the tools are not immune to error or misuse. Documented cases include officers using ALPR access to stalk romantic partners or track individuals for personal reasons. False or low-confidence plate reads have led to wrongful stops, sometimes at gunpoint. Even when the technology works as designed, the absence of a warrant requirement for most queries removes a traditional check that forces officers to articulate particularized suspicion before accessing detailed location histories.

Third, effective policing has long operated with targeted tools, witness descriptions, warrants, and post-incident investigation. Expanding to population-level, always-on recording changes the baseline from investigation of specific wrongdoing to continuous monitoring of everyone in case something useful appears later. That shift is not a small increment; it is a different model of the relationship between the state and the public.

Finally, once the infrastructure exists, dense cameras, long retention options, inter-agency sharing, and powerful search capabilities, it becomes available for broader uses and harder to constrain. What begins as a tool for recovering stolen vehicles or locating missing persons can expand in practice. Treating the privacy cost as trivial risks normalizing a permanent surveillance capacity whose full implications only become clear over time.

## Looking Deeper

The objection is not that every driver is a criminal suspect, nor that public safety tools have no value. It is that a society in which detailed, searchable records of the movements of the entire driving population are routinely created and retained changes the practical reality of anonymity in public space and the balance of power between citizens and government.

License plates were introduced so that specific wrongdoing could be investigated. Mass vehicle fingerprinting creates the capacity to examine nearly anyone’s movements after the fact. Those are not the same thing.

***Readers who value effective crime-fighting tools should still ask hard questions about scale, retention, query standards, data sharing, transparency, error rates, and the cumulative effect of layering such systems across cities and states.***

The issues run deeper than whether an individual has done anything wrong, whether a single plate is visible on a public road, or whether catching some criminals feels worth a modest personal inconvenience. They concern the surveillance capacity we are embedding into everyday infrastructure, and whether that capacity remains compatible with the privacy expectations a free society requires.



## **Law enforcement says Flock cameras remain vital public safety tool despite isolated incidents**

Recent officer investigations have renewed debate over Alabama's Flock license plate reader cameras, privacy safeguards and statewide

[Read More](#)



## **'People's information should be protected': Alabama sheriffs react to Flock camera policy**

## changes

Flock Safety, the developer of controversial cameras that automatically scan license plates to detect criminals, announced Thursday they are making four primary policy changes.

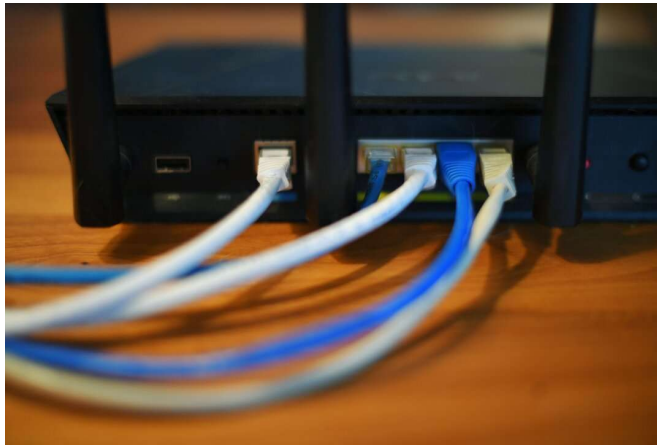
[Read More](#)



## Fake Bank Call Convinced Her to Open Her Safe. Police Say a Man Drove Off With \$1.5 Million in Jewelry and Metals

A phone call from people posing as bank employees ended with a stranger driving into a Florida woman's garage and leaving with approximately \$1.5 million ... [Read More](#)

[Read More](#)



## Cyber Group Finds Surveillance Backdoors in Routers Sold in US

The same hidden software was found operating on at least hundreds of routers in China, most connected through China Mobile.

[Read More](#)

## Pondering Our Security



## FBI eases hiring standards and won't rule out applicants over prostitution or bestiality

Applicants who paid for sex fewer than three times in the last decade will not be automatically ruled out of FBI employment

[Read More](#)



## **Woman who exposed FBI official for working with Russian oligarch found dead**

A judge praised Allison Guerriero for her "extraordinary contributions" to counterespionage ops on behalf of the United States.

[Read More](#)

# Investigations

# Apple / iCloud: What Investigators Need to Know - (2026 Update)

I recently attended a breakout session at a conference in Nebraska, led by two local detectives who were highlighting the sources of information they access via search warrants issued to Apple. It was eye opening as to how much of our data is held by Apple, but just as beneficial was getting a better understanding of the volume of data available for investigative use.

Apple's Legal Process Guidelines for Government & Law Enforcement within the United States (Oct. 2025) is the definitive resource for understanding what Apple retains, how long it keeps it, and what legal process is required.

For investigators working fraud, cybercrime, or multi-device cases, Apple's guide is far more accurate than third-party subpoena charts.

## Key Takeaways for Investigators

1. iCloud content requires a search warrant. Subpoenas only return subscriber and limited connection information.
2. 25-Day Retention Window
3. iCloud connection logs, Mail logs, and Find My logs are retained up to 25 days, making early preservation critical.
4. Preservation Requests:

Under §2703(f), Apple preserves existing data for 90 days, renewable once.

Preservation covers only what exists at the moment Apple receives the request.

Advanced Data Protection (ADP): If enabled, Apple cannot decrypt Photos, iCloud Drive, iCloud Backup, Notes, or Safari Bookmarks. Email, contacts, and calendars remain accessible with a warrant.

## Legal Process Overview

- Subpoena: Subscriber/account info, limited connection logs
- §2703(d) Order: Mail logs, transactional records, certain Find My activity
- Search Warrant: Photos, email content, iCloud Drive, backups, messages, contacts, calendars, Safari/Maps history, stored files

## Don't Forget the Ecosystem

iCloud is only one part of Apple's data universe. Investigators may need separate legal process for Find My device activation, Apple ID/iForgot, FaceTime, iMessage, APNs, Apple Store transactions, and more.

## Identifier Limits

Apple accepts up to 25 identifiers per request. More than 25 requires additional legal process.

If your agency handles fraud or multi-device investigations, consider distributing a one-page Apple/iCloud reference card to investigators. A downloadable version is included below.

[Apple Data Reference Guide](#)

# Leadership Desk



## Leadership Behavior And Generation Gaps

Navigating the dynamics of leadership behavior across generational gaps is critical for organizational success.

[Read More](#)

# Church Leaders and Security

This CISA tool is designed to guide personnel at houses of worship through a security-focused self-assessment to understand potential vulnerabilities and identify options for consideration in mitigating those vulnerabilities.

This self-assessment is a first step in building an effective security program; it is not intended to be an in-depth security assessment. After completing this process and addressing preliminary findings, houses of worship personnel may consider pursuing more detailed security assessments to explore specific issues in greater detail.

Security Self-Assessment

## "Crossroads" Desk

### Youth Sports Programs Reducing Crime!!??



## Youth Football Coach SNAPS! HITS Woman during WILD BRAWL!

[Read More](#)

# One Last Thing

**"The consequences of turning a blind eye to government corruption go far beyond simply letting some corrupt politicians and bureaucrats walk free.**

Tom Fitton



ICJE, Inc. | P.O. Box 293 | Montgomery, AL 36101 US

[Unsubscribe](#) | [Update Profile](#) | [Constant Contact Data Notice](#)



Try email & social marketing for free!